LUISS

Dipartimento di Giurisprudenza

Cattedra di Diritto Processuale Penale

La ricerca della prova digitale: le perquisizioni *online* nel contesto delle indagini informatiche.

Prof. Alberto Macchia
RELATORE

Prof. Mitja Gialuz
CORRELATORE

Marianna Stella Grillo - Matr. 139573
CANDIDATA

Anno Accademico 2021/2022

Alla mia famiglia

«Cominciate col fare
ciò che è necessario,
poi ciò che è possibile.
E all'improvviso vi sorprenderete
a fare l'impossibile».
S. FRANCESCO D'ASSISI

INDICE

CAPITOLO III

LA c.d. PERQUISIZIONE *ONLINE*, IN BILICO TRA DISCIPLINA DELLE INTERCETTAZIONI E REGIME DELLE PERQUISIZIONI

INTRODUZIONE

Il presente elaborato si propone di approfondire talune delle questioni riguardanti le innovazioni in campo tecnologico e informatico che hanno inciso sul processo penale in tema di mezzi di ricerca della prova informatici.

È chiaro come, anche a causa della recente pandemia di Covid-19, le abitudini quotidiane di ogni essere umano siano state influenzate dal globale progresso tecnologico, sempre in costante espansione: ciò ha portato ad un incremento sia della diffusione di nuovi mezzi di comunicazione, ma anche di nuove forme di crimine informatico, spesso difficili da contrastare a causa della difficoltà di individuazione degli autori, delle relative problematiche sul *locus commissi delicti*, e a causa soprattutto di alcune lacune normative che rendono talune condotte illecite ancora prive di una tipizzazione. Infatti, sarà preliminare all'esposizione l'analisi del contesto storico e sociale degli ultimi anni relativo all'evoluzione dei *Cybercrimes* e delle varie tipologie degli attacchi informatici realizzati all'interno del *Cyberspace*.

Successivamente, saranno delineate le misure di contrasto adottate prima in sede sovranazionale, attraverso l'approvazione della Convenzione di Budapest sulla criminalità informatica del 2001, e in seguito recepite dall'ordinamento italiano con la legge di ratifica 18 marzo 2008, n. 48, che hanno ritoccato l'assetto normativo nazionale sul piano del diritto penale sostanziale e procedurale, intensificando la cooperazione giudiziaria tra gli Stati. In particolar modo, saranno poi esaminate le caratteristiche e le tecniche della c.d. *digital forensics*, attuate da professionisti del settore, in relazione alla corretta acquisizione della *digital evidence*, a cui potrà darsi luogo solo mediante l'utilizzo delle *best practices*, in considerazione del concreto pericolo di inquinamento a cui sono soggette le fonti di prova, e più in generale in relazione alla volatilità dei dati digitali, al fine di garantire, attraverso l'uso di questi strumenti, il rispetto del principio del contraddittorio tra le parti e del diritto inviolabile di difesa, stabiliti dalla Costituzione.

Una volta tracciata la cornice normativa di riferimento, verranno esposte le differenze principali tra gli istituti di ricerca della prova tradizionali e i mezzi di ricerca della prova informatici tipici, quali ispezione, perquisizione, sequestro e intercettazioni,

così come disciplinati a seguito della L. 48/2008 e dei successivi interventi riformatori, che hanno apportato alcune modifiche soprattutto in campo delle c.d. intercettazioni ambientali e riguardo all'utilizzo del captatore informatico nello svolgimento di attività non espressamente autorizzate dai provvedimenti esecutivi disposti dal pubblico ministero e convalidati dal giudice.

Per quanto riguarda quest'ultimo aspetto, infine, prendendo spunto dall'esperienza comparata, e in particolare dalla giurisprudenza costituzionale tedesca, si analizzerà la figura delle perquisizioni *online*: l'elaborato cercherà di chiarire quello che rappresenta l'attuale quesito centrale dibattuto dalla dottrina e dalla giurisprudenza, sulla natura di queste operazioni svolte attraverso l'inoculazione del *malware,* e riguardo ai profili inquadrativi di quest'ultime come attività utili alle indagini o utilizzabili solo per scopi preventivi, dalla struttura atipica o incostituzionale, propendendo per quest'ultima conclusione in considerazione della potenziale lesività di numerosi diritti fondamentali che garantiscono la libertà e la *privacy* di ogni essere umano.

Tale punto di approdo rappresenterà la chiave di svolta dell'esposizione, in cui saranno descritti i passaggi che il legislatore in futuro dovrà compiere in modo da effettuare il corretto bilanciamento tra gli interessi in gioco, per rendere finalmente ammissibile questa nuova tecnica investigativa, che potrebbe rivelarsi utile per l'acquisizione di nuove prove digitali, tali da suscitare non indifferenti conseguenze sul piano processuale.

CAPITOLO I

L'IMPATTO DELLA RIVOLUZIONE CIBERNETICA NELL'ANALISI DELLA PROVA DIGITALE

SOMMARIO: I.1 La nuova dimensione del *Cyberspace*. – I.2 Dal *Computer crime* al *Cybercrime*: evoluzione e tipologie di attacchi informatici. – I.3 Inquadramento normativo: rilievi introduttivi. – I.3.1 Sviluppi a carattere sovranazionale nell'Unione Europea. – I.3.2 La Convenzione di Budapest e relativi protocolli addizionali. – I.3.2.1 Interventi post Convenzione del 2001 – I.3.3 Il crimine informatico e la disciplina delle prove digitali nel diritto penale italiano pre Convenzione. – I.3.4. La legge 18 marzo 2008, n. 48, di ratifica della Convenzione di Budapest. – I.4 La *Computer Forensics*. – I.4.1 Le *Best practices*. – I.4.2 *Digital forenser* e attività di *forensics*: le fasi. – I.5 La *Mobile Forensics*.

I.1 La nuova dimensione del *Cyberspace.*

La società attuale è caratterizzata da una crescita esponenziale della tecnologia che ha un impatto sempre più invasivo nella vita privata di ogni singolo. Se in precedenza essa era considerata un semplice ausilio alle attività umane, ora la "rivoluzione tecnologica", costituita dall'uso di strumenti informatici sofisticati capaci di generare e diffondere nel *web* dati di ogni genere, soprattutto personali, rappresenta il nuovo modo di partecipare alla vita pubblica, influenzando il progresso sociale ed espandendo le capacità dell'essere umano, prima più limitate; ma non solo: le informazioni personali costituiscono un grandissimo valore economico, una merca di scambio tale da incidere sul *business* di alcune società.

La nuova dimensione in cui sono concentrate le attività sociali, politiche ed economiche umane è uno "spazio virtuale", inteso come un mondo in cui siamo connessi e interagiamo nello scambio di informazioni da qualsiasi luogo e in qualsiasi momento, meglio definito come *Cyberspace* (Cyberspazio)[1], termine che fu coniato dallo scrittore William Gibson negli anni Ottanta, utilizzato poi nel romanzo *Neuromante.*

[1] Il termine *cyberspace* fu coniato dallo scrittore William GIBSON, Cfr. *Neuromante*, 1986 «*Cyberspazio*: un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione, da bambini a cui vengono insegnati i concetti matematici... Una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. Impensabile complessità. Linee di luce allineate nel non-spazio della mente, ammassi e costellazioni di dati. Come le luci di una città, che si allontanano [...]».

Lo spazio cibernetico comprende una molteplicità di concetti tecnologici: esso non può essere delimitato alla sola dimensione dei beni fisici tangibili dei dispositivi digitali in cui si sviluppa la vera e propria attività informatica di produzione e acquisizione dei dati; né può essere ricompreso nel concetto di *Internet*, quale sistema costituito da collegamenti informatici interconnessi.

Attualmente non esiste una definizione comune capace di ricomprendere l'ampio spettro costituito dal *Cyberspace*; tuttavia, l'art. 2 del decreto del Presidente del Consiglio dei ministri n. 66/2013[2] ha cercato di chiarire questo concetto definendolo come l'insieme di infrastrutture informatiche tra loro connesse, costituito da *hardware, software*, dati ed utenti, nonché dalle relative relazioni intercorrenti tra gli stessi[3] ricomprendendo, perciò, sia la categoria delle reti informatiche del *web*, sia i sistemi informatici in cui i dati sono generati.

Diversi studiosi hanno cercato di scomporre il Ciberspazio in livelli differenti: alcuni, come Martin C. Libicki, dividono il *cyberspace* su tre livelli, quali fisico, sintattico e semantico[4]; altri studiosi rappresentano il Ciberspazio su quattro livelli: un livello fisico, in cui sono presenti gli strumenti e i dispositivi che permettono l'efficienza della rete; un livello logico, caratterizzato dal montaggio delle diverse componenti; un livello informativo, in cui è generata e distribuita l'informazione attraverso una connessione tra gli utenti; un livello personale, che riguarda i singoli soggetti che eseguono operazioni *online*[5].

Davanti alla nuova realtà è cambiato l'approccio alla "criminalità informatica" intesa come l'insieme delle condotte antigiuridiche legate all'utilizzo delle nuove forme di tecnologia[6], divenuta "criminalità cibernetica" o, criminalità "nel" *Cyberspace*. Tale categoria comprende una molteplicità di illeciti e di modalità di offesa di diritti ed

---

[2] V. Direttiva sugli indirizzi per la protezione cibernetica e la sicurezza informatica nazionale adottata con d.p.c.m. 24 gennaio 2013, in *G.U.*,19 marzo 2013, n. 66.

[3] M. MENSI, P. FALLETTA, *Il diritto del web*, Padova, CEDAM, 2018.

[4] L. MARTINO, La quinta dimensione della conflittualità. *L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica&Società*, 2018, 1, p. 62 ss.

[5] B. PANATTONI, *Compliance, cybersecurity e sicurezza dei dati personali*, Assago, 2020.

[6] A. BALLONI, R. BISI, R. SETTE, *Principi di criminologia applicata: criminalità, controllo, sicurezza*. Assago: Wolters Kluwer, 2015, p. 254 ss.

interessi altrui, anche nuovi, essendo il frutto dello stesso sviluppo tecnologico, in cui sono compresi, oltre ai delitti informatici le cui condotte sono già normativamente previste, ulteriori reati con nuove modalità, non necessariamente espresse sul piano della tipicità penale, ma in concreto correlabili all'elaborazione, comunicazione, trasmissione, trattamento in rete di dati, informazioni e contenuti "digitali" di ogni tipo[7].

Il nuovo spazio virtuale è quindi un luogo dove qualsiasi utente può accedere ad ogni tipo di servizio richiesto, e, nonostante offra numerosi aspetti positivi per l'evoluzione sociopolitica ed economica dei singoli Stati, grazie alle *Information and Communication Technologies* (ICT), esso nasconde delle criticità che possono sfociare in minacce cibernetiche, ossia nuove condotte aggressive commesse da singoli o più utenti interconnessi che operano per mezzo o a danno del *cyberspace*, capaci di provocare gravissimi danni su interi sistemi (privati o statali) che spesso, a causa di una scarsa sicurezza informatica, risultano vulnerabili.

Il *Cyberspace* è caratterizzato da una dimensione anonima, aspaziale e atemporale: ciò rende difficile l'applicazione delle fattispecie penali in uno spazio privo di frontiere, considerando i limiti previsti dal principio di territorialità che prescrive l'individuazione del luogo in cui si verifica la condotta. L'atemporalità, tipica del suddetto spazio virtuale, consente agli utenti di poter svolgere ed eventualmente posticipare il loro operato attraverso dei meccanismi automatizzati, e permette di agire in maniera totalmente anonima e senza che vi sia un contatto fisico tra il soggetto utente autore e il sistema informatico[8], e ciò risulta essere problematico per la persecuzione delle nuove condotte offensive.

Ergo, è necessario regolare e offrire una maggiore tutela, in relazione all'ampiezza di tale assetto, alle attività svolte all'interno del *cyberspace*, stabilendone i diritti e delimitandone i contenuti legittimi, come in un sistema armonizzato. Inoltre,

---

[7] L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, Torino, Utet, 2019.

[8] ENCICLOPEDIA TRECCANI, "*Information and Communication Technologies* (ICT)": Tecnologie riguardanti i sistemi integrati di telecomunicazione (linee di comunicazione cablate e senza fili), i computer, le tecnologie audio-video e relativi software, che permettono agli utenti di creare, immagazzinare e scambiare informazioni. Rilevanti incentivi economici favoriscono questo processo di integrazione, promuovendo la crescita delle imprese attive nel settore.

sarà necessario sviluppare una maggiore cooperazione a livello globale tra gli Stati e i privati in materia di cybersicurezza, in modo da riuscire ad evitare i molteplici attacchi informatici a cui il sistema è esposto mediante un'adeguata azione difensiva[9], che si tradurrebbe in una riduzione ingente dei costi per la sicurezza informatica.

I.2 Dal *Computer crime* al *Cybercrime*: evoluzione e tipologie di attacchi informatici.

Nella sua accezione più comune, l'espressione "criminalità informatica" indica l'insieme delle condotte devianti connesse all'uso delle nuove tecnologie e, più precisamente, designa quelle realtà criminali in cui il computer è coinvolto come strumento, simbolo o oggetto del fatto delittuoso[10].

La metà degli anni '90 traccia l'inizio di una nuova epoca: tutti gli utenti potevano finalmente accedere liberamente ad *Internet* tramite i loro dispositivi. Questo evento segna il passaggio dalla categoria dei reati informatici o *Computer crimes*, alla categoria dei reati cibernetici[11] o meglio definiti *Cybercrimes*, una categoria più ampia, che comprende condotte che riguardano globalmente il *Cyberspace*. Una prima definizione generica di *Cybercrime* è stata fornita da uno studio condotto negli Stati Uniti nel 1979, che ravvisa come punto fondamentale del nuovo fenomeno criminale la conoscenza dell'informatica[12] quale presupposto per eseguire e perseguire l'illecito[13].

I due concetti sopraesposti, sebbene spesso possano essere utilizzati come sinonimi, in realtà designano fenomeni che si differenziano tanto per le loro modalità di

---

[9] Presidenza del Consiglio dei Ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, nel dicembre 2013.

[10] D. VULPIANI, *La nuova criminalità informatica. Evoluzione del fenomeno e strategie di contrasto*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, 2007, 1, p. 49.

[11] L. PICOTTI, Presentazione, in ID., *Il diritto penale dell'informatica nell'epoca di Internet,* Padova, 2004, VII.

