UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

CORSO DI LAUREA TRIENNALE IN "DIRITTO E TECNOLOGIA"

Percorso "Giuridico"

TESI DI LAUREA

LA FORMAZIONE DELLA PROVA DIGITALE NEL PROCESSO PENALE

RELATORE

DR. MASSIMO BOLOGNARI

LAUREANDO

ANDREA BUSANA

ANNO ACCADEMICO

2023/2024

Ringraziamenti

Ringrazio per la disponibilità il docente Massimo Bolognari, mio relatore,
che con attenzione ha seguito il mio lavoro.

Ringrazio la mia famiglia e tutti coloro che mi sono stati vicini durante questo percorso
e nella vita in generale, dandomi sostegno tutte le volte in cui ne ho avuto bisogno.

INDICE

Introduzione

Con la seguente tesi di laurea, composta da tre capitoli, si è voluto analizzare l'importanza assunta dalle prove digitali nel processo penale. Il primo capitolo approfondisce aspetti più teorici e normativi, offrendo al lettore un'accurata definizione di prova digitale a partire dall'analisi etimologica del termine ed inoltre spiega approfonditamente cosa siano i dati digitali a partire dall'unità minima che li compone, ossia il bit, e il confronto tra dati e metadati, inoltre si evidenzia come quest'ultimi costituiscano l'elemento di distinzione tra la prova digitale e la prova analogica. Nel primo capitolo si trova inoltre un'ampia spiegazione degli interventi normativi, sia a livello internazionale mediante la Convenzione di Budapest, sia a livello nazionale italiano attraverso la legge n.48 del 18 marzo 2008 di ratifica alla Convenzione. Il secondo capitolo, intitolato l'acquisizione forense delle prove digitali, offre al lettore un'analisi legata a molti aspetti pratici, rispetto a quelli puramente teorici evidenziati nel corso del primo capitolo. Si procederà all'analisi di uno degli aspetti che caratterizza maggiormente le prove digitali, ossia la loro fragilità. Il capitolo si conclude con lo studio della diversa qualificazione degli accertamenti tecnici tra ripetibili e irripetibili e con l'analisi di alcune sentenze della Cassazione italiana a sostegno della ripetibilità.

Il terzo e ultimo capitolo della tesi, si occuperà di analizzare due sentenze emesse rispettivamente nel Regno Unito e negli Stati Uniti, con il fine di far comprendere e riflettere il lettore sulle differenze sostanziali tra l'ordinamento italiano e quello di Common Law, anche e soprattutto per via di una carente regolamentazione del legislatore italiano, mediante la legge n. 48/2008, sulle modalità di svolgimento delle diverse attività di indagine ad oggetto informatico. All'interno del terzo e ultimo capitolo saranno racchiuse inoltre le conclusioni, che sulla base di quanto analizzato in precedenza, daranno al lettore il punto di vista dell'autore su alcuni aspetti critici derivati da questa carenza, in alcuni casi assenza, di regolamentazione sulle modalità che il PM e la polizia giudiziaria durante la fase di indagine mettono in atto e soprattutto sulla mancata previsione di sanzioni per l'inottemperanza delle regole di comportamento, prevedendo solamente una valutazione sull'attendibilità da parte del giudice. Inoltre sempre al suo interno, analizzando in prima battuta le due opposte teorie su cui si fondano, vi sarà un ampio confronto tra la diversa classificazione di accertamenti tecnici data dall'ordinamento italiano attraverso lo studio di diverse sentenze della Cassazione, da un lato, e dall'ordinamento inglese e statunitense di Common Law, dall'altro.

CAPITOLO I

LE PROVE DIGITALI

Sommario: 1. La prova digitale nel processo penale. – 2. Dati digitali: dal bit all'informazione. – 3. Differenza tra prova digitale e prova analogica. – 4. La Convenzione di Budapest del 2001 sulla criminalità informatica. – 5. La Legge 48 del 2008 di recepimento della Convenzione di Budapest.

1. La prova digitale nel processo penale

Prima di analizzare l'utilizzo delle prove digitali all'interno del processo penale, è bene soffermarsi sul significato etimologico delle due parole che compongono questo termine: prova e digitale. Le prove sono disciplinate dal libro terzo del codice di procedura penale che disciplina i principi generali, i mezzi di prova e i mezzi di ricerca della prova. Essa può essere definita come il ragionamento che da un fatto noto ricava l'esistenza di un fatto avvenuto nel passato e sulle quali modalità di svolgimento il giudice deve formare il suo convincimento. L'articolo 27 della Costituzione sancisce la cosiddetta presunzione di innocenza e l'onere della prova, ciò significa che la colpevolezza dell'imputato deve essere dimostrata dalla pubblica accusa, vale a dire dal magistrato del pubblico ministero, che avrà il compito di provare la colpevolezza dell'imputato, senza che permanga in proposito alcun ragionevole dubbio, il quale fino ad allora si presume innocente e potrà a sua volta decidere di provare la sua innocenza[1]. In ossequio al principio accusatorio che governa il sistema processuale italiano, sebbene alcune caratteristiche del sistema inquisitorio siano state riprese dal nostro processo, ai sensi dell'articolo 190 c.p.p. le prove sono ammesse a richiesta di parte, salvo i casi in cui la legge stabilisce che si proceda d'ufficio. Ciò comporta che ad entrambe le parti in causa sia riconosciuto il diritto alla prova[2]. Il termine digitale deriva dal latino digitus o dito, tuttavia in ambito tecnologico, proviene dall'inglese digit o cifra numerica. Molto spesso il termine digitale viene utilizzato come sinonimo di tecnologico, in realtà ha tutt'altra definizione; infatti, il *digital* rappresenta ciò che tratta, misura o elabora grandezze in forma numerica, ad esempio una macchina fotografica digitale memorizza un'impressionante serie di numeri che attribuiscono ad ogni pixel dell'immagine determinati caratteri. Dai significati delle due parole che compongono il termine prova digitale, posso definire quest'ultima come

[1] Costituzione della Repubblica Italiana, art. 27: "La responsabilità penale è personale. L'imputato non è considerato colpevole sino alla condanna definitiva. Le pene non possono consistere in trattamenti contrari al senso di umanità e devono tendere alla rieducazione del condannato. Non è ammessa la pena di morte.".
[2] Prova. Diritto processuale penale in "Enciclopedia on line Treccani".

ogni informazione probatoria che assume rilevanza nel processo penale in virtù del contenuto del dato o dalla sua allocazione su una determinata periferica, in sostanza qualsiasi dato o informazione di natura digitale in grado di assumere una valenza probatoria[3].

La scienza trova applicazione nel processo penale con lo scopo principale di aiutare nell'accertamento dei fatti di reato, un esempio concreto è rappresentato dalla rilevanza assunta nel sistema processuale dalla medicina legale. L'avvento della digitalizzazione e l'utilizzo sempre più diffuso degli strumenti informatici e telematici per la trasmissione, ricezione ed elaborazione delle informazioni, oltre a comportare la creazione giornaliera di una quantità enorme di dati molti dei quali di sicuro interesse ai fini processuali, che risulta difficilmente governabile dall'uomo senza l'ausilio degli appositi strumenti tecnologici, ha fatto sorgere l'esigenza per gli organi investigativi di ricercare elementi di prova tra i dati contenuti in sistemi informatici o telematici[4]. Proprio per questa ragione in un numero sempre più crescente di processi, diventano fondamentali le cosiddette prove digitali, ossia quelle prove che si acquisiscono dai sistemi informatici e telematici, come ad esempio lo sono i file contenuti in tali sistemi, che al loro interno contengono testi, suoni, immagini o registrazioni. Tali prove non sono utilizzate limitatamente alla repressione dei reati informatici, ossia i reati che il Codice penale italiano raggruppa in tre macrocategorie: frodi informatiche, falsificazione informatica e danneggiamento informatico, disciplinate rispettivamente dagli artt. 640 ter, 491 bis e 635 bis del Codice penale, che vengono definiti come quei reati caratterizzati dall'abuso della tecnologia informatica o telematica sia hardware che software, con lo scopo di commettere uno o più crimini, e che sono stati introdotti appunto nel Codice penale attraverso la legge 547/1993[5]. L'ambito operativo potenzialmente illimitato delle prove digitali è tra l'altro disciplinato dal paragrafo 2 dell'articolo 14 della Convenzione di Budapest del 2001, ossia dalla Convenzione del Consiglio di Europa sulla criminalità informatica della quale tratterò in seguito, il quale afferma che ogni Stato aderente alla Convenzione deve applicare i poteri e le procedure menzionati nel paragrafo 1: ai reati previsti in

[3] L. Marafioti, Digital evidence e processo penale, *Cassazione Penale*, 2011, p.4509. «ogni informazione probatoria la cui rilevanza processuale dipende dal contenuto del dato o dalla particolare allocazione su di una determinata periferica, oppure dal fatto di essere stata trasmessa secondo modalità informatiche o telematiche»

[4] L. Lupária - G. Ziccardi, *Investigazione Penale e tecnologia informatica*, Milano, Giuffrè, 2007, p. 127 e ss.

[5] S. Pietropaoli., *Informatica criminale. Diritto e sicurezza nell'era digitale*. Giappichelli, 2022, pag. 11-14.

conformità agli articoli da 2 a 11 della Convenzione, a tutti gli altri reati commessi attraverso un sistema informatico e all'insieme delle prove elettroniche di un reato[6]. Reati che possono essere distinti in tre macrocategorie[7]:

- I *reati informatici e telematici propri*, ossia quei reati in cui il dispositivo digitale o il sistema informatico costituiscono l'oggetto materiale della tutela penale.
- I *reati occasionalmente informatici* (reati comuni a condotta libera) in cui il dispositivo digitale, le sue funzioni di produzione e trasmissione di dati digitali, e/o gli stessi dati digitali, costituiscono lo strumento per la realizzazione di tutta o parte della condotta che costituisce il reato.
- *Reati comuni e/o speciali* per il cui accertamento vengono acquisiti ed analizzati dati digitali generati da dispositivi digitali quali indizi o mezzi di prova.

2. Dati digitali: dal bit all'informazione

Come già anticipato nel paragrafo precedente, l'avvento della digitalizzazione e l'utilizzo sempre più diffuso dei sistemi informatici e telematici, ha reso necessaria la ricerca di elementi di prova tra i dati digitali contenuti in tali sistemi, da parte degli organi investigativi. I dati digitali costituiscono le fondamenta su cui si erge il mondo digitale, essi rappresentano insiemi di informazioni codificate e memorizzate in forma binaria. Questa tipologia di dati si contrappone ai dati analogici, in quanto è rappresentata da una sequenza di bit, unità binarie che possono assumere i valori 0 o 1. Tra le caratteristiche principali, che contraddistinguono i dati digitali, vi sono la velocità di generazione, la varietà delle fonti e la complessità strutturale. La velocità di produzione dei dati è strettamente correlata alla diffusione della tecnologia digitale nella vita quotidiana, mentre la varietà delle fonti riflette i diversi formati e tipologie di dati, tra cui immagini, testi, suoni e video. Tra i principali vantaggi derivanti dall'utilizzo dei dati digitali, spiccano la facilità trasmissione e la facilità di manipolazione. Per quanto riguarda la trasmissione, l'istantaneità ha rivoluzionato le comunicazioni consentendo una connessione globale e facilitando la condivisione di informazioni, mentre la facilità di

[6] Convenzione del Consiglio d'Europa sulla criminalità informatica, Budapest, 2001, art. 14 par.2 "Ambito di applicazione delle disposizioni procedurali".
[7] A. Gammarota, Materiali didattici, UNIPD Seminario 2023.

manipolazione, dal punto di vista giuridico, rappresenta un limite, tanto che si parla della cosiddetta *fragilità delle prove digitali*.

Nel contesto odierno, sempre più digitalizzato, ha assunto particolare importanza l'*informatica forense*, ossia quella branca dell'informatica giuridica che studia le norme giuridiche e le regole tecniche per il trattamento dei dati digitali a fini forensi[8]. Le informazioni, su cui si fonda la verità processuale, dipendono dai dati digitali; dunque, la qualità della verità processuale dipende dalle qualità dei dati digitali. Una rappresentazione visiva di questo rapporto tra dati digitali e informazioni, vedrebbe il bit all'interno del dato che a sua volta si troverebbe all'interno dell'informazione, e da quest'ultima si desumono i fatti su cui si fonda il processo.