[12] A. BAIGUERA ALTIERI, *La cultura Hacker negli Stati Uniti d'America*, in *La criminalità informatica in Svizzera e in Italia*, in *diritto.it*. L'Autore traccia un quadro storico sulla nascita dell'informatica in America dal 1958, anno in cui furono allestiti i primi Corsi Universitari di Informatica presso il Massachusetts *Institute of Technology di Boston* (MIT).

[13] C. F. COLOMBO, *Economia criminale: geodiritto, globalizzazione e nuovi canali per i reati d'impresa.* Milano, Wolters Kluwer, 2021, p. 219.

realizzazione, quanto per gli effetti esercitati dai nuovi media sulla dinamica criminosa[14].

I *Computer crime* coincidono con l'insieme di atti illeciti caratterizzati dal ruolo strumentale svolto dal dispositivo fisico informatico nell'iter criminis e che, per loro stessa natura, possono essere commessi anche senza ricorso alle reti telematiche. I reati informatici che hanno assunto, col passare del tempo, una maggiore importanza (come nel caso dell'accesso abusivo ad un sistema informatico[15], o di altri reati per cui sono state previste delle aggravanti riguardanti il campo tecnologico) ruotano principalmente sul concetto di protezione dei "beni informatici" quale oggetto materiale delle condotte criminose, costituito da tre diverse entità: dati, informazioni e programma[16].

Per *Cybercrime*, invece, si intendono: "*Reato nel quale la condotta o l'oggetto materiale del crimine sono correlati a un sistema informatico o telematico, ovvero perpetrato utilizzando un tale sistema o colpendolo […] La categoria concettuale dei c. non ha, tuttavia, un significato tecnico preciso dal punto di vista giuridico, poiché, fatta eccezione per la presenza di un sistema informatico o telematico, vi rientrano una pluralità di condotte e beni giuridici protetti estremamente disomogenei*"[17].

Questa particolare tipologia non può essere più circoscritta ad un numero chiuso o limitato di reati, ma include oggi un'indefinita molteplicità di illeciti e di modalità di offesa di diritti ed interessi altrui, taluni anche di nuova creazione, in quanto frutto dello stesso sviluppo tecnologico, che comprende, a sua volta, oltre ai delitti informatici in senso stretto, ossia i *computer crime*, qualsivoglia altro reato, che presenta modalità esecutive concretamente nuove, non necessariamente espresse sul piano della tipicità

---

[14] A. BALLONI, A. BISI, R. SETTE, *Principi di criminologia applicata – Criminalità, Controllo, Sicurezza*, Padova, CEDAM, 2015, p. 254.

[15] Nelle Raccomandazioni del Consiglio d'Europa del 1989 contro la criminalità informatica l'accesso abusivo ad un sistema informatico era al quinto posto della c.d. lista obbligatoria dei nuovi reati da incriminare, nella convenzione sul *Cybercrime* del 2001, il delitto di accesso abusivo è diventato primo (art. 2); ad oggi il delitto informatico più ricorrente.

[16] D. PETRINI, *La responsabilità penale per i reati via internet*, Napoli, Jovene, 2004, 29 ss.

[17] Così, ENCICLOPEDIA TRECCANI, voce *Cybercrime*, in https://www.treccani.it/enciclopedia/cybercrime_%28Lessico-del-XXI-Secolo%29/

penale, "ma in concreto correlabili all'elaborazione, comunicazione, trasmissione, trattamento in rete di dati, informazioni e contenuti digitali di ogni tipo"[18].

I *Cybercrimes*, quindi, anche se non prescindono dall'uso di reti informatiche come presupposto della condotta illecita, non richiedono necessariamente l'ausilio dello strumento informatico, essendo potenzialmente realizzabili attraverso un qualsiasi dispositivo connesso in rete. Infatti, si parla di attacchi informatici "attivi" quando essi sono diretti a danneggiare le parti del sistema e i dispositivi collegati, e di attacchi informatici "passivi" diretti ad utilizzare indebitamente e alterare dati o informazioni, senza coinvolgere sistemi o infrastrutture su cui sono memorizzati.

La globalizzazione di *Internet* ha provocato un incremento delle "minacce informatiche", poiché le qualità atipiche del *cyberspazio* hanno semplificato la commissione di alcuni reati, che possono essere eseguiti da singoli individui o da gruppi criminali e sono capaci di offendere chiunque, anche vittime in rete connesse o/a estranee. Secondo l'art. 2 n. 8 del Regolamento sulla *cybersicurezza*, per "minaccia informatica" si intende «*qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone*»[19].

Le minacce cibernetiche sono molto difficili da combattere: possono essere realizzate attraverso un attacco semplice, consistente in un'unica, o tramite attacchi complessi, consistenti nel raggruppamento di più operazioni collegate; inoltre, si possono distinguere a seconda delle finalità previste, riguardanti non solo il *cybercrime*, ma ricomprendendo anche l'*hacktivismo*, ossia l'attivismo politico esercitato tramite attacchi *hacker*, il *cyber*-spionaggio che ha l'obiettivo di estrapolare informazioni sensibili, il *cyber*-terrorismo e la guerra cibernetica.

I *cybercrimes*, pur essendo accomunati da diversi elementi che incidono sulla ratio dell'incriminazione, ricomprendono fattispecie di reati molto differenti tra loro che

---

[18] L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, cit., 2019.

[19] Art. 2 n. 8, Regolamento (UE) 2019/881 del Parlamento e Consiglio europeo del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione.

ledono interessi diversi, riconducibili tuttavia a due macrocategorie: la prima è rappresentata da beni giuridici tradizionali che necessitano di aggiornate tutele per contrastare le nuove modalità di aggressione (come avviene nel campo della difesa dei minori o del patrimonio), e da alcuni beni tradizionali caratterizzati da nuovi "oggetti passivi" della condotta, inteso come ciò che comporta l'uso della tecnologia sulla condotta tipica, configurando una dimensione speciale del bene giudico protetto (come nel caso della *privacy* e della circolazione dei dati personali); nella seconda categoria sono inclusi i beni giuridici nati dall'informatica e dalla telematica, raggruppabili nelle sottospecie della riservatezza e dell'integrità e sicurezza informatica.

Gli attacchi informatici possono essere di vario livello ed è per questo che è necessario predisporre *software antivirus* o *firewall* che permettono, tramite scansione, di individuare, isolare ed eliminare la minaccia presente, prima che questa possa creare seri e gravi danni. Tra le tecniche di attacco più diffuse vi sono i "*phishing and social engineering*[20]" e la sua seguente evoluzione in "*pharming*"[21], i "*Distributed Denial of Service* (DDoS)"[22] e i "*malware*" ossia virus che colpiscono strumenti e dispositivi informatici senza il consenso dell'utente. Rientrano nella categoria dei *malware* rientrano: gli *worm*, intesi come programmi che creano copie di se stessi in diversi punti di un dispositivo collegato alla rete; i *trojan* che hanno la capacità di fingersi programmi o documenti normali; gli *spyware* che, come dice la stessa parola, spiano l'attività dell'utente; e i *ransomware*, uno tra gli attacchi più aggressivi presenti dal 2013, capace di cifrare i *file* presenti nel disco rigido in modo che, solo tramite un pagamento in

[20] "Il *phishing* nasce come fenomeno di *social engieering* che, tramite invio da parte di ignoti truffatori di messaggi di posta ingannevoli, spinge le vittime designate a fornire volontariamente informazioni personali", definizione tratta da F. CAJANI, et al. *Phishing e furto d'identità digitale: indagini informatiche e sicurezza bancaria*, Milano, Giuffrè, 2008, 14 ss.

[21] "Il *pharming* (coniato per la prima volta dal *Sans Institute System administration, networking and security*) è un'evoluzione del phishing consistente in un cracking, attraverso un *server* clone, utilizzata per ottenere l'accesso ad informazioni personali e riservate", *Ibidem*, 37 ss.

[22] "Un attacco DDoS è un attacco massiccio, distribuito, deliberato e coordinato da più macchine compromesse per sopraffare un servizio *online* o un *server*. Gli aggressori tentano di attaccare la disponibilità del servizio inviando dati fittizi voluminosi per rendere a corto di risorse la macchina bersaglio", tradotto da B. GUPTA BRIJ, A. DAHIYA, *Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges, and Countermeasures*, Boca Raton, FL; CRC Press, Taylor & Francis Group, 2021, ss. 9.

criptovalute, il sistema potrà decifrarli[23], talvolta usati anche in materia di acquisizione, conservazione e uso delle prove digitali grazie alle straordinarie peculiarità che il *virus* può assumere in tema di captazione.

A questo punto, è necessario elaborare strategie di *cyber defence* a livello nazionale, e soprattutto internazionale: infatti, uno tra i più importanti aspetti relativi all'evoluzione del *cybercrime* è quello rappresentato dal processo di sviluppo e di armonizzazione della disciplina processualpenalistica, mediante l'introduzione di fattispecie sul reperimento delle prove digitali, ormai considerate elementi centrali per l'indagine forense nella risoluzione dei casi pratici. Nei prossimi paragrafi saranno esposte le politiche in ambito *cyber* intraprese principalmente dall'Unione europea e dall'Italia.

I.3 Inquadramento normativo: rilievi introduttivi.

La rivoluzione "cibernetica"[24] e la centralità assunta dai dati digitali hanno comportato un cambiamento sul diritto, non solo penale, chiamato a disciplinarne le regole, principi e valori condivisi, i comportamenti e le responsabilità[25]. Il diritto, inoltre, deve confrontarsi con altri regolamenti sistemi di regole, come ad esempio le regole informatiche che stabiliscono le operazioni tecnologicamente possibili da poter svolgere, tali da causare poi conseguenze dirette sulle norme. Per questo motivo, è compito del legislatore adattarsi ai mutamenti tecnologici sempre più frequenti, in modo da evitare sia la presenza di vuoti normativi tali da poter costituire una lesione del diritto altrui, sia il rischio di formulare interpretazioni analogiche *in malam partem*.

---

[23] C. CICCIA ROMITO, G. ZICCARDI, *Il GDPR nella micro, piccola e media impresa: un percorso di semplificazione della compliance tra protezione dei dati e adempimenti di legge*, Milano, Giuffrè Francis Lefebvre, 2021.

[24] Il termine "cibernetica" fu coniato dal matematico Norbert WIENER, *Introduzione alla cibernetica. L'uso umano degli esseri umani* (1953), Torino, 1970 – che lo coniò dalla parola greca *kyber*, che significa "timoniere o pilota". La cibernetica studia i meccanismi con cui uomini e macchine comunicano con l'ambiente esterno e lo controllano. Si tratta di una scienza multidisciplinare che interagisce con diverse aree tecnologiche.

[25] F. FAINI, *Regolazione delle società e protezione dei diritti nell'era tecnologica*, in G. CASSANO, S. PREVITI, *Il diritto di internet nell'era digitale*, Milano, Giuffrè, 2020.

Sebbene in altri continenti, come in America del Nord caratterizzata da un forte sviluppo economico e industriale, i legislatori avessero già iniziato a cimentarsi in questa nuova tematica[26], il rapporto fra il diritto penale e le tecnologie informatiche è da pochi decenni all'attenzione della dottrina e della giurisprudenza europea e soprattutto italiana, poiché inizialmente i giuristi tradizionalisti si erano mostrati scettici sulla rilevanza di questo nuovo campo del diritto, che oggi merita sempre più approfondite analisi[27].

Al fine di garantire una tutela giuridica in grado di proteggere le minacce informatiche attuali, è necessario che vi sia una stretta cooperazione e collaborazione multilivello tra gli Stati. Si era posta, perciò, la necessità di stabilire, in maniera puntuale, precisa e soprattutto generale, una disciplina che potesse regolare le nuove fattispecie, le condotte illecite e i criteri di imputazione dei *Cybercrime*, delineando chiaramente quali siano i connotati dei comportamenti e dei "fatti" penalmente rilevanti, che si commettono o manifestano nel Cyberspace, tanto da voler provare a stipulare un sistema di diritti fondamentali di *Internet* pari ad una Convenzione sovranazionale[28].

L'Unione Europea nel 2017 ha invitato esplicitamente «le istituzioni europee a costruire un processo di partecipazione[29] al fine di elaborare una Carta europea dei diritti in *Internet*», all'interno dell'*Internet Governance Forum*, facendo riferimento anche alla Dichiarazione diritti in Internet approvata in Italia[30], in modo da individuare dei principi e valori comuni nonostante la diversità degli ordinamenti giuridici di *civil e*

---

[26] Tradizionalmente si considera punto d'avvio del dibattito dottrinale il volume di PARKER, *Crime by Computer*, New York, 1976.

[27] L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, cit., 2019.

[28] Si sono sviluppati a livello internazionale molteplici iniziative, fra cui i lavori dell'"*Internet Governance Forum*" e la "*Dynamic Coalition* on *Internet Rights* and *Principles*", e a livello nazionale dalla Commissione di studio presieduta da Stefano Rodotà, istituita dalla Presidenza della Camera dei Deputati del Parlamento italiano nel 2014, presentando il 28 luglio 2015 una "*Dichiarazione dei diritti in Internet*", sul sito (e in altre lingue) www.camera.it/*application*/*xmanager*/*projects*/leg17/commissioneinternet/TESTOITALIANODEFINITIVO2015.

[29] In tale direzione l'*European Data Protection Supervisor* (EDPS) ha espresso la necessita di dialogo più etico e multidisciplinare, istituendo nel 2015 l'*European Ethics Advisory Board* e richiedendo nel 2016 l'istituzione di un *Digital Clearing House*, ossia una rete di coordinamento digitale a partecipazione.

[30] F. FAINI, *Regolazione delle società e protezione dei diritti nell'era tecnologica*, in G. CASSANO, S. PREVITI, *Il diritto di internet nell'era digitale*, Milano, Giuffrè, 2020.

common law, e prevedendo un'autorità indipendente che possa vigilare sul rispetto della normativa.

I.3.1 Sviluppi a carattere sovranazionale nell'Unione Europea.

La realtà globale della rete, come già esaminato, implica un mutamento nei confini geografici della regolamentazione; pertanto, è stato fondamentale trovare delle soluzioni a livello sovranazionale sulla protezione dei diritti nel *web* e che possono essere oggetto di violazioni a carattere internazionale, e che hanno bisogno di una tutela globale.