Iniziando dall'unità minima d'informazione, ossia il bit, dall'inglese *BI*nary Digi*T*, in italiano cifra binaria, esso identifica una scelta elementare tra due variabili: vero/falso, destra sinistra, bianco/nero e così via. Un insieme di bit prende il nome di stringa, mentre 8 bit formano un byte, ovvero una sequenza utilizzata per codificare un singolo carattere alfanumerico in un computer. Il byte rappresenta l'unità di misura della capacità di memoria. La codifica delle immagini, dei video e dei suoni segue il codice Unicode, ideato dall'Unicode Consortium, consorzio formato da società produttrici di computer che hanno creato un nuovo sistema di codifica chiamato Unicode, poi divenuto standard nel 2012 (IS 10646), basato prima su una codifica a 16 bit e poi a 21 bit. Tale codice presenta tuttavia dei limiti, accade perciò che la codifica venga effettuata anche con altri codici.

La codifica delle immagini può essere di tipo vettoriale oppure raster (o bitmap)[9]:

- Attraverso la *codifica vettoriale* l'immagine è descritta mediante elementi primitivi quali punti, linee o poligoni, per ognuno dei quali è definita una colorazione o una sfumatura, che poi vanno a comporre l'immagine.
- Con la *codifica raster (o bitmap)* l'immagine è composta da una matrice di punti, detti pixel, la cui colorazione è codificata tramite uno o più bit.

Nelle immagini monocromatiche in scala di grigio, il valore indica l'intensità del grigio, che varia dal nero al bianco, mentre nelle immagini a colori il pixel assume il livello di intensità dei colori fondamentali. Il suono è rappresentato da un'onda sonora che descrive

[8] S. Aterno - F. Cajani - G. Costabile, *Cyber forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*. Giappichelli, 2021, pag. 1.
[9] A. Gammarota, Materiali didattici, UNIPD Seminario 2023.

la variazione della pressione dell'aria, rispetto alla pressione atmosferica, nel tempo. La rappresentazione digitale dell'onda avviene mediante una serie di bit, quanto maggiore è il numero di bit usati, più fedele sarà la rappresentazione dell'audio. Per digitalizzare un'onda sonora si fa il cosiddetto *campionamento*, ossia si misura l'ampiezza dell'onda a intervalli costanti nel tempo, e successivamente ogni misurazione sarà convertita in codice binario[10].

La codifica dei video può avvenire secondo due diverse tecniche: l'*intraframe* e l'*interframe*. Con la prima tipologia viene codificato ogni singolo fotogramma che compone la sequenza video. Con la codifica interframe si parte codificando un fotogramma iniziale secondo la tecnica intraframe, vengono descritti i cambiamenti che si verificano tra un fotogramma ed il successivo[11].

Una volta analizzati i bit e le varie tipologie di codifica delle immagini, dei suoni e dei video, vorrei proseguire con la definizione, di ciò che racchiude questi elementi. Con il termine dato, si indica qualsiasi descrizione iniziale di qualsiasi cosa, inclusi eventi, attività e transazioni registrate, archiviate e classificate, ma non organizzate in un modo che vada il oltre il significato originale. I dati possono essere costituiti da lettere, numeri, suoni, o immagini. I dati sono anche definiti dati interni, in quanto si tratta di quelli creati dall'utente che rappresentano il contenuto del file e che sono normalmente visualizzati. Dalla classificazione e interpretazione dei dati, che determina per il destinatario un valore e un significato che va oltre la loro forma grezza originale, possono essere colte informazioni. Un ulteriore aspetto che deve prendere in considerazione l'informatica forense sono i metadati; infatti, se i dati sono la descrizione grezza di tutto, i metadati non so altro che i dati che riguardano altri dati, in inglese *Data about Data*. I metadati sono anche detti dati esterni, in quanto sono accessori al file, creati dal sistema o dall'applicazione e normalmente non sono visualizzati ma visualizzabili. In questa categoria rientrano ad esempio il nome utente, la data di creazione, il formato e la dimensione del file. Quando ad esempio si salva un file Word, il software aggiunge il nome utente associato al profilo, che era stato definito in precedenza durante l'installazione del programma, al file di testo in base ad un'impostazione predefinita. I metadati come vedremo nel paragrafo successivo possono essere considerati come l'elemento di distinzione tra la prova digitale e la prova analogica.

[10] A. Gammarota, Materiali didattici, UNIPD Seminario 2023.
[11] A. Gammarota, Materiali didattici, UNIPD Seminario 2023.

3. Differenza tra prova digitale e prova analogica

Per comprendere quali siano le concrete differenze tra la prova digitale e la prova analogica, e l'importanza assunta dalle prima in seguito alla globalizzazione e al sempre più diffuso utilizzo di strumenti digitali, vorrei ora evidenziare una serie di esempi a riguardo. Analizzando una fotografia, si può ben comprendere come all'interno di un processo quest'ultima sia in grado di rappresentare lo stato dei luoghi in un determinato momento, che corrisponde a quello in cui la foto viene scattata. Secondo quanto affermato in numerose sentenza dalla Cassazione, la fotografia ha valore di prova analogica , ed è compresa tra le prove documentali, quando è stampata e pertanto si è in grado di conoscere da essa soltanto lo stato dei luoghi. Quando invece la fotografia è presa da un dispositivo elettronico, come ad esempio uno smartphone, si possono ricavare da essa molti più dati, tra cui la data e l'ora, il dispositivo con cui è stata realizzata e se la localizzazione del dispositivo risultava attiva nel momento in cui la foto è stata scattata, si potrà ricavare da essa anche il luogo in cui è stata realizzata. L'acquisizione di una fotografia in formato digitale, oltre a garantire l'accesso a tutti questi dati, permette inoltre di comprendere se siano o meno intercorse delle modifiche a quell'immagine.

Un altro esempio riguarda l'acquisizione a processo di audio, quest'ultimo infatti può essere trascritto e in tal caso è considerato prova analogica, oppure può essere in formato digitale e portare a conoscenza di tutti quei metadati che caratterizzano la fotografia in formato digitale, dunque la data, l'ora, ma anche il formato del file e le sue dimensioni. Un altro aspetto di non poco conto ai fini processuali riguarda le modalità in cui determinate parole sono pronunciate, ciò indubbiamente non sarebbe ricavabile dalla semplice lettura della trascrizione dell'audio

Infine un file di testo, tra cui un documento di Word, come accade nel caso della fotografia quando è stampato diventa un documento analogico, da cui si ha la possibilità di leggere il contenuto, ma non le caratteristiche del contenitore. Dal file Word in formato digitale è possibile ricavare il nome utente, il dispositivo nel quale è stato realizzato, quando è stato creato e a quando risale l'ultima modifica. Tali dati possono risultare di fondamentale importanza in alcuni processi, tra cui anche il delitto di Garlasco di cui parlerò successivamente nel corso del secondo capitolo, dove si era evidenziata l'alterazione o addirittura la perdita di molti dei metadati che come emerso poi dalle relazioni peritali e dal consulente tecnico del PM potevano essere importanti ai fini della ricostruzione del caso e dell'alibi presentato dall'allora indagato.

Evidenziata l'imprescindibile importanza assunta dai metadati in un contesto sempre più digitalizzato, si è resa necessaria un'appropriata regolamentazione in materia. Anche in virtù di quanto appena detto, nei due successivi paragrafi scriverò di come a partire dalla Convenzione di Budapest del 2001 e dalle successive, nel tempo, legislazioni nazionali, tra cui la Legge 48/2008 di ratifica della Convenzione, si sia cercato di porre delle regole a contrasto della criminalità informatica, con l'obiettivo di armonizzare la disciplina interna degli Stati nella lotta ad essa.

4. La Convenzione di Budapest del 2001 sulla criminalità informatica

La Convenzione del Consiglio di Europa sulla criminalità informatica, nota come Convenzione di Budapest, è stata stipulata il 23 novembre 2001 e rappresenta un fondamentale strumento internazionale per la lotta alla criminalità informatica o cybercrime. Alexander Seger, capo della divisione della criminalità informatica del Consiglio d'Europa, e Marija Pejcinovic Buric, segretaria generale del Consiglio d'Europa, intervenuti assieme a numerosi ministri e procuratori generali durante la conferenza annuale del Consiglio d'Europa nel novembre 2021 per celebrare il 20° anniversario della Convenzione, hanno affermato come quest'ultima rappresenti un mezzo per garantire un Internet libero, dove le informazioni possono fluire liberamente, essere consultate e condivise, dove le restrizioni sono definite per contrastare l'uso improprio e dove vengono indagati e perseguiti solo reati specifici, fatte salve le necessarie garanzie[12].

Tra le caratteristiche principali della Convenzione rientrano il carattere innovativo e la flessibilità. È sicuramente innovativa perché si concentra su una definizione piuttosto dettagliata del mondo digitale, con frequenti richiami ai sistemi informatici e telematici, ad internet e ai dati. È flessibile poiché ha lasciato libertà alle parti negoziali di adottare norme nazionali a riguardo, sulla base di quanto avevano previsto e sottoscritto attraverso la Convenzione, e non ha escluso la possibilità futura di sottoscrivere nuovi accordi e utilizzare mezzi e vie di cooperazione internazionali. Questa possibilità è testimoniata dal fatto che durante la redazione della Convenzione, gli Stati non giunsero ad un accordo sul tema inerente al reato di diffusione in rete di propaganda razzista. Nonostante il sostegno generale nell'includere questo crimine alla Convenzione, per via della complessità del

[12] M. Arena, *La Convenzione di Budapest del Consiglio d'Europa sulla repressione della criminalità informatica*, Catania, CRIO Papers, 2021, p. 3.

problema si decise di rinviare la questione al Comitato Europeo per i problemi della criminalità (CDPC), il quale assunse il compito di elaborare un protocollo aggiuntivo alla Convenzione di Budapest, relativo alla criminalizzazione dei reati di natura razzista e xenofoba commessi a mezzo di sistemi informatici, il quale fu firmato a Strasburgo nel 2003[13]. Nel 2017 i lavori preparatori per l'elaborazione di un secondo protocollo aggiuntivo hanno condotto alla redazione di cinque testi provvisori, che sarebbero vincolanti per gli Stati aderenti alla Convenzione di Budapest che hanno ufficialmente acconsentito alla loro adozione. Nonostante qualsiasi Paese possa servirsi della Convenzione come linea guida per la propria legislazione nazionale, è corretto affermare che esserne parte comporta una serie di vantaggi, tra i quali il principale è quello di essere base regolatrice per la cooperazione internazionale, in quanto la Convenzione non è esclusivamente europea, ma è sottoscritta anche da Stati non membri del Consiglio d'Europa, il che le consente di accogliere concetti giuridici non europei e di conseguenza semplificare l'adesione successiva di altri Paesi. Attualmente gli Stati firmatari della Convenzione sono 68, di cui 65 hanno proceduto alla ratifica, tra questi gli appartenenti al consiglio d'Europa sono 47.

L'obiettivo primario della Convenzione di Budapest è dato dall'esigenza di introdurre un livello minimo di tutela dei beni giuridici offesi dai cybercrimes e di strategie di contrasto a tali illeciti, soprattutto in ragione della loro natura tendenzialmente transnazionale, che comporta chiaramente la necessità dell'armonizzazione della relativa normativa di contrasto nell'ambito dei vari ordinamenti[14]. Tra le molteplici finalità della Convenzione vi è quella di agire come deterrente per le azioni dirette contro la segretezza, l'integrità e la disponibilità dei sistemi informatici, delle reti e dei dati informatici, così come per l'uso improprio di questi sistemi; in secondo luogo, mediante rinvio alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, spesso indicata semplicemente con l'acronimo CEDU, ha come scopo ulteriore la necessità di creare un livello di bilanciamento soddisfacente tra norme statali restrittive dell'accesso a Internet, da un lato, e il rispetto dei diritti fondamentali, dall'altro[15]. Un'ulteriore finalità della

[13] European Treaty Series - No. 189, *Protocollo addizionale alla Convenzione sulla criminalità informatica, relativo alla qualifica come reato degli atti di natura razzista e xenofoba commessi attraverso sistemi informatici*.

[14] Consiglio d'Europa, *The Budapest Convention on Cybercrime: benefits and impact in practice*, Strasburgo, 2020.

[15] Preambolo della Convenzione del Consiglio d'Europa sulla repressione della criminalità informatica, 2001, p. 3.

Convenzione è quella di favorire il processo di armonizzazione del diritto penale nazionale e dei codici di rito in materia di reati commessi via Internet, la quale appare indispensabile in virtù del fatto che un controllo statale è reso particolarmente difficile, se non quasi impossibile, a causa della presenza di attori globali. Tale processo risulta dunque di fondamentale importanza soprattutto per evitare la formazione di cosiddetti rifugi sicuri, legati al principio di doppia incriminazione, in cui se la condotta non è criminalizzata in un determinato Paese, le persone in quel Paese possono agire, senza essere incriminate, nel commettere reati che interessino altre giurisdizioni, comportando numerosi ostacoli nella raccolta ad esempio delle prove informatiche, dato che tali condotte illecite sarebbero commesse in un Paese che non le considera integranti di una fattispecie di reato. Un ulteriore aspetto favorevole è quello di fungere da strumento fondamentale nel favorire un'efficace cooperazione tra le forze dell'ordine e autorità giudiziarie degli Stati coinvolti nel perseguimento dei crimini.

La Convenzione è costituita da 48 articoli e l'obiettivo di uniformare la disciplina interna degli Stati nella lotta ai Cybercrimes emerge sin dall'articolo 1, il quale mira a diffondere nozioni comuni tra gli Stati aderenti alla Convenzione[16]. In ragione di quanto appena scritto, posso affermare con assoluta certezza che tale Convenzione rappresenti uno dei mezzi, se non proprio il mezzo più funzionale, per coadiuvare i diversi Stati nell'adozione di una normativa il più possibile uniforme, fornendo loro un quadro normativo esaustivo per quanto riguarda le diverse questioni di diritto sostanziale, processuale e di cooperazione internazionale.

Il secondo capitolo della Convenzione è suddiviso in due sezioni. La prima si occupa di *Diritto Penale Sostanziale* e contiene un elenco delle diverse fattispecie di crimini informatici, con l'obiettivo di imporre agli Stati aderenti alla Convenzione l'adozione di

[16] Convenzione di Budapest, art. 1: "Ai fini della presente Convenzione:
a. "sistema informatico" indica qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati;
b. "dati informatici " indica qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di con sentire ad un sistema computerizzato di svolgere una funzione;
c. "service provider" (fornitore di servizi), indica:
1. qualunque entità pubblica o privata che fornisce agli utenti dei propri servizi la possibilità di comunicare attraverso un sistema informatico;
2. qualunque altra entità che processa o archivia dati informatici per conto di tale servizio di comunicazione o per utenti di tale servizio;
d. "trasmissione di dati" indica qualsiasi informazione computerizzata relativa ad una comunica zione attraverso un sistema informatico che costituisce una parte nella catena di comunicazione, indicando l'origine della comunicazione, la destinazione, il percorso, il tempo, la data, la grandezza, la durata o il tipo del servizio".

specifiche norme di diritto penale sostanziale[17]. L'introduzione di reati armonizzati si rifà ad un preciso obiettivo già anticipato in precedenza, ossia all'eliminazione dei problemi di doppia incriminazione e a migliorare i mezzi per prevenire e reprimere la criminalità informatica. Sulla base della Raccomandazione n° 9 del 1989 del Consiglio d'Europa sulla criminalità informatica, la Convenzione classifica i crimini informatici in quattro categorie:

- *Reati contro la riservatezza, l'integrità e la disponibilità di dati e sistemi informatici.*
- *Reati informatici.*
- *Reati relativi al contenuto.*
- *Reati contro la proprietà intellettuale e diritti collegati.*

Le disposizioni della Convenzione non si applicano soltanto ai *reati cibernetici in senso proprio*, ossia a quei reati che sono commessi solo attraverso la tecnologia, ma si applicano anche a tutti i *reati cibernetici in senso improprio*, dove la condotta illecita può essere commessa attraverso un sistema informatico, ma anche tutti i reati comuni che potrebbero commettersi senza l'uso di tecnologie, per i quali si richiede la raccolta di prove in forma elettronica. Un'ulteriore aspetto che caratterizza la Convenzione, consiste nel fatto che per la maggior parte delle fattispecie criminose è prevista dall'articolo 11 la repressione del tentativo, ai sensi del quale gli Stati aderenti devono definire, nelle proprie legislazioni interne, come reato "*il tentativo di commettere ogni tipo di reato in base agli articoli da 3 a 5, 7, 8, 9.1 a. e c. della presente Convenzione*"[18]. Lo stesso articolo 11, prevede la punibilità anche a titolo di concorso, purché vi sia rispettato il requisito dell'intenzionalità di concorrere alla commissione di una fattispecie di reato. L'articolo 12 disciplina le diverse forme di responsabilità civile, penale e amministrativa, mentre l'articolo 13 dispone che le sanzioni da adottare dagli Stati aderenti devono essere effettive, proporzionate e dissuasive e, nel caso siano disposte nei confronti di persone fisiche, potranno consistere anche nella pena detentiva. Gli elementi costitutivi richiesti delle diverse fattispecie criminose elencate nella Convenzione, sono da un punto di vista oggettivo la mancanza di diritto, mentre da un punto di vista soggettivo, l'intenzionalità.

[17] M. Arena, *La Convenzione di Budapest del Consiglio d'Europa sulla repressione della criminalità informatica*, Catania, CRIO Papers, 2021, p. 12.
[18] Convenzione di Budapest, art. 11, par. 2: "Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commesso volontariamente, il tentativo di commettere ogni tipo di reato in base agli articoli da 3 a 5, 7,8,9.1 a. e c. della presente Convenzione".

Per quanto riguarda la mancanza di diritto, va intesa come la violazione di regole giuridiche extrapenali, per le quali non è presente una causa di giustificazione. Il requisito dell'intenzionalità è strettamente correlato al diritto penale, ed esige che il fatto sia commesso con dolo oppure in alcuni casi è richiesta un'intenzione specifica, che nel nostro ordinamento viene correlata al dolo specifico, ad esempio in materia di frode informatica, l'articolo 8 della Convenzione prevede come elemento costitutivo della fattispecie, il fine di procurare un vantaggio economico[19].

Nella categoria dei reati contro la riservatezza, integrità e disponibilità di dati e sistemi informatici, sono collocati quei reati la cui illiceità è collegata all'ambiente informatico in cui vengono commessi. L'articolo 2 disciplina l'*accesso illegale*[20] e punisce chiunque senza autorizzazione e intenzionalmente accede ad un sistema informatico; gli elementi costitutivi di questa fattispecie sono il dolo e l'abusività dell'azione, mentre il fine illecito rappresenta un elemento ulteriore, non fondamentale. L'*intercettazione illegale*[21] trova disciplina nell'articolo 3 della Convenzione e, ha come obiettivo la tutela del diritto alla riservatezza dei dati informatici durante la loro trasmissione; i due elementi costitutivi sono l'assenza di autorizzazione e l'intenzionalità. La Convenzione disciplina le due fattispecie di *attentato all'integrità dei dati e dei sistemi*, rispettivamente agli articolo 4 e 5. Con la prima, vengono punite condotte di danneggiamento, cancellazione, deterioramento, modifica o soppressione di dati informatici e gli elementi costitutivi di tale fattispecie sono i medesimi previsti per l'intercettazione illegale. L'articolo 5 incrimina le stesse condotte dettate dall'articolo 4; tuttavia, non ha ad oggetto il semplice dato, bensì l'intero sistema informatico e, per la configurazione del reato è richiesto che

[19] Convenzione di Budapest, art. 8: "Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commesso intenzionalmente e senza alcun diritto, il cagionare un danno patrimoniale ad altra persona: a. con ogni introduzione, alterazione, cancellazione o soppressione di dati informatici; b. con ogni interferenza nel funzionamento di un sistema informatico, con l'intento fraudolento o illegale di procurare, senza alcun diritto, un beneficio economico per se stesso o altri".

[20] Convenzione di Budapest, art. 2: "Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per sanzionare come reato in base alla propria legge nazionale l'accesso all'intero sistema informatico o a parte di esso senza autorizzazione. Una Parte può richiedere che il reato venga commesso violando misure di sicurezza con l'intenzione di ottenere informazioni all'interno di un computer o con altro intento illegale o in relazione ad un sistema informatico che è connesso ad un al tro sistema informatico".

[21] Convenzione di Budapest, art. 3: "Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale l'intercettazione senza autorizzazione, fatta con strumenti tecnici, di trasmissioni non pubbliche di dati informatici a, da o all'interno di un sistema informatico, incluse le emissioni elettromagnetiche da un sistema informatico che ha tali dati informatici. Una Parte può richiedere che il reato venga commesso con intento illegale o in relazione ad un sistema informatico che è connesso ad un altro sistema informatico".

la condotta illecita costituisca un ostacolo al funzionamento del sistema. Secondo quanto previsto dall'articolo 5 della Convenzione, ogni Stato deve definire, in base alla propria legge nazionale, quando un impedimento può essere considerato di una serietà tale da integrare una fattispecie di reato.

La categoria dei reati informatici comprende la *falsificazione informatica* e la *frode informatica*. Essi non rappresentano altro che la trasposizione tecnologica dei tradizionali reati di truffa e falsificazione di documenti, perpetrati nel mondo fisico. In particolare, l'articolo 7 della Convenzione definisce la falsificazione informatica come "*una serie di condotte, di alterazione, introduzione, possesso o soppressione di dati, poste in essere con l'intenzione di creare dati non autentici e di utilizzarli o considerarli come se fossero autentici ai fini legali*"[22]. I dati informatici ai quali fa riferimento la disposizione sono quelli che hanno un contenuto probatorio, sia in ambito pubblico che privato, mentre l'interesse protetto è la genuinità delle prove e la sicurezza dei dati elettronici. Ai fini penalistici, per l'insorgere della responsabilità, può essere richiesto l'intento fraudolento nella commissione del fatto. L'articolo 8 disciplina due diverse tipologie di condotta correlate alla frode informatica: la manipolazione dei dati digitali e l'interferenza nel funzionamento di un sistema informatico e, come conseguenza di tale condotte illecite ci sarebbe un danno patrimoniale ad altri, dovuto al fatto di voler ottenere illecitamente un vantaggio economico, per sé o per altri[23].

L'articolo 9 della Convenzione dispone per i reati relativi al contenuto, tra i quali rientra la pornografia infantile. Tale ambito, attraverso il protocollo aggiuntivo di Strasburgo 2003, è stato esteso anche alle condotte di natura xenofoba e razzista commesse mediante sistemi informatici. La Direttiva 2011/92/UE, del 13 dicembre 2011, adottata dal Parlamento Europeo e dal Consiglio e, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, indica come: "*l'abuso e lo sfruttamento sessuale dei minori, compresa la pornografia minorile, costituiscono gravi violazioni dei diritti fondamentali, in particolare del diritto dei minori alla protezione e alle cure*

[22] M. Arena, *La Convenzione di Budapest del Consiglio d'Europa sulla repressione della criminalità informatica*, Catania, CRIO Papers, 2021, p. 20.