In ambito europeo, l'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) ha realizzato uno studio sulla criminalità informatica nel 1983, elaborando una "lista" comune di reati informatici, con l'obiettivo di applicare e armonizzare la disciplina in tutti gli Stati membri[31]. Nel 1986, l'OCSE pubblicò la relazione "*Computer-Related Crime: Analysis of Legal Policy*", che si occupò di analizzare la normativa esistente e articolò delle proposte di riforma caratterizzate dall'elencazione essenziale della tipologia degli abusi che avrebbero dovuto essere tutelati e puniti ai sensi del diritto penale in tutti i diversi paesi[32].

Nel 1989 il Consiglio d'Europa adottò la Raccomandazione sulla criminalità informatica n. R. (9)89[33], in cui non fu fornita una definizione specifica utile al contrasto del suddetto fenomeno, ma furono individuati, per la prima volta, i reati informatici, secondo una ripartizione in due categorie: la lista "minima" dove furono compresi reati che dovevano essere necessariamente repressi in sede penale a causa della loro gravità, come la frode informatica, il falso in documenti informatici, il danneggiamento di dati e programmi, l'accesso abusivo e la violazione delle misure di

---

[31] G. CORASANITI, G. CORRIAS LUCENTE, S. ATERNO, *Cybercrime, responsabilità degli enti e prova digitale: commento alla legge 18 marzo 2008, n. 48, ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*, Padova, CEDAM, 2009.

[32] C. PECORELLA, *Diritto penale dell'informatica*. Ristampa con aggiornamento, Padova, CEDAM, 2006.

[33] CONSEIL DE L'EUROPE, *Recommandation* n. R (89) 9 "*Sur la criminalitè en relation avec l'ordinateur*", Strasbourg, 1990. Tale raccomandazione riconosce l'importanza del fenomeno della criminalità informatica a carattere transfrontaliero e la necessità di una risposta adeguata alla tutela.

sicurezza del sistema, l'intercettazione non autorizzata, la riproduzione non autorizzata di programmi protetti e di topografie; la lista "facoltativa", invece, lasciava una certa discrezionalità agli Stati membri nell'eventualità di incriminare, con tecniche sanzionatorie differenti (anche di tipo amministrativo), al fine di ottenere un sistema armonizzato, reati considerati di minore gravità, come l'alterazione non autorizzata di dati o programmi (se non costituisse già un danneggiamento), lo spionaggio informatico ossia la diffusione di informazioni legate al segreto industriale, l'utilizzo non autorizzato di un elaboratore o di una rete di elaboratori, l'utilizzo non autorizzato di un programma informatico protetto, abusivamente riprodotto[34]. La stessa fu aggiornata nel 1994, mediante una Risoluzione finale approvata dal Congresso dell'AIDP – *Association Internationale de Droit Pénal* – in cui, a causa dello sviluppo tecnologico crescente di quegli anni e delle relative evoluzioni criminali più numerose, furono introdotte delle modifiche alla Raccomandazione: innanzitutto, si è sollecitato l'uso degli strumenti penali per la repressione dei reati facenti parte della c.d. lista facoltativa anche per la prevenzione di fatti colposi, e si è estesa la Raccomandazione al commercio di codici d'accesso ottenuti illegalmente e per la diffusione di *virus* e *malware*. Tali indicazioni sono state poi recepite dal legislatore italiano nella legge n. 547 del 23 dicembre 1993[35].

La Raccomandazione n. R (95) 13, approvata l'11 settembre 1995 del Consiglio d'Europa agli Stati membri, apre la strada alla successiva Convenzione sul *Cybercrime* del 2001, in quanto si occupa delle problematiche processual-penalistiche legate alla tecnologia dell'informazione, dando evidenza del rischio che i sistemi elettronici di informazione possano essere usati "*for committing criminal offences*": in tale sede il Consiglio dei Ministri del Consiglio d'Europa, richiamando delle precedenti raccomandazioni[36], ha fornito una prima risposta ai crimini informatici commessi

---

[34] G. CORASANITI, G. CORRIAS LUCENTE, S. ATERNO, *Cybercrime, responsabilità degli enti e prova digitale: (...)*., cit., 2009.

[35] *Infra*, § I.3.3.

[36] In riferimento: "la raccomandazione n. R (81) 20 relativa all'armonizzazione delle legislazioni in materia di esibizione dei documenti e in materia di ammissibilità di riproduzione di documenti e di registrazioni informatiche, la raccomandazione n. R (85) 10 sulle commissioni rogatorie per la sorveglianza delle telecomunicazioni, la Raccomandazione n. R (87) 15 recante la regolarizzazione dell'utilizzazione di dati a carattere personale nel settore della politica e la Raccomandazione n. R (89) 9

nell'ambito dell'*Information Technology* (IT), e suggeriva ai governi degli Stati membri di ispirarsi, in sede di modifiche legislative interne, ai principi generali di coordinamento e di adattamento della legislazione di procedura penale tradizionale operando distinzioni in tema di acquisizione, raccolta e trattamento delle prove digitali, come la perquisizione dei sistemi informatici, il sequestro dei dati oggetto di raccolta e le intercettazioni di telecomunicazioni, strumenti fondamentali per le investigazioni sui dispositivi digitali[37]; infatti, dovrà essere prevista una notificazione al soggetto interessato sulla natura della perquisizione e del sequestro, con l'eventuale estensione della perquisizione ad altri dispositivi informatici se necessaria un'azione immediata, anche in presenza di giurisdizione estera, e la possibilità dell'indagato di far ricorso nei diversi gradi del processo[38]. Inoltre, vengono predisposti particolari obblighi per i *service providers*, pubblici o privati, affinché offrano le misure necessarie alle autorità per garantire la raccolta, la salvaguardia e l'integrità delle prove elettroniche durante l'intercettazione e l'identificazione delle comunicazioni dei soggetti ascoltati nello svolgimento di procedure nazionali e di cooperazione internazionale.

Successivamente, all'interno del G8[39], l'*High Tech Subgroup of the G-8's Senior Experts on Trasnational Organized Crime* predisponeva un piano d'azione: tra il 1997 e il 1998 fu istituito il Comitato di esperti sulla Criminalità nel Ciberspazio (PC-CY: *Committee of Experts on Crime in Cyberspace*) con il compito di stilare una bozza di convenzione internazionale per combattere e reprimere la criminalità all'interno dello spazio virtuale, fornendo maggiori delucidazioni in tema di definizioni competenze, sanzioni e responsabilità degli autori dei crimini, in modo da facilitare la cooperazione nelle attività investigative e di accertamento dei *computer crimes*, prevedendo misure

---

sulla criminalità informatica", in G. CORASANITI, G. CORRIAS LUCENTE, S. ATERNO, *Cybercrime, responsabilità degli enti e prova digitale: (…)*., cit., 2009

[37] R. FLOR, *Cyber-criminality: le fonti internazionali ed europee"*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, cit., p. 100.

[38] G. CORASANITI, G. CORRIAS LUCENTE, S. ATERNO, *Cybercrime, responsabilità degli enti e prova digitale: (…)*., cit., 28 ss.

[39] Il G8 è "un forum di otto governi del pianeta Terra: Stati Uniti, Giappone, Germania, Francia, Regno Unito, Italia, Canada, e dal 1998 la Russia, oltre ad un rappresentante dell'Unione Europea. I restanti paesi dell'Unione Europea sono ugualmente rappresentati dalla Commissione Europea ma l'UE non può ospitare vertici o presiederli", definizione tratta dal sito istituzionale italiano del Ministero dell'Economia e delle Finanze, www.dt.mef.gov.it/it/attivita_istituzionali/rapporti_finanziari_internazionali/g8.html.

tempestive atte a salvaguardare gli elementi di prova nei sistemi e nelle reti informatiche che possono essere facilmente distrutti, in considerazione del carattere transnazionale del *cyberspace* e i relativi problemi sul principio di territorialità[40].

Le strutture operative sopraelencate e i relativi principi di fondo hanno fornito un quadro generale e hanno costituito il principale riferimento per la realizzazione della Convenzione europea sulla criminalità informatica, avvenuta quattro anni dopo nel 2001[41].

I.3.2 La Convenzione di Budapest e i relativi Protocolli Addizionali.

L'8 novembre del 2001 è stata approvata, grazie al lavoro dei Ministri degli Esteri degli Stati membri insediati nel Consiglio d'Europa nel 1997, la Convenzione sulla criminalità informatica (*Convention on Cybercrime*), elaborata anche grazie alla partecipazione di Stati extraeuropei, quali Giappone, Sud Africa, Stati Uniti e Canada, aperta alle sottoscrizioni nel 23 novembre dello stesso anno a Budapest, ed entrata in vigore il 1° luglio del 2004[42] quando è stato raggiunto il numero minimo (cinque, tre dei quali appartenenti all'UE) di ratifiche necessarie, secondo quanto previsto dall'art. 36 della Convenzione[43]. Dopo l'entrata in vigore della Convenzione, il Comitato dei Ministri del Consiglio d'Europa, consultati gli Stati Contraenti e dopo averne ottenuto il consenso unanime, può invitare ogni altro Stato ad aderirvi. L'intento della Convenzione era di rafforzare la coesione tra i suoi membri e di intensificare la collaborazione tra gli altri Stati parti della Convenzione, definendo così una politica comune in campo penale volta a proteggere la società contro il *cybercrime*[44]. Infatti,

---

[40] R. FLOR, *Cyber-criminality: le fonti internazionali ed europee"*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, cit., p. 101.

[41] G. CORASANITI, G. CORRIAS LUCENTE, S. ATERNO, *Cybercrime, responsabilità degli enti e prova digitale: (…)*., cit., p. 7.

[42] *Ibidem*, 8 ss.,

[43] *Convention on Cybercrime*, *Article* 36 – *Signature and entry into force*, ¶ 3: "*This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2*".

[44] G. CORASANITI, G. CORRIAS LUCENTE, S. ATERNO, *Cybercrime, responsabilità degli enti e prova digitale: (…)*., cit., p. 10.

nacque l'esigenza di introdurre un "*minimum target*" consistente nella produzione di strategie equipollenti tra gli Stati, in considerazione dell'aterritorialità del campo di azione dei reati informatici, tali da evitare sia possibili offese ai beni giuridici oggetto di tutela, ferma restando la volontà degli Stati ratificanti di voler disciplinare in modo più restrittivo le fattispecie oggetto della Convenzione[45], sia l'eventuale presenza di Stati definiti "paradisi del *cybercrime*" in cui non siano vigenti le regole minime prospettate all'interno della Convenzione e che dovranno essere assicurate dalle legislazioni nazionali[46].

La Convenzione è formata da 48 articoli, suddivisi in quattro capitoli, comprendenti: le definizioni (art. 1) per unificare le nozioni di "sistemi informatici", "dati informatici", "fornitore di servizi" e "dati relativi al traffico"; le misure da adottare in ambito nazionale in tema di diritto sostanziale (artt. 2 – 13), e in tema procedurale relativamente alla disciplina delle prove e dei mezzi per la loro acquisizione e raccolta (artt. 14 - 22); la cooperazione internazionale tramite la semplificazione dello scambio di informazioni e dati in tempo reale tra i vari organi investigativi (artt. 23 – 35); le clausole finali, concernenti disposizioni sull'efficacia della Convenzione, possibili riserve o controversie interpretative/applicative, o su nuovi e futuri emendamenti (artt. 36 – 48)[47].

Considerata un punto di svolta necessario in vista dell'ascesa del progresso tecnologico, la Convenzione costituisce uno degli strumenti internazionali più importanti per l'armonizzazione e il bilanciamento della disciplina nella cooperazione al contrasto della criminalità informatica, e rappresenta un modello per lo sviluppo normativo degli Stati ratificanti (attualmente 66) che si occuperanno e si sono occupati di legiferare in materia.

I punti principali dello sviluppo del processo di integrazione giuridica devono essere realizzati attraverso una serie di misure coordinate: standardizzare la scelta delle

---

[45] F. RESTA, *Cybercrime e cooperazione internazionale nell'ultima legge della legislatura, in Giur. Merito*, 2008, p. 9.

[46] L. CUOMO, R. RAZZANTE, *La nuova disciplina dei reati informatici*, Torino, Giappichelli, 2009, p. 41 ss.

[47] R. FLOR, *Cyber-criminality: le fonti internazionali ed europee*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, cit., 2019.

modalità di azione penale; creare un'efficace relazione a carattere verticale tra Stato e organismi sovranazionali; determinare il livello della tutela penale da erogare ai nuovi beni giuridici da proteggere; evitare che si stabiliscano eccessive restrizioni ad *Internet*, che si caratterizza per l'ampia e libera circolazione di idee e informazioni[48], in considerazione dei principi stabiliti dalla Convenzione europea del 1950 "*per la salvaguardia dei diritti umani e delle libertà fondamentali*[49]".

I principali scopi perseguiti dalla Convenzione sono: armonizzare le infrazioni presenti nel diritto penale nazionale e le disposizioni comuni in materia di cybercriminalità e reati collegati; conferire agli organi investigativi nazionali il potere e gli strumenti necessari per poter perseguire i delitti commessi attraverso un sistema informatico, o per i quali vi siano prove digitali da analizzare, e ciò costituisce una particolare novità, in quanto la normativa si estende oltre i *computer crimes*; garantire la cooperazione internazionale, secondo un regime di contrasto comune, rapido ed efficace, data la natura transnazionale dei reati stessi[50].

Analizzando più nello specifico la Convenzione, osserviamo come essa tenda a colmare quelle lacune in campo definitorio che avevano comportato diverse problematiche in tema di applicazione delle fattispecie esistenti alle nuove forme di offensività legate al *cyberspace* e ai crimini informatici in generale. Infatti, la prima sezione della Convenzione si apre con l'art. 1, che chiarisce nozioni come quella di "sistema informatico", in cui si indica "*qualsiasi rete o dispositivo interconnesso o collegato che compiono, insieme o singolarmente, un'elaborazione automatica dei dati, attraverso l'esecuzione di un programma*", così da delineare un concetto che supera la tradizionale distinzione tra *hardware* e *software,* e ricomprende nuove infrastrutture tecnologiche; per "dati informatici" si intende "*qualunque rappresentazione di fatti,*

---

[48] L. CUOMO, R. RAZZANTE, *La nuova disciplina dei reati informatici*, Torino, Giappichelli, 2009, 40 ss.