[23] Convenzione di Budapest, art. 8: "Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commesso intenzionalmente e senza alcun diritto, il cagionare un danno patrimoniale ad altra persona: a. con ogni introduzione, alte razione, cancellazione o soppressione di dati informatici; b. con ogni interferenza nel funziona mento di un sistema informatico, con l'intento fraudolento o illegale di procurare, senza alcun di ritto, un beneficio economico per se stesso o altri".

necessarie per il loro benessere, come sancito nella Convenzione delle Nazioni Unite sui diritti del fanciullo del 1989 e nella Carta dei diritti fondamentali dell'Unione europea dall'articolo 34". Attraverso tale Direttiva, il legislatore europeo ha voluto definire in maniera chiara e precisa, cosa si intende con pornografia minorile, eliminando qualsivoglia interpretazione: "*La pornografia minorile comprende spesso la registrazione di abusi sessuali compiuti sui minori da parte di adulti. Essa può anche comprendere immagini di minori coinvolti in atteggiamenti sessuali espliciti o immagini dei loro organi sessuali, ove tali immagini siano prodotte o utilizzate per scopi prevalentemente sessuali, indipendentemente dal fatto che siano utilizzate con la consapevolezza del minore. Inoltre, il concetto di pornografia minorile comprende altresì immagini realistiche di un minore in atteggiamenti sessuali espliciti o ritratto in atteggiamenti sessuali espliciti, per scopi prevalentemente sessuali*"[24].

Come nel caso dell'articolo 8 del GDPR, relativo alle "*Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione*", anche l'articolo 9 della Convenzione di Budapest, seppur con parametri diversi, stabilisce l'età per cui un soggetto è da qualificarsi come minore. Nel paragrafo 3 è definito minore, il soggetto che non ha compiuto i 18 anni di età; tuttavia, le parti possono stabilire un'età inferiore , con il limite minimo posto a 16 anni di età.

La pornografia minorile, secondo quanto indicato nel paragrafo 2 dell'articolo 9, comprende il materiale pornografico che raffigura, rispettivamente alle seguenti lettere:

a) *un minore coinvolto in un comportamento sessuale esplicito*;
b) *un soggetto che sembra essere un minore coinvolto in un comportamento sessuale esplicito*;
c) *immagini realistiche raffiguranti un minore coinvolto in un comportamento sessuale esplicito*.

Le condotte per essere incriminate devono essere commesse senza diritto e intenzionalmente. Alcune di queste sono incriminate obbligatoriamente anche a titolo di tentativo, tra queste rientrano quelle indicate alle lettere a ("*la produzione di pornografia minorile in vista della sua diffusione tramite un sistema informatico*") e c ("*la diffusione o la trasmissione di pornografia minorile tramite un sistema informatico*") del paragrafo

[24] M. Arena, *La Convenzione di Budapest del Consiglio d'Europa sulla repressione della criminalità informatica*, Catania, CRIO Papers, 2021, p. 22.

1, mentre le condotte indicate nelle lettere b ("*offerta o messa a disposizione di pornografia minorile tramite un sistema informatico*"), d ("*procurarsi o procurare ad altri pornografia minorile tramite un sistema informatico*") ed e ("*possedere pornografia minorile in un sistema informatico o in un mezzo di memorizzazione di dati informatici*") dello stesso paragrafo, non ammettono l'incriminazione a titolo di tentativo.

I reati contro la proprietà intellettuale e diritti collegati comprendono le fattispecie di *violazione del diritto d'autore e diritti connessi*, le quali sono disciplinate nella Convenzione, con rinvio al diritto interno di ogni singolo Stato aderente, dall'articolo 10. Seconda la norma le violazioni devono essere dolose e le sanzioni penali devono intervenire in contrasto alle violazioni di carattere commerciale.

La Convenzione non si limita alle sole questioni di diritto penale sostanziale, ma anche a quelle di carattere procedurale, di cui parlerò nel secondo capitolo, inerenti ai principi processuali generali, agli strumenti di indagine convenzionali e alla cooperazione. Tuttavia, prima di affrontare l'argomento successivo, relativo alla legge 48 del 2008, vorrei soffermarmi brevemente, sul fare una disamina finale della Convenzione di Budapest.

La Convenzione ha rappresentato e rappresenta ancora oggi, uno strumento guida per ciascuno Stato aderente nell'adottare una legislazione esaustiva a contrasto della criminalità informatica, grazie alle misure di diritto sostanziale, già definite in precedenza, e a quelle di diritto processuale, di cui parlerò nel successivo capitolo. L'armonizzazione flessibile rappresenta sicuramente un aspetto positivo, in quanto la libertà garantita agli Stati nell'elaborazione del diritto interno, nonostante non sia assoluta ma nel rispetto di certi standard minimi, favorisce la cooperazione giudiziaria, eliminando uno degli ostacoli più difficili da oltrepassare, ossia la doppia incriminazione. Inevitabilmente è sorta la necessità di bilanciare le attività di repressione della criminalità informatica, da un lato, e la tutela della privacy, dall'altro. Per tale ragione, e per le numerose critiche sollevate a riguardo, nel 2017, presso il Consiglio d'Europa, sono iniziati i lavori preparatori per l'introduzione di un secondo protocollo aggiuntivo alla Convenzione, il quale è stato ratificato nel maggio 2022, in materia di cooperazione internazionale rafforzata e accesso alle prove nel cloud. Gli elementi chiave di questo secondo protocollo riguardano le misure per l'assistenza giudiziaria reciproca, per la cooperazione tra autorità e fornitori di servizi di altri Paesi, ma soprattutto specificano

una serie di condizioni e garanzie per l'accesso alle informazioni da parte delle autorità di altri Paesi, comprendendo tra queste anche degli standard minimi di protezione dei dati.

5. La Legge 48 del 2008 di recepimento della Convenzione di Budapest

La legge n.48 del 18 marzo 2008, ratifica ed esegue in Italia la Convenzione del Consiglio d'Europa sulla Criminalità informatica del 23 novembre 2001, nota semplicemente come Convenzione di Budapest[25]. L'obiettivo principale della legge 48/2008, secondo l'articolo 2, è quello di dare "piena ed intera esecuzione" alla Convenzione; lo stesso articolo afferma che gli effetti di diritto internazionale si produrranno soltanto a partire dal 1° ottobre 2008, vale a dire dal primo giorno del mese successivo al termine di cui all'art. 36 della Convenzione. Mi occorre sottolineare come tale legge non sia il primo intervento normativo sulla criminalità informatica; infatti, le particolari esigenze investigative dovute alla diffusione capillare degli strumenti telematici e informatici in tutti diversi ambiti della vita, avevano già ricevuto un precedente intervento normativo attraverso la legge 547/1993 "*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*", la quale aveva introdotto in precedenza diverse nuove fattispecie criminose, inoltre aveva affrontato il tema della necessità di adeguamento degli strumenti d'indagine.

La legge 48/2008 ha in primo luogo consentito all'Italia di adempiere agli obblighi assunti sette anni prima attraverso la sottoscrizione della Convenzione di Budapest; infatti, tale intervento legislativo italiano ha introdotto diverse novità di particolare importanza, sotto l'aspetto penale ad esempio, ha portato a numerose modifiche alle norme penali, processuali e sostanziali, con il fine di adeguarsi alle disposizioni della Convenzione, ma anche alle nuove forme di criminalità informatica[26]. L'ambito principale sul quale la legge è intervenuta riguarda l'introduzione di nuovi strumenti di indagine per le forze dell'ordine. Le modifiche apportate al codice di rito hanno interessato in particolare i mezzi di ricerca della prova e le indagini della polizia giudiziaria (PG), disciplinando le modalità di esecuzione di sequestri, ispezioni e perquisizioni relativi a materiale informatico. L'obiettivo principale dettato dalle legge n. 48/2008 attraverso la previsione di una serie di regole di conservazione, riguarda l'intangibilità dei dati originali e la

[25] Legge 18 marzo 2008, No. 48, art. 1: "Il Presidente della Repubblica è autorizzato a ratificare la Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, di seguito denominata "Convenzione" ".
[26] M. Arena, *Il recepimento in Italia della Convenzione di Budapest. La legge 18 marzo 2008 n. 48,* Fogli di Lavoro per il Diritto Internazionale, 2021, p. 3.

conformità delle copie durante un processo penale, ossia di tutte quelle attività relative alla *digital forensics*, la cui definizione consisterebbe nell'insieme delle attività volte 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[27].

La legge 48/2008, oltre alle diverse modifiche sul piano penale, ha introdotto tutele maggiori per la protezione dei dati personali. Essa si compone di 14 articoli, suddivisi in 4 capi:

- Il capo I, intitolato "*Ratifica ed esecuzione*", contiene i primi due articoli.
- Il capo II, intitolato "*Modifiche al Codice penale e al decreto legislativo 8 giugno 2001, n. 231*", contiene gli artt. 3-7.
- Il capo III, intitolato "*Modifiche al Codice di procedura penale e al Codice di cui al decreto legislativo 30 giugno 2003, n. 196*", contiene gli artt. 8-12.
- Il capo IV, intitolato "*Disposizioni finali*", contiene gli artt. 13 e 14.

Dall'analisi del capo III, sul quale intendo focalizzarmi, si può comprendere come il legislatore italiano si sia limitato, nell'introdurre i nuovi principi per l'assunzione delle prove informatiche, a definire il risultato finale, piuttosto che le modalità di esecuzione da attuare concretamente nell'impiego dei diversi mezzi di ricerca della prova, al fine di raggiungerlo. Il legislatore ha circoscritto la sua area di intervento, attraverso operazioni di cosiddetta chirurgia lessicale, nell'adeguare le disposizioni processuali già vigenti attraverso gli artt. 8,9 e 11, inserendo espressioni che rimandano ad attività connesse a dati, informazioni e programmi informatici. Questa volontà del legislatore la si vince anche dalla Relazione al Progetto di legge, le novelle in materia processuale "*consistono in un adeguamento prevalentemente lessicale delle disposizioni processuali già vigenti, finalizzato a rendere esplicite le potenzialità applicative in campo informatico, che già oggi, peraltro, dottrina e giurisprudenza riconoscono agli istituti procedurali che ne sono interessati*"[28]. Non esistono dunque grandi novità apportate dall'intervento del legislatore, se non l'unica prevista dall'articolo 10 relativa alla procedura di *conservazione rapida dei dati*, cosiddetto *freezing*, e apportata attraverso l'aggiunta di commi all'articolo 132 del Codice della privacy, ossia del Decreto legislativo n. 196/2003. Il legislatore è

[27] E. Casey, Digital evidence and Computer Crime. 3ª Edizione, Elsevier Science Publishing, 2011, p. 7.
[28] A. Vitale, La nuova disciplina delle ispezioni e perquisizioni in ambiente informatico o tele matico, *Diritto dell'internet*, Milano, Wolters Kluwer Italia S.r.l., 2008.

intervenuto poi, sul titolo III del libro III, relativo ai mezzi di ricerca della prova[29], e sul titolo IV e V, dedicato alle indagini su iniziativa della polizia giudiziaria.

Tale sistema creatosi con l'introduzione della legge n. 48/2008, in perfetta armonia con quanto disciplinato dalla Convenzione di Budapest, non si limita ai soli crimini informatici, ma trova applicazione con riferimento a qualsiasi tipologia di reato. Il legislatore è inoltre intervenuto sull'impianto codicistico originario, mediante l'introduzione di una disciplina ad hoc relativa al trattamento delle prove digitali. Tale disciplina ruota attorno al *dovere di non alterare il dato originale*, ciò significa che le tecniche utilizzate per gestire gli elementi digitali devono essere in grado di lasciare inalterato l'originale, sia nella fase di acquisizione, che nella fase successiva di conservazione[30].

[29] C. Maioli – E. Sanguedolce, *I nuovi mezzi di ricerca della prova fra informatica forense e L. 48/2008*, articolo presente in www.altalex.com, pubblicato il 7 maggio 2012.
[30] M. Arena, *Il recepimento in Italia della Convenzione di Budapest. La legge 18 marzo 2008 n. 48,* Fogli di Lavoro per il Diritto Internazionale, 2021, p. 9.

CAPITOLO II

L'ACQUISIZIONE FORENSE DELLE PROVE DIGITALI

Sommario: 1. Le indagini preliminari ad oggetto informatico. – 2. La fragilità delle prove digitali. – 3. Attività ripetibili e irripetibili (Il principio del male captum bene retentum). – 4. Le sentenze della Cassazione a sostegno della ripetibilità.