[49] In particolar modo, l'art. 8 CEDU riconosce ad ogni persona il diritto al rispetto della vita privata e della corrispondenza, affermando che "non può esservi ingerenza della pubblica autorità nell'esercizio di diritto di tale diritto, se non in quanto tale ingerenza sia prevista dalla legge e in quanto costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, l'ordine pubblico, la prevenzione di disordine o reati, la protezione dei diritti e delle libertà altrui", da G. CORASANITI, G. CORRIAS LUCENTE, S. ATERNO, *Cybercrime, responsabilità degli enti e prova digitale: (...)*., cit., p. 11.

[50] C. SARZANA DI S. IPPOLITO, *La Convenzione europea sulla cibercriminalità*, in *Dir. pen. proc*., 2002, 4, pag. 509 ss.

informazioni o concetti, tali da poter svolgere funzioni ed essere utilizzati da un programma o di un sistema informatico"; il "prestatore di servizi" è "*qualsiasi soggetto pubblico, privato, o un ente, che fornisce, che collabori o che archivi dati per conto di essi, e dia la possibilità di comunicare mediante un sistema informatico*"; per "dati relativi al traffico" si intende "*qualunque informazione o comunicazione realizzata e prodotta attraverso un sistema informatico, osservando il suo percorso dal punto di origine a destinazione*"[51].

Negli articoli successivi (artt. 2 - 13) la Convenzione elenca una serie di adattamenti normativi a livello nazionale riguardanti il diritto penale sostanziale. Nel titolo I sono articolate le fattispecie volte alla protezione del bene giuridico della riservatezza, dell'integrità e della disponibilità dei dati e dei sistemi informatici aggrediti intenzionalmente e abusivamente, che, sebbene già esistenti negli Stati membri, vengono riformate alla luce del carattere globalizzante della criminalità informatica: in particolar modo, la condotta dell'accesso abusivo (del tutto o in parte) ad un sistema informatico viene sanzionata all'art. 2, prevedendo che tutte le parti devono adottare le misure necessarie per sanzionare l'accesso non autorizzato e illegale al sistema, e ai fini dell'integrazione il reato possa essere commesso violando le misure di sicurezza e con intenzioni delittuose; all'art. 3 si stabilisce il reato di intercettazione illecita, ossia quella fatta durante trasmissioni non pubbliche, senza la previa autorizzazione e mediante strumenti tecnici, incluse le emissioni elettromagnetiche di un dispositivo. Il danneggiamento informatico e gli attacchi all'integrità dei sistemi sono previsti dagli articoli 4, 5 e 6 della Convenzione, che puniscono le condotte caratterizzate dal danneggiamento, deterioramento, modifica o soppressione e cancellazione di dati informatici, nonché il grave impedimento del funzionamento del sistema informatico attraverso atti abusivi di introduzione, alterazione, trasmissione, cancellazione di dati informatici, nonché la fabbricazione, vendita e cessione, senza diritto, di dispositivi, *software*, *password* o codici utili all'accesso al sistema, per commettere una delle condotte penalmente rilevanti, o il semplice possesso di tali strumenti, per la commissione di altri reati. Nel titolo II sono disciplinati i "reati

[51] Cfr. art. 1 della Convenzione del Consiglio d'Europa sulla criminalità informatica, Budapest, 23 novembre 2001.

informatici" propri, tipizzandosi, agli articoli 7 e 8, le condotte di falsificazione informatica, definita come la fruizione impropria di dati informatici alterati o non autentici, con l'intenzione di usarli come se lo fossero, e la condotta di frode informatica intesa come la volontà di cagionare un danno patrimoniale attraverso ogni alterazione, introduzione, cancellazione, soppressione di dati informatici o con interferenze in sistemi telematici volte a procurare un ingiusto beneficio economico. Nel titolo III viene disciplinato il reato di pornografia infantile stabilito all'art. 9, che ne sanziona la produzione allo scopo della sua distribuzione, diffusione, offerta o fruizione *online*; inoltre viene uniformata l'interpretazione di "pornografia infantile" comprendendo qualsiasi materiale fotografico, videografico o grafico inequivocabile che coinvolge un minore (sotto ai 18 anni) in un comportamento sessualmente esplicito. Al titolo IV è punita la violazione della proprietà intellettuale, che sancisce che l'ordinamento nazionale deve adottare misure volte alla protezione delle condotte aggressive dei diritti della proprietà intellettuale, in base a quanto previsto dagli accordi commerciali internazionali riguardanti il diritto d'autore[52].

La Convenzione stabilisce all'art. 12 le modalità relative alla responsabilità delle persone giuridiche che possono aver commesso un reato informatico, ovvero possono averlo reso possibile a causa della mancanza di sorveglianza e controllo. Lo Stato deve prevedere la responsabilità (penale, civile o amministrativa[53]) delle persone giuridiche nella realizzazione di un reato informatico, commesso direttamente da parte di un soggetto apicale o sottoposto a tale ente, o che per mancanza di sorveglianza o controllo sia stato comunque realizzato; la Convenzione funge da modello integrativo alla disciplina italiana del d.lgs. 231/2001 aumentando le condotte illecite imputabili agli enti, recepite successivamente all'art. 7 della legge di Ratifica n. 48/2008 con la previsione dell'art. 24 *bis*.

Il titolo V della Convenzione prevede la disciplina del tentativo e del concorso nei reati informatici: l'art. 11 stabilisce che ogni Stato firmatario deve predisporre

---

[52] Artt. 2-10 della Convenzione del Consiglio d'Europea sulla criminalità informatica, Budapest, 23 novembre 2001.

[53] *Convention on Cybercrime, Article* 12 – *Corporate liability*, ¶ 3: "*Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative*.".

misure legislative atte a sanzionare penalmente ogni complicità intenzionale degli articoli sopraelencati, come i casi di tentativo, escludendo però le fattispecie dell'accesso illecito ai sistemi informatici e dell'abuso degli stessi (artt. 2 e 6 della Convenzione). Inoltre, l'art. 13 dispone che le pene previste siano caratterizzate da effettività e siano dissuasive e proporzionate alla gravità della condotta realizzata, in modo che gli Stati nazionali possano decidere di applicare misure esemplari, anche coercitive volte alla privazione della libertà[54].

Nella seconda sezione della Convenzione sono elencate, agli articoli da 14 a 22, le misure procedurali che gli Stati dovranno adottare per l'efficace perseguimento dei reati precedentemente classificati. Si tratta di innovazioni che hanno comportato la revisione di alcune disposizioni già recepite nella Raccomandazione n. R (95) 13 dell'11 settembre 1995 sui problemi di procedura penale legati alla tecnologia dell'informazione. I primi articoli della seconda parte prevedono delle disposizioni comuni sugli aspetti del diritto processuale penale: in particolar modo, l'art. 14 disciplina l'ambito di applicazione delle disposizioni processuali stabilendo che ogni Stato deve adottare le misure legislative necessarie previste dalla Convenzione per le indagini o procedimenti penali specifici relativi ai reati informatici, e per tutti gli altri reati commessi attraverso un sistema informatico e in ogni altro caso di acquisizione di prove digitali di un reato[55]; ciò consente di focalizzare l'attenzione non sulla, ormai chiarita, distinzione tra *computer* e *cyber crimes*, ma sull'esigenza dell'acquisizione della prova nella sua integrità in un ordinamento specializzato in materia che assicuri la disponibilità di apparecchiature sofisticate tali da poter compiere determinate operazioni di raccolta. Tuttavia, è ammessa una riserva agli Stati, previa richiesta espressa, al fine di limitare l'applicazione delle disposizioni previste dalla Convenzione ad una cerchia ristretta di reati, che dovrà essere minore rispetto alla categoria dei reati soggetti alla normativa comune, ovvero nel caso di mancata immediata adozione delle disposizioni comuni previste dalla Convenzione per taluni fornitori di servizi di telecomunicazioni non connessi a reti e sistemi informatici pubblici, in caso di contrasto con la legislazione

---

[54] L. CUOMO, R. RAZZANTE, *La nuova disciplina dei reati informatici*, cit. 41 ss.

[55] G. CORASANITI, G. CORRIAS LUCENTE, S. ATERNO, *Cybercrime, responsabilità degli enti e prova digitale: (...)*., cit., 28 ss.

processuale interna; tuttavia, gli Stati dovranno far in modo di ridurre al minimo l'eventuale riserva, al fine di garantire la piena adozione dell'ordinamento comune. Infatti, l'art. 15 specifica che le misure processuali previste dalla Convenzione devono essere in armonia con le condizioni e le garanzie previste dal diritto nazionale, che devono includere, oltre alle tutele regolate dalle precedenti Convenzioni sui diritti umani, civili, politici e le libertà fondamentali, anche la costituzione di un organo indipendente, di tipo non necessariamente giudiziario, che si occuperà di supervisionare le decisioni statali relative all'applicazione e alle limitazioni del potere o della procedura prevista.

I successivi articoli della Convenzione (16 – 22) si occupano delle procedure relative alla raccolta delle prove digitali nell'espletamento delle indagini informatiche volte al contrasto dei *cybercrimes*, le quali dovranno essere costituite dalle necessarie garanzie giudiziarie in tema di riservatezza e libertà delle comunicazioni. Una delle caratteristiche fondamentali della prova digitale è la velocità con cui viaggia e la volatilità dei dati che facilmente possono essere cancellati, alterati, copiati, conservati, trasferiti o distrutti. Pertanto, il tracciamento di un percorso elettronico finalizzato all'identificazione dell'indagato presuppone la conservazione dei dati che devono essere preservati e raccolti in modo da assicurare la loro integrità secondo le regole e le garanzie del processo penale[56].

All'art. 16, infatti, si richiede che gli Stati si adoperino nell'adottare misure per la conservazione rapida dei dati digitali particolarmente vulnerabili e soggetti a rapida modificazione o cancellazione[57]; la c.d. "*data retention*" è lo strumento con cui le autorità possono reperire i dati informatici archiviati e che saranno custoditi da un soggetto da loro incaricato in modo da preservarne l'integrità per il periodo di tempo stabilito di 90 giorni con possibile rinnovo del termine. L'art. 17, allo stesso modo, amplia la disciplina, prevedendo le misure uniformi che gli Stati ratificanti dovranno adottare per garantire la custodia e la divulgazione d'urgenza dei dati relativi al traffico comunicativo, attraverso provvedimenti specifici per i coloro che li detengono, quali

[56] L. CUOMO, R. RAZZANTE, *La nuova disciplina dei reati informatici*, cit., p. 42.

[57] *Ivi*.

service providers o soggetti privati[58]. Nel titolo III della seconda sezione è previsto, all'art. 18, l'ordine di esibizione alle autorità investigative competenti (*disclosure*) di specifici dati informatici di cui un soggetto è detentore o ha il controllo, conservati all'interno di un supporto informatico; l'ordine in questione è rivolto anche ai fornitori di servizi offerenti prestazioni nel territorio, che saranno obbligati a concedere i dati relativi agli abbonati, ossia dati sensibili indicanti l'identità del cliente e le sue informazioni personali riguardanti l'indirizzo e numero di telefono, il tipo e la durata del servizio utilizzato, gli accordi contrattuali stabiliti, e ogni altra informazione sull'apparecchiatura installata all'interno dell'abitazione[59].

Al titolo IV sono previste disposizioni che richiedono agli Stati di assicurare misure armonizzate per consentire agli organi competenti di procedere alla perquisizione, al sequestro ovvero all'accesso a sistemi, dati e supporti informatici, nonché di adottare regole comuni per la raccolta e registrazione in tempo reale dei dati relativi al traffico, e l'intercettazione e registrazione delle comunicazioni telematiche[60]. Infatti, all'art. 19 della Convenzione sono disciplinati gli ordini di perquisizione e sequestro dei dati informatici archiviati in dispositivi o supporti informatici, includendo gli obblighi di esposizione, per la finalità di dare esecuzione a tali misure, di tutte le informazioni di cui siano in possesso coloro che abbiano competenze sul funzionamento delle apparecchiature.

Il titolo V si occupa, all'art. 20, della *real time tracking* prevedendo l'introduzione di disposizioni che consentano di raccogliere e registrare, utilizzando strumenti tecnici, dati informatici acquisiti in tempo reale relativi a comunicazioni specifiche, eventualmente attraverso la cooperazione del *service provider*, in totale segretezza.

Le intercettazioni sul contenuto sono disciplinate all'art. 21 della Convenzione, che obbliga ogni parte firmataria ad adottare disposizioni legislative o di altra natura,

---

[58] G. CORASANITI, G. CORRIAS LUCENTE, S. ATERNO, *Cybercrime, responsabilità degli enti e prova digitale: (…)*., cit., 30 ss.

[59] *Ivi*, 31 ss.

[60] G. AMATO, *I reati informatici: nuova disciplina e tecniche processuali di accertamento*, Padova, CEDAM, 2010, p. 7.

per consentire alle autorità investigative competenti la raccolta o la registrazione di dati relativi al contenuto delle comunicazioni, mediante strumenti tecnici e anche attraverso l'ausilio dei fornitori dei servizi telematici, così da consentire l'efficace contrasto di gravi infrazioni che dovranno essere definite dal diritto nazionale[61].

Tra i principi generali penalistici, il principio della territorialità risultava essere quello più problematico in relazione ai profili caratterizzanti dei *cybercrimes* che possono essere commessi ovunque e da chiunque in completo anonimato; per questo motivo, per limitare l'area delle fattispecie non punibili, è stato introdotto l'art. 22 sulla giurisdizione penale per cui ogni Stato deve adoperarsi nel predisporre misure necessarie atte a perseguire penalmente le condotte integranti gli illeciti previsti dalla Convenzione, qualora siano state commesse nel proprio territorio, o a bordo di una nave o di un aeromobile, anche quando siano state realizzate da un proprio cittadino, se l'infrazione è penalmente punibile dove è stata commessa, o se l'infrazione non rientra nella competenza territoriale di alcuno Stato; inoltre, è stato creato uno spazio giuridico comune, in base al quale, quando vi siano problemi di competenza tra Stati che ne rivendicano la propria competenza, le parti coinvolte si consulteranno in modo da stabilire come esercitare opportunamente l'azione penale[62].

L'articolo sopra menzionato conduce la III sezione della Convenzione in materia di cooperazione giudiziaria penale tra gli Stati ratificanti (artt. 23 – 35): l'art. 23 impone agli Stati il principio generale di cooperazione ampia nelle indagini o nei procedimenti sui reati collegati a sistemi informatici o telematici, per la raccolta della prova in forma elettronica, tenendo conto delle disposizioni prevista dalla cooperazione e dagli strumenti internazionali sulla materia processuale penale; i principi sull'estradizione sono previsti all'art. 24, riconoscendone l'ammissibilità per i reati informatici stabiliti dalla Convenzione, a condizione che siano punibili in entrambi gli Stati mediante una pena detentiva di un anno o più severa, salva l'applicazione di accordi bilaterali che prevedano una pena minima differente. Inoltre, per garantire la celerità e la semplificazione delle indagini informatiche nella raccolta della prova digitale, sono

---

[61] G. CORASANITI, G. CORRIAS LUCENTE, S. ATERNO, *Cybercrime, responsabilità degli enti e prova digitale: (…)*., cit., 33 ss.

[62] L. CUOMO, R. RAZZANTE, *La nuova disciplina dei reati informatici*, cit., p. 42.

contemplate ulteriori misure di cooperazione, come: la mutua assistenza tra Stati (art. 25) o per le procedure di assistenza giudiziaria in assenza in assenza di accordi internazionali applicabili (art. 27), attraverso strumenti di rapida comunicazione elettronica[63] e previa conferma ufficiale tra gli ordinamenti cooperanti; la trasmissione di informazioni spontanee tra gli Stati (art. 26) e l'eventuale obbligo di usare le informazioni in modo confidenziale o solo in limitate condizioni (art. 28); la rapida detenzione dei dati informatici (art. 29); la diffusione rapida dei dati sul traffico (art. 30); la cooperazione in materia di assistenza autorizzata alla perquisizione, accesso transfrontaliero, sequestro e conservazione, dei dati digitali e delle relative intercettazioni sul contenuto di comunicazioni informatiche trasmesse attraverso elaboratori elettronici (artt. 31, 32, 33 e 34 della Convenzione)[64]. Le disposizioni sopraelencate consentono di tracciare costantemente il dato informatico oggetto delle indagini, e al fine di garantire un'assistenza immediata per l'organizzazione delle prove digitali da raccogliere in relazione ai reati commessi, è stato istituito, all'art. 35, un punto di contatto "rete 24/7", sempre raggiungibile dalle autorità grazie alla procedura accelerata di comunicazione prevista per le Parti ratificanti.

Nell'ultima sezione (artt. 36 – 48) la Convenzione specifica le clausole finali riguardanti le modalità di adesione tramite firma della Convenzione, dell'entrata in vigore e successiva applicazione in conformità al diritto nazionale.

Insieme alla Convenzione sul *cybercrime* è stato adottato un protocollo addizionale di 16 articoli che integra le disposizioni della Convenzione con norme specifiche sulla criminalizzazione di atti di natura razzista e xenofoba commessi e diffusi attraverso sistemi informatici. Il protocollo è stato aperto alla firma il 28 gennaio del 2003, ma è entrato in vigore il 1° marzo del 2006, e ratificato in Italia solo il 9 novembre 2011[65], prevedendo che ogni Stato firmatario debba adottare le misure

---

[63] Si intendono strumenti come fax o posta elettronica, purché tali da garantire l'autenticazione e la sicurezza dei dati rilevati, da G. CORASANITI, G. CORRIAS LUCENTE, S. ATERNO, *Cybercrime, responsabilità degli enti e prova digitale: (…)*., cit., p. 35 ss.

[64] L. CUOMO, R. RAZZANTE, *La nuova disciplina dei reati informatici*, p. 42.

[65] "*Ratifica ed esecuzione del Protocollo addizionale alla Convenzione del Consiglio d'Europa sulla criminalità informatica, riguardante la criminalizzazione degli atti di razzismo e xenofobia commessi a mezzo di sistemi informatici, fatto a Strasburgo il 28 gennaio 2003*", A.C. 3084, in Dossier n° 371 - Schede di lettura, Camera dei deputati, XVII legislatura, 17 novembre 2015.

legislative necessarie per far sì che le condotte incriminate di diffusione del materiale razzista e xenofobo, di minaccia attraverso un sistema informatico, e di denigrazione pubblica, laddove commesse intenzionalmente e ingiustamente (*without right*), costituiscano reato.

Recentemente, è stata valutata la possibilità di costruire nuovi strumenti di collaborazione giudiziaria in ragione delle tipicità della prova digitale, caratterizzate per l'estrema mobilità e fragilità in vista delle nuove invenzioni in campo tecnologico: si pensi ai sistemi di *cloud computing*, in cui i dati informatici sono localizzati nella rete e possono essere recuperati ovunque, rendendo problematica e limitata la cooperazione internazionale, soprattutto con i *service providers*, precedentemente disciplinata dalla Convenzione di Budapest. All'esito dei lavori svolti dal Consiglio d'Europa, e successivamente dal *Cloud Evidence Group*, l'8 giugno 2017 la Commissione per la Convenzione sulla criminalità informatica (T-CY) ha adottato il mandato per la preparazione di un secondo Protocollo alla Convenzione di Budapest, prorogato fino al maggio 2021[66].

In seguito alla pubblicazione, nel novembre 2019, di una bozza di un nuovo progetto di implementazione dei protocolli aggiuntivi alla Convenzione di Budapest sulla criminalità informatica, il Comitato europeo per la protezione dei dati (EDPB) ha adottato nel febbraio 2021 una dichiarazione sull'eventualità di adozione del secondo protocollo, relativa al potenziamento delle misure di cooperazione e divulgazione delle prove elettroniche a carattere transfrontaliero[67]. Tale dichiarazione offre una normativa utile per la diffusione di informazioni relative alla registrazione dei nomi di dominio e per la cooperazione diretta con i fornitori di servizi, prevedendo mezzi validi per ottenere informazioni sugli abbonati e sui dati relativi al traffico, cooperazione immediata in situazioni di emergenza prevedendo squadre investigative comuni sulle

---

[66] S. TOGNAZZI, *Criminalità informatica e cooperazione internazionale: verso il Secondo Protocollo Addizionale alla Convenzione di Budapest*, in L. ALGERI, G. BACCARI, F. CAJANI, C. CONTI, D. CURLOTTI, M. MARRAFINO, W. NOCERINO, S. TOGNAZZI, M. TORRE, *Nuove tecnologie e processo penale. Articoli estratti dalla rivista "Diritto penale e processo"*. Wolters Kluwer, novembre 2021, p. 77 ss.

[67] "*Dichiarazione 2/2021 sul nuovo progetto di disposizioni del secondo protocollo addizionale alla Convenzione del Consiglio d'Europa sulla criminalità informatica (Convenzione di Budapest)*", sul sito di *European Data Protection Board*, sottoscritto dal Presidente del Comitato europeo per la protezione dei dati Andrea JELINEK, www. edpb.europa.eu/system/files/2021-06/statement022021onbudapestconventionnewprovisions_it.pdf

indagini congiunte, e strumenti di assistenza reciproca e tutele per la protezione dei dati personali. Il progetto sembra essere ancora in fase di elaborazione, e tale adozione costituirebbe un importante avvio in termini di progresso tecnologico e di cooperazione tra governo e *service providers*, al fine di proteggere gli utenti dalle minacce cibernetiche, risolvendo i problemi di competenza e giurisdizione, e garantendo al meglio l'efficiente accesso e divulgazione delle prove digitali; infatti, "l'EDPB ribadisce l'importanza di coinvolgere le autorità preposte alla protezione dei dati nel processo di redazione del protocollo addizionale ed è pronto a contribuire e coadiuvare nella redazione del testo provvisorio delle disposizioni (…)"[68]. L'adozione del testo definitivo rappresenterebbe, non la chiusura alla lotta della criminalità informatica che purtroppo è sempre in continua espansione, ma uno spunto essenziale per la riflessione di quei temi tecnologici non ancora inclusi nel Protocollo addizionale[69].

I.3.2.1 Interventi post Convenzione del 2001.

Tra gli interventi successivi di maggior rilievo vi è la Decisione quadro 2005/222/GAI del Consiglio del 24 febbraio 2005, relativa agli attacchi contro i sistemi di informazione, che ha costituito uno dei primi atti adottati a livello europeo per combattere la criminalità informatica, in seguito al recepimento della comunicazione della Commissione nel piano d'azione *eEurope* del 2001[70]; la decisione prevedeva che ogni Stato membro adottasse le misure necessarie, sia per punire penalmente gli attacchi informatici[71], come, ad esempio, l'accesso illecito a sistemi di informazione, sia per migliorare la cooperazione tra le autorità giudiziarie e le altre autorità competenti all'applicazione della legge degli Stati membri, basate al fine di prevenire l'accertamento di attacchi ai danni di sistemi di informazione della criminalità

[68] *Ibidem*, p. 6.

[69] S. TOGNAZZI, *Criminalità informatica e cooperazione internazionale: verso il Secondo Protocollo Addizionale alla Convenzione di Budapest*, cit., p. 86.

[70] G. CORASANITI, G. CORRIAS LUCENTE, S. ATERNO, *Cybercrime, responsabilità degli enti e prova digitale: (…)*., cit., p. 43 ss.

[71] C. SARZANA DI S. IPPOLITO, G. CONSO, *Informatica, internet e diritto penale*. 3. ed., Milano, Giuffrè, 2010, p. 627 s.

organizzata, soprattutto in ambito terroristico[72]; la decisione è stata poi sostituita dalla Direttiva 2013/40/UE, che, oltre ad introdurre ulteriori aspetti definitivi, dispone che siano previste pene più severe per chi realizza attività di intercettazione illecita di comunicazioni informatiche o telematiche, e prevede incriminazioni per le fattispecie caratterizzate dalla diffusione e vendita di *software* e *password*, utili alla commissione dei reati previsti dalla direttiva[73].

Notevole importanza assume la Direttiva 2006/24/CE, in sostituzione alla Direttiva 2002/58/CE, sulla conservazione dei dati di comunicazione elettronica generati o trattenuti da fornitori di servizi di comunicazioni pubbliche o in reti pubbliche di comunicazione. L'obiettivo della direttiva era di armonizzare le disposizioni degli Stati membri in tema di archiviazione dei dati delle conversazioni telefoniche e del traffico telematico trattati dai fornitori di comunicazione elettronica, e di garantirne la disponibilità a fini di indagine e per il perseguimento di reati gravi[74]. Tuttavia, la direttiva in questione fu oggetto di numerose criticità[75] per il mancato rispetto dei criteri di proporzionalità e ingerenza stabiliti dalla Carta dei diritti fondamentali dell'Unione europea, tali da portare la Corte di Giustizia dell'Unione europea, nell'aprile del 2014 a dichiararla l'invalida, e quindi inefficace fin dalla sua entrata in vigore. La sentenza della Corte di Giustizia annulla, per la prima volta, un atto di diritto derivato riguardante il bilanciamento fra le esigenze di repressione ed accertamento dei reati e la tutela dei diritti fondamentali dell'individuo, che possono essere limitati dagli obblighi di conservazione dei dati di traffico telefonico e telematico nella società informazione. La decisione ha avuto un forte impatto anche sugli

---

[72] R. FLOR, *Cyber-criminality: le fonti internazionali ed europee*, da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, cit., p. 112 ss.

[73] V. CONIGLIARO, *La nuova tutela penale europea dei sistemi di informazione, Una prima lettura della direttiva 2013/40/UE del Parlamento europeo e del Consiglio*, in *Dir. pen. cont.*, 30 ottobre 2013.

[74] G. CORASANITI, G. CORRIAS LUCENTE, S. ATERNO, *Cybercrime, responsabilità degli enti e prova digitale: (…)*., cit., p. 53 ss.

[75] Sollecitazioni sollevate dall'alta Corte Irlandese (Corte di giustizia UE, 8 aprile 2014, *Digital Rights Ireland, Seitlinger* e a., cause riunite C-293/12 e C-594/12) e dalla Corte costituzionale austriaca (Corte di giustizia UE, sent. 21 dicembre 2016, *Tele2* e *Watson*, cause riunite C-203/15 e C-698/15).

ordinamenti nazionali e sulle attività investigative che si basano sull'acquisizione di dati e informazioni presso i *service providers*[76].

Tra gli interventi successivi, inoltre, è fondamentale il primo approccio del Consiglio d'Europa all'armonizzazione delle diverse metodologie investigative del 2013: tra il 2010 e il 2013 fu instaurato il progetto di ricerca *CyberCrime@IPA* che, con lo scopo di contrastare la criminalità informatica e di incrementare le competenze delle autorità (forze dell'Ordine, giudici, pubblici ministeri, avvocati, notai e cancellieri), mediante corsi multidisciplinari sulle tecniche di investigazioni digitali, ha proposto un protocollo per il trattamento delle fonti di prova digitale, *l'Electronic Evidence Guide*. La Guida alla prova digitale delinea, in primis i concetti base dell'informatica e dei vari dispositivi digitali, per poi giungere alle fasi del procedimento per repertare correttamente le *digital evidence*, definite come "informazioni generate, memorizzate o trasmesse mediante dispositivi elettronici che possono essere utilizzate in giudizio"[77].

I.3.3 Il crimine informatico e la disciplina in materia di prove digitali nel diritto penale italiano pre Convenzione del 2001.

I primi cenni giuridici riguardanti il crimine informatico risalgono alla fine degli anni Settanta, quando il legislatore italiano è intervenuto sporadicamente per disciplinare il contrasto a nuove condotte aggressive in campo tecnologico[78].

La dottrina e la giurisprudenza italiane furono chiamate a regolamentare in maniera più specifica questo nuovo mondo tecnologico che costituiva diversi problemi a

---

[76] Così, R. FLOR, *la corte di giustizia considera la Direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Riv. trim Diritto penale contemporaneo*, 2014, 2.

[77] Cfr. M. EPIFANI, D. LA MUSCATELLA, C. MEDA, *Guida alla prova digitale: il primo approccio del Consiglio d'Europa all'armonizzazione delle diverse metodologie investigative*, in *Ciberspazio e diritto*, vol. 15, n. 51 (2/3-2014), pp. 375-411.