1. Le indagini preliminari ad oggetto informatico

Il sistema di diritto processuale penale odierno prevede che il procedimento di formazione della prova si componga delle quattro fasi seguenti: la ricerca, l'individuazione, l'acquisizione e infine la valutazione della prova. Sono *mezzi di ricerca della* prova quelli che il codice di procedura penale disciplina nel libro terzo al titolo terzo, ossia quegli atti di indagine che non costituiscono di per sé fonte di convincimento, ma che rendono possibile l'acquisizione di cose materiali, tracce o dichiarazioni dotate di attitudine probatoria; rientrano in questa categoria: le ispezioni, le perquisizioni, i sequestri e le intercettazioni di conversazioni e di comunicazioni[31]. I *mezzi di prova* sono invece quelli disciplinati dallo stesso Codice di procedura penale negli artt. 194-243, presenti nel titolo secondo del libro terzo, i quali hanno l'attitudine ad offrire al giudice, nella fase di valutazione, risultanze probatorie direttamente utilizzabili in sede di decisione. Sono mezzi di prova: la testimonianza, le perizie, gli esperimenti giudiziali e i documenti[32].

Le caratteristiche principali delle indagini preliminari ad oggetto informatico, cosiddette indagini digitali, che le contraddistinguono da quelle tradizionali, sono l'immaterialità, la transnazionalità, e la necessaria cooperazione con soggetti terzi[33].

Per quanto riguarda l'*immaterialità* delle indagini digitali[34], ha costituito per un lungo periodo un ostacolo rispetto a quanto previsto dal codice del 1988, secondo il quale le indagini erano fondate sulla materialità degli elementi di prova, fatta eccezione per le intercettazioni, di conseguenza si è assistito per lungo tempo ad una sovrapposizione concettuale del contenitore sul contenuto, confondendo il supporto con i dati in esso memorizzati. Ciò comportava ad esempio il sequestro del pc, anziché dei soli dati in esso contenuti. In prima battuta si è cercato di introdurre nuove norme per adattare gli istituti tradizionali alle nuove tipologie investigative, ma ci si accorse della necessità di elaborare istituti non più basati sulla materialità e che tenessero conto delle caratteristiche dei dati

[31] S. Pietropaoli., *Informatica criminale. Diritto e sicurezza nell'era digitale*. Giappichelli, 2022, pag. 89.
[32] Prova. Diritto processuale penale in "Enciclopedia on line Treccani".
[33] S. Signorato, *Le indagini digitali: profili strutturali di una metamorfosi investigativa*, Torino, Giappichelli, 2018.
[34] M. Pittiruti, *Digital evidence e procedimento penale*. Giappichelli, 2018, pag. 7.

digitali, ossia la loro facile alterazione ed eliminazione, prevedendo misure adeguate a preservarli, non solo nel momento acquisitivo, ma anche in quelli precedenti e successivi ad esso.

Il secondo aspetto che caratterizza le indagini digitali è la *transnazionalità*. La giurisdizione italiana presenta una forte vocazione espansiva, poiché tende ad applicare la propria legge penale anche in rapporto a reati che presentino elementi di transnazionalità; tuttavia, ad essa si contrappone un approccio di tipo territoriale in sede investigativa. Questo significa che le acquisizioni oltre confine delle fonti di prova richiedono di regola l'attivazione degli strumenti della cooperazione giudiziaria e di polizia tra gli Stati. La cooperazione giudiziaria è molto importante per le indagini digitali, in quanto spesso l'acquisizione riguarda elementi contenuti in un dispositivo informatico che sia ubicato all'estero, sia quando essi si trovino in server ubicati in territorio straniero. Un altro aspetto da considerare riguarda il fatto che la tecnologia rende infatti possibile una scissione tra il luogo in cui si trovano gli elementi probatori e il luogo dal quale possono essere acquisiti.

Il terzo e ultimo aspetto che caratterizza le indagini digitali è la necessaria *cooperazione con soggetti terzi* rispetto all'autorità giudiziaria o di polizia[35]. Sono soggetti terzi: i *Computer Security Incident Response Team*, noti con l'acronimo CSIRT, i quali hanno funzioni preventive e repressive. Si tratta di gruppi di esperti per la sicurezza informatica che mirano a contrastare e a prevenire incidenti informatici, sia di origine tecnica sia delittuosa. Inoltre, possono aiutare la polizia giudiziaria ad elaborare misure tecniche preventive più adeguate. Tra i soggetti terzi i vi rientrano anche gli *Internet Service Provider,* o ISP, ossia gli operatori dei servizi di telecomunicazione, coloro che forniscono o gestiscono servizi di telefonia o servizi internet. Con il termine *data retention* ci si riferisce a quell'obbligo che il legislstore ha previsto in capo agli ISP di conservare i dati relativi al traffico telefonico e telematico in loro possesso, la cui disciplina è contenuta nell'articolo 132 del Codice della privacy, modificato dalla legge 48/2008 di ratifica della Convenzione di Budapest, in base al quale il fornitore deve mantenere i dati relativi al traffico telefonico, telematico e delle chiamate senza risposta per finalità di accertamento e repressione dei reati[36]. La norma fissa la durata temporale di conservazione a seconda della tipologia di dati: 24 mesi dalla data di comunicazione per i dati relativi al traffico

[35] M. Pittiruti, *Digital evidence e procedimento penale*. Giappichelli, 2018, pag. 52-57.
[36] S. Aterno - F. Cajani - G. Costabile, *Cyber forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*. Giappichelli, 2021, pag. 289.

telefonico, 12 mesi dalla data della comunicazione per i dati relativi al traffico telematico, e 30 giorni per i dati relativi alle chiamate senza risposta[37]. Ciò causa problemi nella distinzione tra telefonico e telematico , ad esempio in riferimento alle chiamate effettuate attraverso whatsapp, e ulteriori criticità sul valore giuridico effettivo attribuito a tali dati, in quanto ad esempio la chiamata senza risposta potrebbe valere molto in caso di stalking. Secondo un mio personale punto di vista, sembra auspicabile una modifica di tale disciplina omologando i termini di conservazione dei dati telefonici e di quelli telematici. La data retention presenta ulteriori aspetti problematici, da un lato legati alla stessa vigenza dell'articolo 132, che secondo alcuni andrebbe disapplicato, in quanto prescriverebbe a sua volta una disciplina sproporzionata, secondo quanto dichiarato anche dalla Corte di Giustizia nel 2014, e dall'altro lato legati ad uno squilibrio, tra i termini previsti dall'articolo 132 e quelli previsti dall'articolo 4 bis del d.l. 7/2015 della normativa in tema di contrasto al terrorismo, in base al quale il fornitore non conoscendo il motivo per cui custodisce i dati, tenderà a rispettare la disciplina che preveda di volta in volta la durata massima, ossia di 72 mesi, comportando una serie di problemi di violazione della privacy[38].

Un'ulteriore categoria di soggetti terzi è rappresentata dai i fornitori ed i gestori di servizi cloud. Nell'ambito del cloud la visualizzazione dei dati è di regola protetta da codici di accesso, con la conseguenza che, se gli investigatori non dispongono dei medesimi dovranno necessariamente chiederli ai fornitori del servizio. Tale necessità comporta diversi ostacoli, da un lato legati alla difficoltà nell'individuare il soggetto giuridico a cui rivolgere la richiesta, in quanto i servizi cloud sono costruiti a scatole cinesi, e dall'altro lato dovuti alla tecnologia impiegata dal cloud definita load balancing o ridondanza, la quale rende assai difficoltoso rintracciare i dati a tal punto che nemmeno il fornitore del servizio è a conoscenza del luogo in cui si trovano i dati, poiché questi si spostano in automatico. Andrebbe quindi operato un mutamento di paradigma, non riferendosi più al luogo in cui si trova il server, ma, ad esempio, al luogo in cui il fornitore del cloud ha la propria sede legale, o il luogo in cui si fruisce del servizio cloud.

Evidenziate quelle che sono le principali caratteristiche delle indagini digitali, vorrei proseguire nel paragrafo successivo con l'analisi di un'ulteriore aspetto, non meno rilevante dei precedenti, che contraddistingue le prove digitali, ossia la loro fragilità.

---

[37] S. Aterno - F. Cajani - G. Costabile, *Cyber forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*. Giappichelli, 2021, pag. 300.

[38] M. Pittiruti, *Digital evidence e procedimento penale*. Giappichelli, 2018, pag. 122-133.

2. La fragilità delle prove digitali

I dati digitali sono facilmente alterabili ed eliminabili, per questo motivo occorre preservarli, non solo nel momento acquisitivo, ma anche in quelli precedenti e successivi ad esso. La legge n. 48/2008 ha recepito la Convenzione di Budapest e, come già indicato in precedenza, ha sottolineato l'importanza dell'impiego di standard operating procedure, note anche come *best practices*, le quali sono attualmente riconosciute a livello internazionale[39]. L'articolo 244 c.p.p. che disciplina l'ispezione, e gli articoli 247 e 352 c.p.p. che disciplinano la perquisizione, precisano che l'attività investigativa debba svolgersi adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. Da queste disposizioni si riconosce un più generale principio che impone di garantire l'integrità dei dati digitali in ogni frangente, che tra l'altro è possibile ritrovare nell'articolo 326 c.p.p, ma anche nell'articolo 358 c.p.p. che introduce il principio di completezza delle indagini, in base al quale un'indagine è completa se l'acquisizione degli elementi di prova avviene in modo corretto. La legge n. 48/2008 riconosce la preservazione dell'integrità dei dati come principio guida delle indagini informatiche[40].

La computer forensics ha ad oggetto lo studio dell'attività di ricerca, di analisi e di conservazione dei dati digitali nel quadro di un procedimento penale. Esistono diversi tipi di forensics, tra cui ad esempio la mobile forensics e la network forensics, ma in generale possiamo parlare di *digital forensics*. Le tecniche inerenti a quest'ultima nascono nel mondo angloamericano, dunque in un sistema di common law diverso dal nostro, il che determina alcuni problemi di fondo, ad esempio legati al principio di separazione delle fasi e al sistema del doppio fascicolo di cui parlerò all'inizio del capitolo successivo. Inoltre, all'interno delle digital forensics si sono sviluppati approcci diversi che hanno portato all'elaborazione di modelli e protocolli differenziati che possono giungere a risultati non coincidenti. Un esempio è dato dalla *ISO/IEC 27037,* la quale fornisce linee guida per attività specifiche nella gestione delle prove digitali, che sono l'identificazione, la raccolta, l'acquisizione e la conservazione di potenziali prove digitali che possono avere valore probatorio[41]; esse rappresentano uno standard creato dall'*International Organisation for Standardization*, o ISO, la quale individua delle norme tecniche in

[39] S. Aterno - F. Cajani - G. Costabile, *Cyber forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*. Giappichelli, 2021, pag. 13-16.
[40] M. Pittiruti, *Digital evidence e procedimento penale*. Giappichelli, 2018, pag. 100-102.
[41] ISO/IEC 27037:2012, scopo principale preso dall'abstract in https://www.iso.org/standard/44381.html.