[78] Come esempi, la legge n. 191 del 1978, che ha introdotto l'art. 420 c.p., sull'attentato ad impianti di elaborazione dati; la legge n. 121 del 1981, per la tutela dei dati archiviati in un sistema informatico; la legge n. 197 del 1991 sull'utilizzo indebito di carte di credito; la legge n. 518 del 1992, a tutela del diritto d'autore nel contrasto alla pirateria informatica. Sul punto R. FLOR, *Cyber-criminality: le fonti internazionali ed europee*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, cit., 2019.

carattere sostanziale e procedurale, in modo da consentire agli utenti di poter usufruire ed operare liberamente tramite le tecnologie a disposizione.

In precedenza, risultava estremamente difficile qualificare il fatto commesso mediante i dispositivi e la rete informatici, in una delle fattispecie già presenti nel nostro codice penale: in risposta vi fu la legge del 23 dicembre 1993 n. 547[79], in seguito alla Raccomandazione europea n. R (95) 13, primo approccio alla criminalità informatica dei legislatori italiani, con titolo "Modificazioni ed integrazioni alle norme del Codice penale e del codice di procedura penale in tema di criminalità informatica". La normativa in questione fu necessaria per scongiurare la continua violazione dei principi di legalità e tassatività, che sarebbero stati lesi se fossero applicate le leggi penali al tempo esistenti; l'inadeguatezza delle norme procurò una lacuna nel diritto penale, tale da rendere esenti da punizione i comportamenti devianti che si concretizzassero in un *computer crime*. Inoltre, l'adozione di questa legge ha consentito di adeguare la normativa interna ai dettami sovranazionali, che invitava gli Stati, nella Raccomandazione del 1995, a reprimere le condotte presenti nella lista "minima" con lo strumento penale, e con strumenti anche di ulteriore natura le fattispecie contenute nella lista "facoltativa".

Non fu inserito uno specifico titolo da destinare esclusivamente ai delitti in materia informatica nel codice penale, diversamente dalle scelte legislative di altri Stati europei[80], ma i nuovi reati informatici furono collocati vicino a figure di reato preesistenti, in considerazione del fatto che le "nuove forme di aggressione" presentavano beni giuridici già oggetto di tutela in diverse parti del codice e quindi, a detta della Commissione ministeriale, già protetti dalle corrispondenti norme esistenti in tema di fede pubblica, patrimonio e *privacy*[81]. Questa scelta fu necessaria per sopperire il dilagante aumento della legislazione penale speciale; tuttavia, l'esperienza del sistema

---

[79] Legge 23 dicembre 1993 n. 547, "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica" in G.U. del 30 dicembre 1993, n. 305.

[80] Si pensi al Portogallo che sviluppo una legge sui *computer crimes*, e alla Francia che introdusse un titolo nuovo all'interno del codice penale, a differenza del legislatore tedesco che ha intrapreso una scelta simile a quella italiana, cfr. M. FARINA, G. GOMETZ, *Elementi di diritto dell'informatica*., Milano, Wolters Kluwer, 2019, p. 244.

[81] C. F. COLOMBO, *Economia criminale: geodiritto, globalizzazione e nuovi canali per i reati d'impresa*, Milano, Wolters Kluwer, 2021, p. 221.

giuridico italiano insegna che, per impedire i danni che possono essere provocati dalle minacce cibernetiche, non serve introdurre singole circostanze aggravanti[82] che modificano attraverso un'interpretazione estensiva le fattispecie penali, poiché queste non consentono la comprensione dei nuovi fenomeni informatici che si trasformano con l'evolversi della tecnologia[83].

Fondamentale è stata l'individuazione del bene giuridico protetto, comunamente definito come ciò che è socialmente rilevante e meritevole di protezione giuridico-penale, in ossequio ai principi di offensività e sussidiarietà che prevedono che vi sia una lesione del bene giuridico tale da essere punita con lo strumento penale in extrema ratio[84]. Nonostante, secondo diversi autori, la riforma n. 547 del 1993 non delinei una nuova figura di bene informatico meritevole di autonoma protezione penale, l'art. 3 della stessa legge estende l'oggetto della tutela "ben oltre «i comuni interessi finali lesi, di natura patrimoniale o privatistica», anche ai «nuovi interessi emergenti, di rilevanza collettiva, dell'affidabilità dei dati informatici in quanto tali nel traffico giuridico"[85].

Siffatto intervento normativo modificò la disciplina penale dei reati informatici "classici", che prevedono espressamente, tra gli elementi costitutivi del reato, riferimenti a strumenti informatici, come frodi informatiche, condotte di falsificazione di documenti, integrità e riservatezza dei dati e delle comunicazioni informatiche[86]: esso stabiliva che i reati in questione potessero essere punibili solo se commessi in reti telematiche chiuse o ad accesso circoscritto, come, ad esempio, per l'accesso a banche dati, o reati riguardanti il diritto d'autore, e pertanto, la normativa del 1993 non era

[82] Come esempi, le circostanze aggravanti introdotte per i delitti di frode informatica (art. 640-ter, nuovo comma 3, c.p.), o di atti persecutori (art. 612-bis, nuovo comma 2, c.p.), o nel caso del reato di diffamazione *online* per cui è giuridicamente applicata la circostanza aggravante dell'utilizzo di "altro mezzo di pubblicità" di cui al comma 3 dell'art. 595 c.p., in riferimento ai siti *web* accessibili a numerosi utenti.

[83] F. BERGHELLA, R. BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, in *Cass. Pen*., 9/1995, 2329; di contro V. MILITELLO, *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*, in *Riv. trim. dir. pen. econ*., 1992, p. 364 ss.

[84] G. FIANDACA, E. MUSCO, *Diritto penale. Parte generale*, Settima edizione, Bologna, Zanichelli, 2014, p. 3 ss.

[85] D. PETRINI, *La responsabilità penale per i reati via internet*, Napoli, Jovene, 2004, p. 41 ss.

[86] G. NERI, *Criminologia e reati informatici: profili di diritto penale dell'economia*, cit., p. 40.

concepita (sebbene possa essere estesa in via interpretativa) per considerare la dimensione globale dei *Cybercrime*[87].

Mentre nel campo procedurale, accanto alle nuove forme di criminalità informatica presenti in Rete a livello globale, si sviluppano nuove tecniche d'indagine, di ricerca e di raccolta delle prove, attraverso l'uso di dispositivi tecnologicamente avanzati tali da esemplificare l'acquisizione delle prove digitali. Le comunicazioni telematiche hanno subito negli ultimi tre decenni una crescita esponenziale, tale da qualificare il nostro secolo come "il secolo dell'informazione". Tra i vari mezzi di comunicazione di cui disponiamo, spicca la "comunicazione telematica polifunzionale"[88], che si realizza attraverso la connessione tra un dispositivo elettronico e una rete a banda a larga. Questo potente mezzo di comunicazione ha inciso sul *modus operandi* dei criminali, che sfruttano la tecnologia per eludere le attività pubbliche di accertamento e repressione, e ciò ha indotto il legislatore ad intervenire attraverso la L. 547/ 1993, che ha introdotto nel codice di rito l'art. 266-*bis*, sulle "Intercettazioni di comunicazioni informatiche o telematiche"[89]. Si ritiene che per "flussi telematici" si debba intendere "la captazione, ad opera di terzi, mediante registrazione diretta e segreta, di comunicazioni o corrispondenze riservate effettuate tramite strumenti telematici o informatici; l'intercettazione è autorizzata mediante decreto del procuratore della Repubblica[90]. L'introduzione, da parte del legislatore, dell'art. 266-*bis* c.p.p., che inserisce nei mezzi di ricerca della prova l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi, per i procedimenti riguardanti i reati presenti nell'art. 266 c.p.p. e ai reati commessi tramite

---

[87] L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*", in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime,* cit., 2019.

[88] E. CATANIA, *Profili essenziali delle intercettazioni telematiche. Dalla tutela costituzionale della segretezza ed inviolabilità di qualsiasi forma di comunicazione alla disciplina ex art. 266 c.p.p.*, in *Diritto.it*, https://www.diritto.it, 27 dicembre 2013.

[89] F. NEVOLI, *Intercettazioni informatiche e telematiche: ricorso ad impianti esterni ed obbligo motivazionale del pubblico ministero*, in *Arch. nuova proc. pen*., 2010, p. 76.

[90] D. D'AGOSTINI (et. al.), *Diritto penale dell'informatica: dai computer crimes alla digital forensic*, Forlì, Experta, 2007, p. 174 ss.

dispositivi informatico-telematici, ha suscitato diversi dubbi: una parte della dottrina[91], presupponendo che la tassatività delle ipotesi in cui è consentita la violazione della segretezza delle comunicazioni non può non essere valida per tutte le "categorie" di intercettazioni, riteneva la scelta del legislatore orientata nel "limitare" l'uso delle intercettazioni informatiche all'accertamento di una determinata categoria di reati compresi nell'elenco dell'art. 266 c.p.p.; un' altra interpretazione più estensiva[92], riteneva, invece, che l'articolo introdotto dalla legge n. 547 del 1993 non dovesse essere interpretato restrittivamente, ma le intercettazioni dovevano essere ammesse sia per i reati informatici "propri" (in cui l'uso del computer è elemento costitutivo), sia per quelli impropri (in cui l'uso del computer integra solo una delle modalità della condotta). A riguardo, la Corte di Cassazione a Sezioni Unite[93] ha risolto la questione attraverso un'interpretazione estensiva di tale disposizione. Inoltre, sempre a riguardo delle intercettazioni è stato previsto nell'art. 268 c.p.p., il comma 3-*bis* per cui, ai sensi di tale articolo, le intercettazioni saranno effettuate attraverso impianti di privati, quando vi è la necessità di usare particolari strutture o apparecchiature, e ciò ha suscitato ulteriori dubbi interpretativi, risolti successivamente dalla Corte di Cassazione[94].

Sono seguite ulteriori integrazioni, avvenute con l'inserimento, nel decreto-legge n. 306 del 1992 e modificato e convertito dalla legge n.356 del 1992, dell'art. 25-*ter* disciplinante le intercettazioni preventive, estendendo l'intercettazione anche alle comunicazioni su sistemi informatici o telematici[95], che possono essere utilizzate su richiesta delle autorità di polizia e dalla Direzione investigativa antimafia, qualora necessarie per le attività di prevenzione e di informazione relative ai delitti di cui all'art.

---

[91] S. ATERNO, *Acquisizione dati traffico ed intercettazioni telematiche*, in S. ATERNO, F. CAJANI, G. COSTABILE, M. MATTIUCCI, G. MAZZARCO, *Computer Forensics e Indagini digitali*, vol.1, Experta, 2011, p. 344.

[92] C. PARODI, *La disciplina delle intercettazioni telematiche*, in *Dir. pen. e proc*., 2003, p. 889.

[93] Cass. Sez. Un., 24 settembre 1998, n. 21, in *Giust. Pen*., p. 614.

[94] Sulle opinioni contrastanti si veda, S. ATERNO, *Acquisizione dati traffico ed intercettazioni telematiche*, cit., p. 357, e F. NEVOLI, *Intercettazioni informatiche e telematiche: ricorso ad impianti esterni ed obbligo motivazionale del pubblico ministero*, in *Arch. nuova proc. pen*., 2010, p. 76., Risoluzione interpretativa in Cass. Sez. I Sent. 28 settembre 1999 n. 5239.

[95] Presentazione del Ministro di Grazia e Giustizia (Conso G.) del Disegno di legge n. 2773, Camera dei Deputati, XI Legislatura, 12.

51 comma 3-*bis* c.p.p.; tuttavia, la novella è stata riformata, a causa degli attacchi terroristici del 2001, e il legislatore ha nuovamente riformato la disciplina delle intercettazioni preventive abrogando l'art. 25-*ter* sopra menzionato[96].

Sostanzialmente la legge 547/1993 ha apportato innovazioni nell'ordinamento nel campo dei *computer crimes*, ma modifiche più significative riguardanti lo sviluppo informatico e il diritto penale sostanziale e processuale saranno disciplinate con la Ratifica della Convenzione di Budapest del 2001.

I.3.4 La legge 18 marzo 2008, n. 48, di ratifica della Convenzione di Budapest.

Il legislatore italiano ha ratificato la Convenzione del Consiglio d'Europa sulla criminalità informatica fatta a Budapest nel 2001 con la legge del 18 marzo 2008, n. 48, ed entrata in vigore il 5 aprile dello stesso anno[97].

La ratifica è il risultato di un difficile processo che ha visto la partecipazione di diverse figure istituzionali: nel 2007 fu istituita, con decreto congiunto del Ministro di Grazia e Giustizia e degli Affari esteri, una commissione interministeriale che aveva il compito di redigere, insieme ad esperti del settore e studiosi della *computer forensics*, uno schema di legge di ratifica, che fu esaminato in aula nel febbraio del 2008, al fine di accelerarne l'adesione prima che vi fosse lo scioglimento delle Camere[98]. Il testo di

---

[96] B. AGOSTINI, *La disciplina delle intercettazioni preventive nel sistema antiterrorismo.*, in Riv. trim. *Diritto penale contemporaneo*, Milano, 2016, p. 143 ss.

[97] Il primo dubbio a cui è stata soggetta l'entrata in vigore della legge 48/2008 ha riguardato un errore del Tribunale del Riesame di Roma, che in una sentenza dell'8 luglio del 2008 ha sollevato la problematica, pienamente risolta dalla Suprema Corte di Cassazione, riguardante la differenza tra l'entrata in vigore della Convenzione – che in base a quanto stabilito dall'art. 36, comma 4, " *(...) la Convenzione entrerà in vigore il primo giorno successivo la scadenza dei tre mesi successivi la data in cui viene espresso il consenso in conformità alle disposizioni dei paragrafi 1 e 2.*" – e l'entrata in vigore della legge 48/2008, che all'art. 14 recita che "*La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale*.", cfr. G. CORASANITI, G. CORRIAS LUCENTE, S. ATERNO, *Cybercrime, responsabilità degli enti e prova digitale: (...)*., cit., p. 73 ss.

[98] Il secondo dubbio sollevato riguarda l'approvazione della ratifica nel regime di *prorogatio* delle Camere, secondo cui, per autorevole dottrina le Camere del 2008 "non avrebbero avuto i poteri per approvare la legge e ratificare la Convenzione in quanto non sussisterebbero i presupposti stabiliti dall'art. 61, comma 2, Cost.", *Ibidem*, p. 75 ss.

legge fu approvato nel 27 febbraio 2008: tale decisione non è stata immune da critiche[99] e dibattiti dei membri della Commissione parlamentare, in quanto alcuni hanno ritenuto che, a causa della celerità con cui è avvenuta l'approvazione, si sia persa l'opportunità di poter disciplinare in modo approfondito e omogeneo i reati informatici, considerando che molte norme riguardanti i reati informatici sono state sviluppate in ragione di una semplice estensione dei reati preesistenti, migliorati e adeguati a seconda delle specifiche disposizioni in materia[100].