materia di digital forensics, ma essendo tale organizzazione non governativa, gli standard da lei creati non sono vincolanti per gli Stati anche se tendenzialmente sono recepiti.
Sull'inosservanza delle best practices non esiste una visione univoca, ma anzi ne esistono molteplici che si sono formulate nel corso degli anni, anche se mi occorre evidenziare, come tra l'altro fra poco spiegherò più nel dettaglio, che molte opinioni risultano inapplicabili in quanto contrarie ad alcune disposizione del nostro codice di rito.
Secondo una prima visione, dall'inosservanza o il mancato impiego delle best practices per ispezioni o perquisizioni, per le quali si prevede espressamente l'adozione di misure tecniche volte ad assicurare la conservazione dei dati originari e ad impedirne l'alterazione, ne deriverebbe la nullità, ex articolo 178 c.p.p. . Tale impostazione tutela la custodia dei dati digitali, ma si scontra con il principio di tassatività della nullità ex articolo 177 c.p.p., in base al quale l'inosservanza delle best practices non appare vincolante e causa di nullità.
Secondo una seconda impostazione, il mancato impiego di best practices comporterebbe l'inutilizzabilità dei dati acquisiti, tuttavia anche questa ipotesi andrebbe respinta perché manca una specifica previsione che sancisca un divieto probatorio.
Infine la terza visione, accettata dalla giurisprudenza, afferma che dal mancato impiego di best practices non potrebbe derivare un'invalidità. Piuttosto l'inosservanza potrebbe incidere sull'affidabilità del dato probatorio e dunque influenzare la valutazione di quel dato da parte del giudice[42].
Per quanto riguarda la fragilità delle prove digitali e ancora prima dei dati da cui si ricavano, mi sembra opportuno richiamare alcuni esempi chiarificatori su tale aspetto. In relazione alle attività di indagine su dispositivi informatici, posso distinguere la post mortem forensics e la live forensics; la prima riguarda le indagini effettuate su dispositivi spenti, laddove tale atto è considerato ripetibile, mentre la live forensics viene impiegata per svolgere indagini che riguardano dispositivi accesi[43]. L'accensione o lo spegnimento rappresentano l'emblema di quanto siano facilmente modificabili i dati e soprattutto i metadati contenuti in un dispositivo, che ai fini processuali possono assumere a secondo del caso un'importanza fondamentale. È opportuno che il dispositivo sia analizzato e da esso sia eventualmente estratta una copia dei dati, nelle medesime condizioni nelle quali lo si ritrova per evitarne l'alterazione. Un altro aspetto da tenere in considerazione è

[42] S. Signorato, *Le indagini digitali: profili strutturali di una metamorfosi investigativa*, Torino, Giappichelli, 2018.
[43] M. Pittiruti, *Digital evidence e procedimento penale*. Giappichelli, 2018, pag. 93-94.

costituito dalla mancata cura o competenza nel maneggiare certi dispositivi, il che crea un forte rischio di rendere illeggibili i dati contenuti al loro interno. In conclusione posso evidenziare quelli che sono i caratteri, oltre a quelli che ho appena citato, che hanno spinto la Convenzione di Budapest prima, e la legge n. 48/2008 poi, ad appoggiare la tesi che sostiene l'irripetibilità dell'accertamento tecnico in relazione al rischio concreto di alterare lo stato dei dati digitali: l'alterazione della timeline, l'alta probabilità di alterare in via accidentale i file, il rischio di perdita di mezzi di prova e di malfunzionamento[44].

3. Attività ripetibili e irripetibili (Il principio del male captum bene retentum)

Nelle indagini tradizionali la perquisizione precede di regola il sequestro, tanto che si riteneva che vi fosse un nesso di logica consequenzialità tra questi due atti investigativi. Nel caso delle indagini digitali è frequente che questo rapporto si inverta, in quanto prima si opera il sequestro del dispositivo informatico e poi si procede alla perquisizione.

Secondo una prima impostazione, si faceva derivare l'illegittimità del sequestro ove venisse rilevata l'illegittimità della perquisizione. Si tratta della *teoria dell'albero avvelenato*, elaborata dalla giurisprudenza nordamericana degli '20 del secolo scorso e inizialmente avallata dalla Cassazione italiana, secondo la quale l'invalidità dell'atto precedente si propaga su quello successivo, rendendolo a sua volta invalido.

Con l'avvento della tecnologia, e il conseguente maggiore impiego di indagini digitali, si è assistito ad un rovesciamento di questa impostazione, in quanto si è evidenziata, ad esempio, l'importanza del sequestro nell'ottenere la copia dei dati, sui quali poi verrà effettuata la perquisizione. Secondo questa nuova impostazione, accolta sia dalla Cassazione sia dalla Corte costituzionale, si ritiene che non si possa tanto parlare di logica consequenzialità tra perquisizione e sequestro, quanto piuttosto di atti separati la cui invalidità di uno non produce come conseguenza diretta l'invalidità dell'altro. Questa nuova impostazione prende il nome di principio del *male captum bene retentum*.

La legge 48/2008 ha modificato il comma secondo dell'articolo 354 c.p.p., introducendo la possibilità per gli ufficiali di polizia giudiziaria di effettuare le attività necessarie ad assicurare la conservazione e impedire l'alterazione dei dati e delle informazioni contenuti nei sistemi informatici e telematici. In merito a tali attività di informatica forense, urge compiere una distinzione, per la quale è emerso nel corso degli anni un

[44] A. Gammarota, Materiali didattici, UNIPD Seminario 2023.

acceso dibattito, tra *accertamenti tecnici ripetibili* e *irripetibili*[45]. Infatti occorre analizzare due articoli del codice di procedura penale che, per quanto dispongono, sembrano l'uno disciplinare gli accertamenti ripetibili, mentre il secondo quelli irripetibili. L'articolo 359 c.p.p. disciplina tutti quei casi in cui il PM può avvalersi di un consulente dotato di specifiche competenze per compiere determinati accertamenti[46]. Dall'analisi di tale articolo posso desumere che tra gli accertamenti esso includa, seppur implicitamente, anche tutte quelle attività che non causano un'alterazione delle cose o dei luoghi, e che pertanto sono da definirsi come accertamenti ripetibili, ossia tutti quegli accertamenti, che indipendentemente dal numero di volte e da chi li esegue, producono sempre lo stesso risultato. L'articolo 360 c.p.p. disciplina invece i casi opposti, ossia "quando gli accertamenti previsti dall'articolo 359 riguardano persone, cose o luoghi il cui stato è soggetto a modificazione, il pubblico ministero avvisa, senza ritardo, la persona sottoposta alle indagini, la persona offesa dal reato e i difensori del giorno, dell'ora e del luogo fissati per il conferimento dell'incarico e della facoltà di nominare consulenti tecnici"[47]. Tale articolo disciplina gli accertamenti irripetibili, ossia tutti quelli nei quali lo stato delle persone, cose o luoghi è soggetto ad alterazione. Ciò porta a diversi risultati oppure all'impossibilità di effettuare attività future in quanto l'accertamento è esperibile una sola volta. Posso distinguere tre tipologie differenti di irripetibilità degli accertamenti: in senso giuridico, in senso di indifferibilità e in senso tecnico; quella che più mi interessa analizzare, in quanto strettamente connesse al tema dell'acquisizione forense in ambito informatico, è l'*irripetibilità in senso tecnico*.

Secondo quanto indicato in una sentenza della Cassazione, l'attività di accertamento non riguarda la fase di constatazione o la raccolta di dati materiali pertinenti al reato o alla sua prova, ma il loro studio e la relativa elaborazione critica[48], ma riguarderebbe invece quella dell'acquisizione forense, la quale si sostanzia nella formazione della cosiddetta copia forense o copia bit-a-bit, ossia una copia identica all'originale. Terminata la constatazione e raccolta dei dati, si apre la seconda fase inerente all'accertamento tecnico o analisi dei dati raccolti mediante la creazione delle copie forensi. La Convenzione di Budapest prima

[45] S. Aterno - F. Cajani - G. Costabile, *Cyber forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*. Giappichelli, 2021, pag. 442-444 e 634.

[46] Codice di procedura penale, articolo 359, comma 1: "Il pubblico ministero, quando procede ad accertamenti, rilievi segnaletici, descrittivi o fotografici e ad ogni altra operazione tecnica per cui sono necessarie specifiche competenze, può nominare e avvalersi di consulenti, che non possono rifiutare la loro opera".

[47] Codice di procedura penale, articolo 360, comma 1.

[48] Cassazione, Sez. I, 14 marzo 1990, n. 301.

e la legge n. 48/2008 poi hanno sottolineato la fragilità delle prove digitali e ancor prima dei dati che le compongono. Pertanto, si sono modificati numerosi articoli del codice di procedura penale in merito alle attività di indagine, imponendo l'adozione di misure tecniche adeguate alla conservazione dei dati digitali. Inoltre, per garantire la loro conservazione, si sono create delle linee guida riconosciute a livello internazionale, ossia le ISO/IEC 27037. Queste regolamentazioni sostengono in linea generale l'irripetibilità degli accertamenti tecnici, in quanto, come già ho evidenziato in precedenza, anche il semplice spegnimento di un dispositivo acceso è idoneo a modificare lo stato dei dati contenuti nel dispositivo, è bene dunque estrarre i dati, tramite copia forense, dal dispositivo nello stato in cui questo si trova. Analizzando quanto è accaduto in Italia, il Tribunale del riesame di Torino sembra anch'esso essere orientato verso il considerare l'irripetibilità degli accertamenti tecnici, ad esempio nell'ordinanza del 7 febbraio 2000 ha considerato inutile il sequestro dell'hard disk e ha indicato come gli ufficiali di polizia giudiziaria avessero dovuto procedere alla creazione di una copia forense, con specificazione di ogni singola operazione[49]. Lo stesso Tribunale di Vigevano nel caso noto come *il delitto di Garlasco* ha manifestato una certa contrapposizione rispetto alla ripetibilità degli accertamenti tecnici su materiale informatico, sostenendo la loro irripetibilità e ribadendo la fragilità dei dati digitali e la facilità di alterazione che ne deriva[50]. Nel caso di Garlasco erano stati eseguiti numerosi accessi al computer e alla tesi dell'allora indagato Alberto Stasi, senza osservare le procedure raccomandate dalla Convenzione e dalle linee guide sopra citate; le relazioni peritali e il consulente tecnico del PM hanno evidenziato come vi sia stata un'alterazione dei dati e metadati che ha causato secondo le stime fatte una perdita di quasi il 75% dei dati informatici contenuti nel dispositivo di Stasi[51], il quale poteva essere considerato l'elemento basilare dell'indagine su cui si fondava tra l'altro il suo alibi .

[49] Tribunale Penale di Torino, Sez. del riesame, Ordinanza del 7 febbraio 2000.
[50] S. Pietropaoli, *Informatica criminale. Diritto e sicurezza nell'era digitale*. Giappichelli, 2022, pag. 94-96.
[51] Tribunale Penale di Vigevano, sentenza del GUP in data 17 dicembre 2009.

4. Le sentenze della Cassazione a sostegno della ripetibilità

Vorrei ora terminare questo secondo capitolo attraverso l'analisi di alcune sentenze della Cassazione, da cui più si evidenzia il sostegno alla ripetibilità nell'acquisizione e nell'analisi dei dati informatici, mi preme iniziare dalla sentenza n. 14511 del 5 marzo 2009, dove è stato stabilito che "Non rientra nel novero degli atti irripetibili l'attività di estrazione di copia di file da un computer oggetto di sequestro, dal momento che essa non comporta alcuna attività di carattere valutativo su base tecnico-scientifica, né determina alcuna alterazione dello stato delle cose, tale da recare pregiudizio alla genuinità del contributo conoscitivo nella prospettiva dibattimentale, essendo sempre comunque assicurata la riproducibilità d'informazioni identiche a quelle contenute nell'originale"[52]. Ancora prima di questa sentenza, la stessa Cassazione nel febbraio del 2009 ha voluto sottolineare come "l'estrazione dei dati contenuti in un supporto informatico, se eseguita da personale esperto in grado di evitare la perdita dei medesimi dati, costituisce un accertamento tecnico ripetibile"[53]. In relazione a questa ultima sentenza occorre sottolineare fin da subito, come tra l'altro ho già fatto precedentemente, che data la complessità delle indagini informatiche si richiedono specifiche competenze tecniche agli operatori, in modo da garantire presidio per l'indagato e rapidità delle indagini. Accade molto spesso che tali necessità si scontrino da un lato con ostacoli interni legati al fatto che le indagini partono in ritardo, e dall'altro lato con ostacoli esterni dovuti all'ubicazione all'estero dei server e la conseguente necessità di cooperazione investigativa. In ossequio alla richiesta di specifiche conoscenze informatiche, giuridiche, investigative e d'ingegneria informatica, mi occorre evidenziare come in Italia ci sia arretratezza sotto questo punto di vista, in quanto ad esempio, l'albo dei periti istituito presso i tribunali prevede solo otto categorie, tra le quali non rientra la digital forensics. Per la ragione anzidetta, si nota una certa discrepanza tra la visione della Cassazione data con la sentenza n. 11683 del febbraio 2009, in cui si afferma che nel caso in cui l'accertamento sia eseguito da personale esperto allora dovrà essere considerato ripetibile, e le competenze richieste per rientrare nell'albo dei periti, previsto dallo stesso ordinamento.