La ratifica ha apportato significative novità inerenti al diritto penale sostanziale, alla responsabilità degli enti, e alla disciplina processuale penale, in cui sono state introdotte, per la prima volta in Italia, disposizioni che regolano le esigenze di immodificabilità della *digital evidence* e di genuinità degli elementi di prova, grazie alla modifica degli articoli sulla perquisizione, sul sequestro, e sulla acquisizione e conservazione dei dati su supporti informatici.

Dal punto di vista del diritto penale sostanziale sono sorti diversi problemi riguardanti la scelta, del legislatore italiano, di opporsi ai nuovi sviluppi criminali con strumenti antichi e inadeguati, senza considerare la marcata eterogeneità e i problemi pratico-applicativi delle nuove fattispecie, caratterizzate da una significativa eterogeneità rispetto ai modelli d'origine[101]. Le modifiche sulla parte sostanziale hanno evidenziato l'ampiezza della criminalità informatica, in grado di aggredire una pluralità di beni giuridici estremamente diversi.

---

[99] C. SARZANA DI S. IPPOLITO, G. CONSO, *Informatica, internet e diritto penale*, cit., p. 631 ss., che esamina lo sviluppo della legge di ratifica, avvenuto in modo sbrigativo, tanto da non concentrarsi pienamente nella disamina della materia criminale-informatica disciplinata dalla Convenzione di Budapest. Anche la dottrina ha mosso ulteriori critiche, affermando che vi fossero delle "incongruenze" di tipo interpretativo nelle norme approvate, che sarebbero state superate dalla magistratura, in ragione di evitare l'impedimento dell'approvazione finale della legge di ratifica., Cfr. L. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa* (l. 18 marzo 2008, n. 48). *Profili di diritto penale sostanziale*, in *Dir. pen. proc*., 6/2008, p. 700 ss.

[100] F. RESTA, *Cybercrime e cooperazione internazionale nell'ultima legge della legislatura, in Giur. Merito*, 2008, fasc. 9, pp. 2147-2161.

[101] G. MORGANTE, *Commento a L. 18 marzo 2008, n. 48. Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*. Pubblicata nella Gazz. Uff. 4 aprile 2008, n. 80, in *Legislazione Penale*, 2008, vol. 3, p. 253.

In particolar modo, viene segnalata la modifica compiuta dall'art. 3, comma 1, lett. *b*), della legge n. 48/2008, all'art. 491-*bis* introdotto in precedenza con la legge 547/1993, sull'applicazione della fattispecie della falsità documentali ai documenti informatici (pubblici o privati) aventi valore probatorio, mediante rinvio alla disciplina prevista per gli atti pubblici e per le scritture private. La modifica ha riguardato l'abrogazione della seconda parte della disposizione, che definiva il documento informatico come "qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli"[102]: il legislatore ha riconosciuto la "sopravvenuta inadeguatezza" della definizione, in quanto non era stato compreso il carattere dematerializzato del dato informatico, che può essere slegato dal dispositivo materiale su cui è impresso, e inoltre, non era stata chiarita l'efficacia probatoria dei dati informatici in oggetto[103]. La definizione di documento informatico è stata fornita dall'art. 1, lett. p), d.lgs. 7 marzo 2005 n. 82, nel Codice dell'amministrazione digitale, ed è intesa come "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti". La rilevanza giuridica e l'efficacia probatoria del documento informatico costituivano elementi caratterizzanti tra loro affini, seppur logicamente distinti, affinché potesse integrarsi il reato di falso informatico: infatti, il documento informatico poteva considerarsi "rilevante" solo se capace di incidere su una specifica situazione giuridica, non considerando le informazioni sulla sfera personale che non sono capaci di modificare n qualche modo ciò che è giuridicamente rilevante. Centrale risulta l'efficacia probatoria del documento informatico, inteso come il requisito implicito per i delitti di falso[104]: parte della dottrina afferma che tale requisito dovrebbe avere un'accezione più ampia, in considerazione che il documento informatico merita "una protezione penale "equivalente" a quella apprestata ai documenti tradizionalmente intesi»[105].

---

[102] G. CORASANITI, G. CORRIAS LUCENTE, S. ATERNO, *Cybercrime, responsabilità degli enti e prova digitale: (…)*., cit., p. 81 ss.

[103] G. AMATO, *I reati informatici: nuova disciplina e tecniche processuali di accertamento*, cit., p. 28 ss.

[104] M. SCOLETTA, *Il nuovo regime penale delle falsità informatiche*, in L. LUPARIA, *Sistema penale e criminalità informatica: profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cybercrime (l. 18 marzo 2008, n. 48)*, Milano, Giuffrè, 2009, p. 8 ss.

[105] L. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa, Profili di diritto penale sostanziale*, cit., p. 704.

Ulteriori modifiche hanno avuto ad oggetto le norme sulla falsa dichiarazione o attestazione del certificatore di firma elettronica (art. 495-*bis* c.p.), sulla diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-*quinquies* c.p.), sul danneggiamento informatico (artt. 635-*bis*, 635-*ter*, 635-*quater*, 635-*quinquies* c.p.), e sulla frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-*quinquies* c.p.)[106].

Anche il settore della responsabilità delle persone giuridiche, disciplinato dal d.lgs. 231/2001, ha subito delle modifiche con l'intervento della legge di ratifica: l'introduzione dell'art. 24-*bis* ha esteso alla maggior parte dei reati informatici la responsabilità da reato degli enti, cosicché venisse punito penalmente il soggetto che realizza la condotta, e con una sanzione amministrativa, pecuniaria o interdittiva (a seconda della gravità del reato), l'ente. Tuttavia, non indifferente è stata l'estromissione, dal novero dei rati dell'art. 24-*bis*, delle fattispecie di frode informatica, se il danno non è commesso allo Stato o ente pubblico (art. 640-*ter*), e di falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o qualità personali proprie o di altri, (art. 495-*bis*): l'esclusione appare anomala, considerando che tali delitti sono commessi nell'interesse o/a vantaggio degli enti, da soggetti apicali o subordinati[107].

Le norme processuali sulla ricerca e sulla conservazione della *digital evidence* trovano applicazione in un ambito più ampio rispetto al tradizionale sistema dei reati informatici. Prima dell'entrata in vigore della legge di ratifica, le investigazioni digitali aventi ad oggetto la *digital evidence* erano prive di una disciplina specifica: ciò causava dei problemi pratico-applicativi non indifferenti, in quanto la mancanza di una regolamentazione propria tale da garantire l'attendibilità degli elementi di prova acquisiti mediante operazioni "alternative" inficiava il principio di legalità probatoria, di cui all'art. 111, co. 1, Cost. Lo scopo assunto è stato quello di uniformare, in conformità agli obblighi assunti dall'appartenenza dell'Italia all'Unione europea, le norme del

---

[106] L. CUOMO, R. RAZZANTE, *La nuova disciplina dei reati informatici*, cit., p. 45 ss.

[107] *Ibidem*, p. 50 s.; L. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa* (l. 18 marzo 2008, n. 48). cit., p. 716; C. SARZANA DI S. IPPOLITO, G. CONSO, *Informatica, internet e diritto penale*., cit., p. 658.

codice di rito alle *best practices* di derivazione scientifica[108]. Il legislatore italiano, nel recepire la Convenzione di Budapest, si è ispirato al principio di neutralità tecnologica, non prescrivendo l'adozione di specifiche procedure per l'acquisizione delle evidenze digitali ma, fissando gli obiettivi da raggiungere con le stesse, ossia garantire la conservazione dei dati originari impedendone l'alterazione e assicurando anche la ripetibilità degli accertamenti[109]. Tuttavia, i legislatori sono stati cauti nell'adeguare la disciplina, ricorrendo (forse volutamente) a definizioni piuttosto generiche, e ponendo l'attenzione più al risultato finale da perseguire che al metodo da utilizzare[110], lasciando così numerosi dubbi interpretativi ripresi poi dalla giurisprudenza.

Con riferimento ai profili processuali, il legislatore, con la legge 48/2008, ha modificato il codice di procedura penale intervenendo sul titolo III del libro III, relativo ai mezzi di ricerca della prova, e sul titolo IV del libro V, dedicato alle indagini della polizia giudiziaria, introducendo un "protocollo d'azione della prova digitale", indicando le modalità previste per l'esecuzione in sede di ispezioni (art. 244 c.p.p.) e perquisizioni, ad iniziativa della polizia giudiziaria (art. 352 c.p.p.) o delegate dal pubblico ministero (art. 247 c.p.p.)[111], nel sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni, (art. 254-*bis* c.p.p.), o per accertamenti urgenti (art. 354, co. 2, c.p.p.)[112], prevedendo quindi le regole sulla detenzione e conservazione dei dati informatici, ossia i cardini della *computer forensics*.

---

[108] "La suscettibilità del dato informatico ad essere alterato o modificato, ha imposto al legislatore della Convenzione di Budapest e, di riflesso, a quello italiano, l'indicazione di specifiche modalità per cercare di garantire una tempestiva tutela dell'integrità del dato" in G. CORASANITI, G. CORRIAS LUCENTE, S. ATERNO, *Cybercrime, responsabilità degli enti e prova digitale: (…)*., cit., p. 195; cfr., inoltre, G. ZICCARDI, *L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*", in L. LUPARIA, *Sistema penale e criminalità informatica (…)*, p. 165 ss.

[109] E. TUCCI, *Il diritto di famiglia tra reati informatici, responsabilità genitoriale e digital forensics*, in M. IASELLI, *Investigazioni digitali*, Milano, Giuffrè Francis Lefebvre, 2020, p. 121.

[110] G. ZICCARDI, *L'ingresso della computer forensic nel sistema processualpenalistico italiano: alcune considerazioni informatico-giuridiche*, in L. LUPARIA, *Sistema penale e criminalità informatica (…)*, cit., p. 165.

[111] Artt. 244, co. 2, 247, co. 1-*bis*, c.p.p. e 352, comma 1-*bis*, c.p.p., è necessario: 1) che vengano adottate misure tecniche; 2) che le misure tecniche adottate assicurino la conservazione dei dati originali; 3) che le misure tecniche adottate impediscano l'alterazione dei dati originali.

[112] Art. 354 c.p.p.: 1) l'acquisizione, «ove possibile», deve avvenire mediante copia dei dati; 2) la copia dei dati informatici deve essere effettuata su adeguato supporto; 3) la procedura di acquisizione deve essere condivisa e controllabile; 4) la procedura scelta deve essere tale da assicurare l'immodificabilità dei dati copiati; 5) i dati originali devono comunque essere conservati e protetti adeguatamente.

Secondo autorevole dottrina, la legge di ratifica ha modificato la disciplina investigativa e probatoria, indipendentemente dal reato informatico oggetto del procedimento, considerando «il ruolo fondamentale che la *digital evidence* finisce con l'assumere pressoché in ogni inchiesta criminale […]»[113]. Riguardo alle ispezioni su sistemi informatici o telematici è prescritta l'adozione di misure tecniche modernizzate finalizzate a garantire la conservazione dei dati e ad impedirne l'alterazione: viene riconosciuta la labilità dei dati digitali, che devono essere conservati in modo corretto, affinché ne venga preservata la loro integrità.

È prevista la perquisizione dei dati informatici[114], quando vi sia fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce pertinenti al reato siano contenuti in un dispositivo informatico o telematico, mediante l'adozione di misure tecniche volte a garantirne la conservazione.

In tema di sequestri[115], è stato disciplinato il sequestro di dati informatici, presso i fornitori di servizi informatici, telematici e di telecomunicazioni: la norma in questione prevede un onere di collaborazione tra le parti e dispone che vi debba essere l'acquisizione dei dati informatici mediante copia dell'originale e attraverso una procedura capace di preservare la conformità e l'immodificabilità del dato copiato; inoltre, è possibile sequestrare oggetti di corrispondenza, anche se inoltrati telematicamente.

La norma che ha subito maggiori trasformazioni, nella fase delle indagini preliminari, è l'art. 354 c.p.p. relativa agli accertamenti urgenti su luoghi, cose e persone, con l'eventualità del sequestro da parte della polizia giudiziaria: per le indagini, è disposta la possibilità di procedere alla perquisizione, previo utilizzo delle dovute misure tecniche, di sistemi informatici o telematici per gli ufficiali di polizia giudiziaria, quando ritengono che vi siano dati informatici occultati o tracce pertinenti al reato che potrebbero essere disperse; è disposto, inoltre, che gli ufficiali della polizia giudiziaria adottino le misure tecniche necessarie e impartiscano le prescrizioni che

---

[113] L. LUPARIA, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa* (l. 18 marzo 2008, n. 48). *Profili di diritto processuale*, in *Dir. pen. proc.*, 2008, 6, p. 717.

[114] Art. 247, comma 1-*bis*, c.p.p.

[115] Art. 254-*bis* c.p.p.

assicurino la conservazione del dato, in modo da non impedirne l'alterazione dei dati, delle informazioni, o dei programmi informatici e di sistemi informatici o telematici; è prevista l'immediata duplicazione su supporti adeguati, ove possibile, affinché l'oggetto di indagine non venga alterato durante svolgimento delle operazioni di indagine[116].

Dalla legge n. 48 del 2008 sono state dedotte cinque garanzie fondamentali[117] che dovrebbero essere utilizzate in relazione ai mezzi di ricerca del documento informatico: 1) Il dovere di conservare inalterato il dato informatico originale nella sua genuinità; 2) Il dovere di impedire l'alterazione successiva del dato originale[118]; 3) Il dovere di formare una copia che assicuri la conformità del dato informatico acquisito rispetto a quello originale[119]; 4) Il dovere di assicurare la non modificabilità della copia del documento informatico[120]; 5) La garanzia dell'installazione di sigilli informatici sui documenti acquisiti[121]. La garanzia fondamentale su cui ruota la materia della *digital evidence* è il "dovere di non modificare il dato originale", che dovrà essere inalterato sia nella fase acquisitiva, che nella fase conservativa; pertanto, seguendo la *ratio* del legislatore, bisognerebbe lavorare sul duplicato fatto all'originale, in modo da non comprometterne l'integrità durante il suo utilizzo nell'estrapolazione del dato oggetto di prova, e garantendone sia la genuinità, ossia l'esatta corrispondenza tra il documento originale e quello copiato, che la corretta conservazione, ossia la sua totale

---

[116] L. LUPARIA, *La ratifica della Convenzione Cybercrime,* cit., 717 ss.