Vorrei concludere l'analisi di alcune delle sentenze della Cassazione più rilevanti in materia di qualificazione di accertamenti tecnici ripetibili o irripetibili, analizzando prima

[52] Cassazione, I Sezione, sentenza del 5 marzo 2009, n. 14511.
[53] Cassazione, I Sezione, sentenza del 26 febbraio 2009, n. 11863.

la sentenza n. 24998 del 4 giugno 2015 e poi la sentenza della Suprema Corte n. 11905 del 21 marzo 2016.

La Cassazione, II Sezione, con sentenza n. 24998 ha voluto ribadire quanto indicato in precedenza con la sentenza del marzo 2009, di cui sopra ho già scritto, affermando che "non dà luogo ad accertamento tecnico irripetibile la mera estrazione dei dati archiviati in un computer, trattandosi di operazione meramente meccanica, riproducibile per un numero indefinito di volte"[54]. La Cassazione in questo caso ha posto alla base di questa decisione l'assenza di uno standard prestabilito per la metodologia di trattamento ed analisi della prove informatiche.

Infine con la V Sezione, sentenza n. 11905 del 21 marzo 2016, la Suprema Corte ha di fatto consolidato l'orientamento italiano, affermando e confermando che "L'estrazione di dati archiviati in un supposto informatico (nella specie: floppy disk) non costituisce accertamento tecnico irripetibile anche dopo l'entrata in vigore della legge 18 marzo 2008, n. 48". La quale come ho già scritto in precedenza ha introdotto l'obbligo in capo alla polizia giudiziaria di rispettare determinati protocolli di comportamento, senza però prevedere alcun tipo di sanzione processuale in caso di mancata loro adozione, con l'unica eccezione di poter derivare, dal mancato rispetto di essi, effetti sull'attendibilità della prova[55].

[54] Cassazione, II Sezione, sentenza del 4 giugno 2015, n. 24998.
[55] Cassazione, V Sezione, sentenza del 21 marzo 2016, n. 11905.

CAPITOLO III

COMPARAZIONE CON L'ORDINAMENTO DI COMMON LAW

Sommario: 1. Il diverso orientamento nei Paesi di Common Law. – 2. Differenze sostanziali con il nostro ordinamento.

1. Il diverso orientamento nei Paesi di Common Law

Per documentare le varie fasi di individuazione, acquisizione, analisi e conservazione si è creato un processo di documentazione definito *chain of custody*. Tale processo di documentazione è stato elaborato nel contesto angloamericano, e rappresenta una raccolta di documenti unica che inizia con la fase di individuazione e termina con quella di conservazione. Ciò appare in netto contrasto rispetto a quanto indicato dal nostro principio di separazione delle fasi, a cui tra l'altro si lega il sistema del doppio fascicolo, ossia quello del dibattimento che si forma appunto in fase dibattimentale nel contradditorio tra le parti e quello del PM che si forma nella fase preliminare, precedente al dibattimento. Nel nostro ordinamento, dunque, la documentazione assume una forma progressiva, in quanto la catena di custodia sarà costituita dalla somma dei verbali che documentano le singole attività riguardanti i dati digitali e ciò comporta il rischio di incompletezza della catena di custodia, determinata ad esempio dal dualismo tra atti ripetibili e irripetibili. Tale documentazione assume inoltre una natura che potremmo definire *ibrida*, in quanto composta, da un lato, dall'attività d'indagine e, dall'altro, dall'attività processuale.

Data l'inadeguatezza della chain of custody del modello angloamericano, essa dovrebbe essere convertita in un verbale a formazione progressiva, acquisito in dibattimento e aggiunto al fascicolo di quest'ultimo, ad implementazione obbligatoria anche durante le diverse impugnazioni che si possono avere nel corso del processo.

Analizzate nell'ultimo paragrafo del precedente capitolo alcune sentenze emesse dalla Cassazione italiana in merito alla classificazione delle attività di indagine, nell'ambito informatico della digital forensics, e ora tale aspetto di contrasto tra il nostro ordinamento e quelli di common law, vorrei proseguire con l'evidenziare le differenze che si riscontrano con gli ordinamenti di Common Law britannico e americano, portando all'attenzione due casi inerenti alla digital forensics, focalizzandomi dapprima su un caso avvenuto negli Stati Uniti e successivamente su uno piuttosto recente nel Regno Unito. Ci tengo a sottolineare come la scelta di questi non sia casuale, in quanto entrambi

racchiudono quella che è la visione condivisa nell'ordinamento di Common Law, più nello specifico in materia di qualificazione degli accertamenti tecnici.

Nel caso *Jayzon Decker, Colter Peterson v. Deserae Turner* accaduto nel febbraio 2017, l'adolescente Decker allora sedicenne ha attirato, assieme all'amico Colter Peterson anche lui sedicenne, la quattordicenne Deserae Turner in un luogo isolato e le hanno sparato alla nuca. Questo gesto è stato compiuto poiché Peterson si era stancato dei suoi messaggi e Decker gli ha consigliato di ammazzarla cosicché non lo "disturbasse" ulteriormente. Fortunatamente la ragazzina è stata ritrovata dopo alcune ore dall'accaduto ancora viva e al processo, svoltosi circa tre anni dopo, ha potuto partecipare. Questo caso è molto importante in materia di digital forensics poiché i sospettati sono stati ritrovati con dispositivi elettronici, appositamente distrutti per cancellare ogni traccia, che durante la fase delle indagini sono stati analizzati dal Digital Forensics Crime Lab della Utah Tech University. Il giudice ha infatti sottolineato come l'estrazione di dati da dispositivi rotti o spenti rappresenti un'attività particolarmente delicata, che deve essere svolta con molta attenzione seguendo delle tecniche specifiche in quanto si tratta di un'attività irripetibile. La scelta di inviare tali dispositivi al Laboratorio della Utah University è stata fatta non soltanto per la prossimità alla vicenda ma anche per l'esperienza e la formazione di chi lavora all'interno della struttura. Dall'estrazione dei dati sono stati scoperti i messaggi scambiati dai due sull'organizzazione di quello che poi è stato giudicato dalla Corte dello Utah e ha portato Decker e Peterson ad essere condannati a 15 anni di carcere per tentato omicidio e ostruzione alla giustizia[56].

Un altro caso più recente che vorrei analizzare è quello del rapimento, stupro e omicidio di Sarah Everard, compiuto dall'agente di polizia Wayne Couzens il 3 marzo 2021 nel Sud di Londra[57]. In questo caso la competenza in materia di digital forensics da parte degli investigatori è stata di assoluta importanza nel chiarire la vicenda e poi soprattutto ai fini della sentenza emanata dal giudice. In particolare nel valutare i fatti, durante la fase di indagine si sono consultati dapprima i filmati delle telecamere nel luogo del rapimento, e tale operazione è stata di molto facilitata dal fatto che la vittima quel giorno indossava abiti colorati e ciò la rendeva rapidamente individuabile e successivamente sono stati analizzati i ripetitori a cui i cellulari di Sarah e di Couzens si erano collegati per

[56] Caso J. Decker, C. Peterson vs. D. Turner, informazioni prese dal sito: https://dfcl.utahtech.edu/notable-cases/.

[57] Caso S. Everard vs. W. Couzens, informazioni prese dai siti: https://www.bbc.com/news/uk-england-london-58747614 e https://www.theguardian.com/uk-news/2021/sep/30/sarah-everard-murder-wayne-couzens-whole-life-sentence

comprendere la posizione dei due al momento del rapimento della donna. Nel compiere tali attività il giudice ha sottolineato l'importanza di considerare l'estrazione e l'analisi dei dati come accertamento tecnico ripetibile quando i cellulari sono accesi, come nel caso in questione, e ha ribadito la necessità di compiere immediatamente una copia forense dei filmati per evitare la manipolazione di questi e la perdita di dati utili ai fini della valutazione della vicenda. Couzens, compresa non tanto la facilità, quanto invece l'effettività con la quale avrebbe potuto la polizia ricollegare l'accaduto alla sua persona, decise di dichiarsi colpevole del rapimento dell'uccisione di Sarah Everard e venne così condannato all'ergastolo.

2. Differenze sostanziali con il nostro ordinamento

Come ho potuto evidenziare attraverso l'analisi di alcune sentenze, emerge una differenza sostanziale nella dottrina che si pone come base nell'assunzione delle decisioni, in questo caso in merito alla qualificazione di un accertamento come attività ripetibile o irripetibile. Nei Paesi di Common Law, in particolare negli Stati Uniti, si è diffusa una teoria completamente opposta rispetto a quella sviluppatasi nel nostro ordinamento del *male captum bene retentum*. Conosciuta come *fruit of the poisonous tree*, o teoria dei frutti dell'albero avvelenato, essa prevede che l'inutilizzabilità dell'atto si estenda anche a tutte le prove acquisite in successione all'atto illegittimo. Ad esempio, riguardo al tema della digital forensics, nel caso di acquisizione di dati mediante estrazione da un dispositivo, il mancato rispetto delle best practices comporterebbe l'inutilizzabilità di tali dati come prove in sede processuale. La stessa logica opera anche nelle sedi di indagine tradizionali, dove ad esempio le prove sequestrate in seguito ad una perquisizione illegittima diverrebbero inutilizzabili.

Tale teoria viene manifestata dalla Corte Suprema degli Stati Uniti nel 1914, nel corso della sentenza Weeks v. United States, attraverso la formulazione di una regola, che verrà poi definita *exclusionary rule*, la quale si estenderebbe a tutte le prove, ossia i frutti, di un atto illegittimo, in quanto tale inteso l'albero avvelenato. La finalità perseguita dai giudici americani, attraverso l'elaborazione di questa regola, consiste nel "prevenire il diffondersi di tecniche di indagine a tal punto illegittime da provocare un sostanziale offuscamento, una radicale vanificazione delle garanzie costituzionalmente riconosciute all'imputato.

Così si afferma che l'esclusione della prova costituisce un efficace deterrente contro perquisizioni irragionevoli"[58].

In Italia trova applicazione la teoria del *male captum bene retentum*, in base alla quale l'inutilizzabilità di un atto non si estende a quello successivo. Ciò si evince da quanto è affermato nell'art. 191 c.p.p.[59], il quale fa esclusivo riferimento alle prove acquisite in via primaria o in violazione di un divieto previsto dalla legge, mentre in tutti gli altri casi l'inutilizzabilità derivata non trova applicazione nel nostro ordinamento. In tema di nullità invece, il nostro Codice di procedura penale all'art. 185, prevede che "la nullità di un atto rende invalidi gli atti consecutivi che dipendono da quello dichiarato nullo"[60].

Da queste due diverse impostazioni si possono ricavare due principi che possono essere posti come base per meglio comprendere le decisioni delle rispettive Cassazione italiana e Corte Suprema americana. Da un lato la Cassazione italiana ha affermato a più riprese la ripetibilità degli accertamenti tecnici, e questo trova senza dubbio conferma nella teoria del bene captum male retentum accolta nel nostro ordinamento, in quanto nel caso la Cassazione avesse affermato il contrario sarebbe andata in contrasto a quest'ultima, oltre che ai principi di diritto in materia. Dall'altro lato la Corte Suprema introducendo sin dal 1914 la teoria dei frutti dell'albero avvelenato, ha voluto porre delle regole precise alle attività di indagine così da salvaguardare la legittimità di ogni processo a partire dalle prove su cui esso si fonda. Dunque secondo la visione statunitense, dichiarare l'irripetibilità di un accertamento tecnico, significa garantire l'utilizzabilità delle prove acquisite da esso nel rispetto delle regole in materia, senza compromettere la validità del processo nel quale verranno utilizzate.

Nonostante la differenza appena indicata, vorrei tuttavia evidenziare come in materia di digital forensics, in particolare relativamente alla necessità di sequestrare le sole cose pertinenti al reato, tra i due ordinamenti si presenta una visione condivisa, in quanto si ammette in entrambi la necessità di procedere all'acquisizione dei soli dati contenuti nel dispositivo, senza procedere al sequestro di quest'ultimo. In ambito italiano, tale aspetto si ricava ad esempio dalla sentenza della Cassazione n. 34265, nella quale si è dichiarata la violazione di legge e mancanza di motivazione in ordine al sequestro dell'intero

[58] R. Gambini Musso, Il processo penale statunitense. Soggetti ed atti. 3ª Edizione, Torino, Giappichelli, 2009, pag. 15.

[59] Codice di procedura penale, art. 191, comma 1: "Le prove acquisite in violazione dei divieti stabiliti dalla legge non possono essere utilizzate".

[60] Paolo Ferrua, *Teorie della prova: dialogo con Franco Cordero*, Intervento svolto in ricordo di Franco Cordero, al XXXIV Convegno dell'Associazione tra gli Studiosi del processo penale su «Immediatezza nel processo penale», Discrimen, 16 dicembre 2020.

dispositivo, piuttosto che procedere alla realizzazione di una copia forense avente ad oggetto la totalità dei messaggi contenuti nel telefono e la totalità di mail personali e professionali[61].

[61] Cassazione, VI Sezione, sentenza del 22 settembre 2020, n. 34265.

CONCLUSIONI

Analizzati gli aspetti comuni, ma soprattutto quelli sulla diversa qualificazione di accertamenti tecnici tra l'ordinamento italiano e quello di Common Law, vorrei ora prima di volgere alla conclusione evidenziare quali possono essere alcuni dei motivi che hanno indotto la Cassazione italiana a certe conclusioni in materia di digital forensics.

Uno degli obiettivi in ambito processuale, che colpisce un po' tutte le materie, è quello della deflazione del contenzioso. In ambito penale si è cercato a più riprese di raggiungere questo obiettivo così da ridurre l'eccessivo carico giudiziario, dapprima mediante l'istituzione del giudice di pace con competenza penale e successivamente con due interventi normativi nel 2016, i D.lgs. n. 7 e n. 8, con i quali si è trasformato il reato di ingiuria in un illecito civile e gli atti osceni in luogo pubblico sono ora puniti mediante una sanzione amministrativa[62]. Diversamente da quanto accaduto in altre materie, tra cui quella economica che ha visto l'introduzione dell'art. 840 bis c.p.c.[63] per ridurre il carico e migliorare l'accesso alla giustizia, gli interventi in materia penale sopra citati non hanno sortito gli effetti sperati, in quanto hanno visto non la riduzione ma lo spostamento del contenzioso in un'altra sede.

In materia di digital forensics, in relazione alla deflazione processuale, si sottolinea come l'assenza di competenze specifiche degli esperti e di linee guida chiare abbiano portato la Cassazione italiana a qualificare gli accertamenti tecnici come ripetibili, poiché altrimenti si farebbero molti più ricorsi sulla validità delle operazioni e delle prove raccolte attraverso di esse, ciò dunque si scontrerebbe anche con l'obiettivo di ridurre il carico giudiziario.

Evidenziato questo aspetto, vorrei ora analizzare nel dettaglio quelle che secondo il mio punto di vista sono le motivazioni che hanno portato la Cassazione a definire gli accertamenti tecnici su dispositivi informatici come attività meramente meccanica, che in quanto tale è qualificata ripetibile. Innanzitutto, come ho già indicato in relazione alla deflazione processuale, alla base di queste pronunce della Cassazione ci sarebbe anche la mancanza di diffuse competenze in materia di digital forensics, in quanto affermando la ripetibilità degli accertamenti si garantirebbe una maggiore libertà di azione all'attività investigativa, piuttosto che la irripetibilità, la quale comporterebbe invece oltre che dei limiti operativi anche una competenza maggiore sulle diverse misure tecniche da adottare.

---

[62] P. Grillo, La deflazione del contenzioso penale è davvero una chimera?, 29 maggio 2021.

[63] Codice di procedura civile, art. 840 bis, comma 1: " I diritti individuali omogenei sono tutelabili anche attraverso l'azione di classe, secondo le disposizioni del presente titolo".

Questo aspetto appare evidente in relazione alle competenze richieste ai consulenti tecnici per accedere all'albo, le quali sono otto ma tra queste non rientra la digital forensics.
Un altro aspetto di cui tener conto è quello legato alla difficoltà dello Stato nel sostenere un'eccessiva quantità di cause pendenti, un qualcosa che appare assai complicato vista la situazione economica italiana attuale. La Cassazione secondo alcuni giuristi ha voluto classificare le attività di accertamento tecnico come ripetibili per evitare numerosi ricorsi alla giustizia sulla validità delle operazioni e di conseguenza dei dati estratti dai dispositivi in conseguenza ad esse.
Dal mio personale punto di vista trovo che questa qualificazione da parte della Cassazione non sia del tutto centrata rispetto all'obiettivo di ridurre il carico giudiziario e di conseguenza le spese e i tempi. Infatti la teoria accolta nel nostro ordinamento del male captum bene retentum tiene aperte le porte del processo e non farebbe altro che aumentare ulteriormente il carico giudiziario, consentendo infatti alle parti di ricorrere sulle singole attività svolte in fase investigativa.
Nell'ordinamento di common law attraverso la qualifica degli accertamenti tecnici come irripetibili si determina a priori l'improcedibilità nel caso in cui si contrasti con tale qualifica nell'eseguire le operazioni tecniche; dunque, non si rimette al giudice la valutazione delle prove, diversamente da quanto accade nel nostro ordinamento, e non si aumenta di conseguenza il carico giudiziario.
In sostanza ciò che invece dovrebbe essere preso in considerazione per raggiungere questo obiettivo, è il fissare una serie di regole precise da adottare in ottemperanza soprattutto ai principi della Convenzione di Budapest, cosa che tra l'altro è già stata parzialmente fatta a livello nazionale italiano mediante la legge n. 48/2008, tuttavia ciò che risulta mancare attualmente è la previsione di una serie di sanzioni per l'inottemperanza di tali regole di comportamento, infatti è prevista solamente una valutazione del giudice sull'attendibilità delle prove raccolte in sede investigativa.

BIBLIOGRAFIA

ARENA M., *La Convenzione di Budapest del Consiglio d'Europa sulla repressione della criminalità informatica*. Catania, CRIO Papers, 2021.
https://www.lex.unict.it/sites/default/files/crio/papers/CRIO_Papers_n59_Arena.pdf

ARENA M., *Il recepimento in Italia della Convenzione di Budapest. La legge 18 marzo 2008 n. 48.* Fogli di Lavoro per il Diritto Internazionale, 2021.
https://www.lex.unict.it/sites/default/files/files/Crio/FogliLavoro/2021-2/FLADI_2021_2-11.pdf

ATERNO S. - CAJANI F. - COSTABILE G., *Cyber forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*. Giappichelli, 2021.

CASEY E., *Digital Evidence and Computer Crime: Forensics Science, Computers and the Internet.* 3ª Edizione, Elsevier Science Publishing, 2011.

FERRUA P., *Teorie della prova: dialogo con Franco Cordero*. Intervento svolto in ricordo di Franco Cordero, al XXXIV Convegno dell'Associazione tra gli Studiosi del processo penale su «Immediatezza nel processo penale», Discrimen, 16 dicembre 2020.
https://discrimen.it/teorie-della-prova-dialogo-con-franco-cordero/

FIANDACA G. - MUSCO E., *Diritto penale: Parte generale*. 8ª Edizione, Zanichelli, 2019.

GAMBINI MUSSO R., *Il processo penale statunitense. Soggetti ed atti*. 3ª Edizione, Torino, Giappichelli, 2009.

LUPARIA L. - G. ZICCARDI, *Investigazione Penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*. Milano, Giuffrè, 2007.

MAIOLI C. - SANGUEDOLCE E., *I "nuovi mezzi di ricerca della prova fra informatica forense e L. 48/2008*. 7 maggio 2012.
https://www.altalex.com/documents/news/2012/05/03/i-nuovi-mezzi-di-ricerca-della-prova-fra-informatica-forense-e-l-48-2008

MARAFIOTI L., Digital evidence e processo penale, *Cassazione Penale*, 2011.
http://www.iusimpresa.com/risultati.php?hdd_lg=&hdd_mono=2499&hdd_autore=34615&hdd_ricerca=RB

NOCERINO W., *Il captatore informatico nelle indagini penali interne e transfrontaliere*. Padova, Cedam, 2021.

PIETROPAOLI S., *Informatica criminale. Diritto e sicurezza nell'era digitale*. Giappichelli, 2022.

PITTIRUTI M., *Digital evidence e procedimento penale*. Giappichelli, 2018.

SIGNORATO S., *Le indagini digitali: profili strutturali di una metamorfosi investigativa*. Torino, Giappichelli, 2018.

VITALE A., La nuova disciplina delle ispezioni e perquisizioni in ambiente informatico o tele matico, *Diritto dell'internet*. Milano, Wolters Kluwer Italia S.r.l., 2008.

SITOGRAFIA

BBC & THE GUARDIAN, *Sentenza sull'omicidio di Sarah Everard*. Data dell'ultima consultazione: 05/06/2024, da https://www.bbc.com/news/uk-england-london-58747614 https://www.theguardian.com/uk-news/2021/sep/30/sarah-everard-murder-wayne-couzens-whole-life-sentence

BOLLETTINO TRIBUTARIO, *Tribunale Penale di Vigevano, sentenza del GUP in data 17 dicembre 2009*. Data dell'ultima consultazione: 09/05/2024, da https://bollettinotributario.com/blog/3126

COUNCIL OF EUROPE, *European Treaty Series - No. 189*, Protocollo addizionale alla Convenzione sulla criminalità informatica, relativo alla qualifica come reato degli atti di natura razzista e xenofoba commessi attraverso sistemi informatici.
Data dell'ultima consultazione: 28/04/2024, da https://rm.coe.int/168008160f

DE JURE, *Sentenze di Cassazione*. Data dell'ultima consultazione: 28/05/2024, da https://dejure.it/

GARANTE PRIVACY, *GDPR*. Data dell'ultima consultazione: 28/04/2024, da https://www.garanteprivacy.it/il-testo-del-regolamento

ICTLEX, *Tribunale Penale di Torino, Sez. del riesame, Ordinanza del 7 febbraio 2000 sull'inutilità dei sequestri dei computer*. Data dell'ultima consultazione: 09/05/2024, da https://www.ictlex.net/ord-trib-torino-722000-inutili-i-sequestri-di-computer/

KSL, *Caso Deserae Turner*. Data dell'ultima consultazione: 04/06/2024, da https://www.ksl.com/article/46251086/teen-who-shot-deserae-turner-sentenced-to-15-years-to life#:~:text=LOGAN%20%E2%80%94%20A%20judge%20ordered%20prison,stealing%20the%20wounded%20girl's%20belongings.

NORMATTIVA, *Costituzione*. Data dell'ultima consultazione: 20/04/2024, da https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:costituzione

POLIZIA DI STATO, *Convenzione del Consiglio d'Europa sulla criminalità informatica*. Data dell'ultima consultazione: 28/04/2024, da https://www.poliziadistato.it/statics/14/convenzione-cybercrime.pdf

POLIZIA DI STATO, *Preambolo della Convenzione del Consiglio d'Europa sulla repressione della criminalità informatica*. Data dell'ultima consultazione: 28/04/2024, da https://www.poliziadistato.it/statics/14/convenzione-cybercrime.pdf

STUDIO LEGALE NAPPI, *I diversi orientamenti in merito alla natura ripetibile/irripetibile dell'accertamento tecnico forense*. Data dell'ultima consultazione: 24/05/2024, da https://www.studiolegalenappi.it/i-diversi-orientamenti-in-merito-alla-natura-ripetibile-irripetibile-dellaccertamento-tecnico-forense/

TRECCANI, *Prova. Diritto processuale penale.* Data dell'ultima consultazione: 20/04/2024, da https://www.treccani.it/enciclopedia/prova-diritto-processuale-penale/