[117] Queste garanzie sono il frutto di una complicata ricostruzione interpretativa attuata dalla dottrina e dalla giurisprudenza, in considerazione del carattere frettoloso e non sistematico con cui la legge n. 48 del 2008 è stata approvata, cfr. P. TONINI, C. CONTI, *Manuale di procedura penale*, Ventiduesima edizione, Milano, Giuffrè Francis Lefebvre, 2021, p. 385 ss.

[118] Le prime due garanzie riguardano le ispezioni e nelle perquisizioni disposte dall'autorità giudiziaria (artt. 244, comma 2, e 247, comma 1-bis) e nelle perquisizioni e nel sopralluogo di polizia giudiziaria (artt. 352, comma 1-bis, e art. 354, comma 2), e non appaiono nella richiesta di consegna presso banche (art. 248, comma 2) e nel dovere di esibizione (art. 256).

[119] La garanzia è presente nel sopralluogo ad iniziativa della polizia giudiziaria (art. 354, comma 2) e nel sequestro disposto dall'autorità giudiziaria, in relazione ai dati informatici acquisiti presso i fornitori di servizi (art. 254-bis), e non per tutti i tipi di sequestro. Inoltre, la copia deve essere fatta su un supporto adeguato, che sia vergine e diverso dall'originale. Cfr. S. ATERNO, *Acquisizione e analisi della prova informatica*, in *Dir. pen. proc*., 2008, n. 6, (Dossier*: La prova scientifica nel proc. pen*., a cura di Tonini).

[120] La garanzia appare nel sopralluogo di polizia giudiziaria e nel sequestro disposto dall'autorità giudiziaria, in relazione ai dati informatici presso i fornitori di servizi (art. 254-bis), e non per tutti i tipi di sequestro e per gli altri atti. La garanzia viene realizzata con la c.d. catena di custodia (*chain of custody*) documentando ogni passo del procedimento per l'acquisizione e analisi dei dati.

[121] La garanzia è prevista dall'art. 260 come meramente facoltativa per il sequestro, e non come obbligatoria; ed invece i tecnici affermano che tale adempimento è essenziale per i dati informatici.

immodificabilità. Tuttavia, risulta problematica la qualificazione giuridica dell'attività tecnica di realizzazione della "copia forense"[122]: per poter duplicare il dato originale è necessario comunque intervenire sullo stesso, realizzando, dunque, un'attività di trattamento che potrebbe in qualche modo compromettere il dato originale. Considerando che i dati digitali sono labili, a causa del loro carattere dematerializzato intrinseco, essi non possono essere acquisiti in sede di incidente probatorio, ma è necessario trovare una disciplina che semplifichi e giustifichi l'attività di replica degli stessi, operazione che potrà essere eseguita o meno in base alla tipologia del dato originale in oggetto. Il legislatore individua l'attività "urgente" della polizia giudiziaria e gli "atti a sorpresa" come i momenti acquisitivi di riferimento giuridico della prova digitale: queste attività dovranno comunque essere svolte con "ponderazione"[123], tale da garantire il diritto costituzionalmente garantito di difesa e il principio di parità delle armi nel processo, e soprattutto l'attendibilità oggettiva dell'accertamento che ne determina una eventuale responsabilità penale.

Inoltre, le attività dovranno essere svolte con mezzi idonei tali da preservare l'integrità del dato analizzato, che potranno essere suscettibili di verifica delle controparti: i requisiti, oltre ad essere una garanzia dal punto di vista oggettivo dell'attività tecnica e soggettivo, in relazione al relativo controllo che può essere svolto su di essi[124], sono indefettibili[125], nel senso che in mancanza di uno il dato acquisito non

---

[122] In particolare, è controverso se si possa parlare di accertamento tecnico irripetibile: v. M. DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, 2, p. 295. La giurisprudenza lo nega, v. Cass., Sez. VI, 20 dicembre 2018, n. 15838.

[123] «L'urgenza, dunque, esige meditazione, in ottemperanza a un monito *prima facie* dissonante che *in subiecta materia* doppiamente si impone, involgendo il momento pratico di concreta operatività dell'esplorazione informatica non dilazionabile e, prima ancora, la dimensione teorica del suo astratto inquadramento». Così, E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, in L. LUPARIA, *Sistema penale e criminalità informatica (…)*, cit., p, 136.

[124] M. TORRE, *Aspetti giuridici e tecnici relativi al trattamento della prova digitale nel processo penale. La prova informatica nella legge 18 marzo 2008, n. 48*, in *Informatica e diritto*, 2015, 1-2, pp. 65-104; cfr., P. TONINI, *Il documento informatico: problematiche civilistiche e penalistiche a confronto*, in *Corriere giuridico* (Il), 2012, n. 3, p. 435.

[125] "Il nodo interpretativo scivola sulle questioni inerenti alle metodiche operative e alla possibilità di una loro successiva verifica. Invero, soltanto ove l'azione si uniformi a canoni condivisi, idonei ad assicurare la corretta preservazione del dato digitale ed ex post controllabili, sarà possibile annoverarla tra le autentiche rilevazioni indifferibili suscettibili di compimento unilaterale (artt. 354, comma 2, secondo periodo, 359 e 391-sexies c.p.p.). Per converso, allorché l'azione segua protocolli inadeguati a garantire l'integrità della risultanza ovvero non passibili di successiva verifica, dovrà concludersi che con la rilevazione è stata compiuta un'irreversibile modifica dell'oggetto digitale, il quale ultimo potrà essere

potrà essere considerato come prova dal giudice[126]. La ratio è quella di garantire *standard operating procedures* durante le indagini digitali, indipendentemente da chi le implementa: "trattasi […] di norme precauzionali di buona condotta investigativa che si riflettono sulla successiva utilizzabilità della risultanza digitale sì da imporsi come decalogo operativo per ciascun investigatore 'urgente' di *computer forensics*"[127].

Gli adeguamenti apportati al codice di rito non sono il risultato di una operazione forzata volta al rispetto degli impegni internazionali assunti con la Convenzione di Budapest, ma possono essere considerati il primo passo per l'approfondimento di una materia già considerata da gran parte della dottrina italiana, che da molto tempo esprimeva diversi dubbi riguardanti l'uso dei tradizionali istituti processuali per l'apprensione dei documenti digitali, segnalando come, in mancanza di un provvedimento legislativo, si potesse incorrere nel fenomeno della "deriva tecnicistica"[128].

La legge interviene anche sul codice in materia di protezione dei dati personali, imponendo in capo ai fornitori di servizi telematici, determinati obblighi relativi alla conservazione dei dati di traffico[129]. Inoltre, la legge di ratifica ha inciso sul tema della competenza investigativa sui reati informatici, di cui sono designate le procure distrettuali, in modo da semplificare il coordinamento delle indagini e la formazione di gruppi di lavoro specializzati.

---

preso in considerazione soltanto ove assistito, nella fase di originaria captazione, del contraddittorio preventivo prescritto dall'art. 360 c.p.p.". Così, E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, in L. LUPARIA, *Sistema penale e criminalità informatica (…)*, cit., p. 148.

[126] Opinione non univoca, Cass., Sez. VI, 20 dicembre 2018, n.15838.

[127] M. TORRE, *Aspetti giuridici e tecnici relativi al trattamento della prova digitale nel processo penale. La prova informatica nella legge 18 marzo 2008, n. 48*, cit., pp. 65-104.

[128] Si rimarca il rischio di una "deriva tecnicistica": "Del resto, per quanto sia innegabile che i nuovi settori dell'investigazione pongono sempre l'interprete in uno stato di smarrimento (…) è altrettanto vero che, il più delle volte, i princìpi consolidati della teoria processuale possono essere sufficienti per risolvere le questioni connesse al nuovo fenomeno delle indagini informatiche e che, anzi, l'eccessivo scostamento dallo *ius commune indiciale*, perseguito da chi sostiene la bandiera di quella presunta "autonomia sistematica" delle operazioni di *computer forensics*, finisce col provocare pericolosi scostamenti tecnicisti e fenomeni di aggiramento delle garanzie processuali", in L. LUPARIA DONATI, G. ZICCARDI, *Investigazione penale e tecnologia informatica: l'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, Giuffrè, 2007, p. 136.

[129] Modifiche all'articolo 132 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

Dall'analisi si evince che questo intervento normativo è il risultato della necessità di disciplinare una materia, che avrebbe necessitato di maggiori approfondimenti tecnici, in considerazione delle finalità previste dalla Convenzione di Budapest, consistenti in una maggiore armonizzazione e coordinamento tra gli Stati nel contrasto ai crimini informatici. Inoltre, nella legge di ratifica non sono state introdotte clausole definitorie in attuazione dell'art. 1 della Convenzione, e non si è tenuto conto della Decisione Quadro UE 2005/222/GAI, che contiene disposizioni di contrasto agli attacchi informatici, e ha per oggetto le norme minime di coordinamento in diritto sostanziale.

Nonostante le critiche a cui è stata soggetta, la L. n. 48/2008 ha apportato diversi vantaggi, tra cui quello di aver consolidato e intensificato il rapporto tra natura giuridica dei reati informatici e la peculiarità delle investigazioni digitali, rendendo stringente «l'interazione tra norme penali incriminatrici di parte speciale e istituti processuali, ratificando il ricorso agli strumenti operativi che si andavano affermando nella prassi giudiziaria e nelle aule dei tribunali, unitamente ad un più moderno e consapevole approccio alle problematiche afferenti l'informatica forense»[130]. Il principio fondante della legge di ratifica fu quello di sviluppare un modello unificato per gli Stati membri della Convenzione al fine di combattere la criminalità informatica, rappresentando un punto focale nel contrasto di questo nuovo fenomeno, che ha trasformato le relazioni sociali dell'attualità, di cui «il *Cyberspace* rappresenta solo l'emblema»[131].

I.4 La *Computer Forensics.*

La disciplina della *computer forensics* è internazionale[132] e ha origine negli anni '80 negli Stati Uniti d'America e nasce come uno strumento di ausilio per l'FBI, e altre

---

[130] G. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in L. LUPÁRIA, *Sistema penale e criminalità informatica,* cit., p. 183 s.

[131] L. PICOTTI, *Ratifica della convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Diritto dell'internet*, 2008, 5, p. 448.

[132] Esiste una *soft law* a livello europeo per l'identificazione e la gestione delle fonti di prova digitale, che si occupano di garantire l'autenticità della prova digitale nel processo penale: il manuale (*Electronic Evidence Guide*) fu finanziato dal *Council of Europe* e dall'Unione Europea nel 2013, è disponibile *online* in italiano al seguente indirizzo: http://bit.ly/eeg-ita-form. A livello internazionale, invece, cfr. la norma ISO/IEC 27037:2012 sulle fasi acquisitive delle prove digitali (consultabile al sito: www.iso.org).

agenzie investigative, nell'analisi dei dati digitali utili per recuperare gli elementi di prova al fine di contrastare i reati informatici, e successivamente i *cybercrimes*[133]. La tecnica dell'analisi dei dati digitali è molto vasta e cambia a seconda dell'oggetto analizzato; infatti, la *digital forensics* si differenzia in: *computer forensics* che riguarda dispositivi informatici fisici come computer, fissi o portatili, e di tutte le periferiche di archiviazione di massa con essi utilizzabili; *network forensics*, che si riferisce a parti immateriali come l'analisi di server e di reti; *mobile forensics* che esamina i dispositivi cellulari, specificandosi poi in *PDA* o *SIM forensics* a seconda delle parti o del tipo di dispositivo mobile esaminato.

La *computer-informatic forensics* è «la scienza che studia sia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione, e ogni altra forma di trattamento del dato informatico per essere valutato in un processo giuridico, sia le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici ai fini probatori»[134]. In sostanza, la *computer forensics* può essere esaminata in due livelli: il primo è strettamente correlato ai dati (o *file*) informatici, ossia «qualsiasi rappresentazione di fatti, informazioni o concetti idonei ad essere oggetto di trattamento ed elaborazione da parte di un programma o un sistema informatico»[135]; il secondo livello è pratico e comprende gli aspetti tecnici della disciplina, in cui si analizza la figura dell'investigatore forense che si occupa di ricercare le evidenze digitali con accuratezza, in modo da non inquinare, intaccare o danneggiare la scena del crimine e il relativo materiale probatorio, ai fini dell'ammissibilità nel processo penale[136].

Lo studio della *computer forensics* è diventato un aspetto fondamentale per condurre indagini più efficienti, in quanto l'evoluzione tecnologica è strettamente collegata allo sviluppo del diritto, soprattutto nella risoluzione dei casi pratici: è proprio

---

[133] S. ATERNO, *Acquisizione e analisi della prova informatica*, in *Dir. Pen. Proc*., 2008, p. 61.

[134] M. FERRAZZANO, *L'informatica forense: profili giuridici, tecnici e metodologici nel trattamento della digital evidence,* in T. CASADEI, S. PIETROPAOLI, *Diritto e tecnologie informatiche*, CEDAM, 2021, p. 151.

[135] G. AMATO, *I reati informatici: nuova disciplina e tecniche processuali di accertamento.*, cit., p. 4 ss.

[136] G. GHIRARDINI, G. FAGGIOLI, *Digital forensics.*, Apogeo, 2013.

grazie alla giurisprudenza che sono state gradualmente introdotte e ampliate le indagini informatiche, colmando i vuoti normativi lasciati dalla legge[137].

Un lavoro introduttivo svolto nel 2007 dall'ordinamento italiano ha definito la *computer forensics* legandola ai concetti di "valore" e di "resistenza" dei dati: in particolar modo, per *computer forensics* si intendeva "quella scienza che studia il valore che un dato correlato ad un sistema informatico o telematico può avere in un ambito socio-giuridico". Il concetto del valore del dato, a carattere strettamente tecnologico, era inteso sotto l'aspetto della "resistenza informatica" in ambito processuale, ossia la capacità dell'immodificabilità del dato tale che lo stesso non possa essere in nessun modo contestato in ogni stato e grado, e al contempo possa essere posto a fondamento del libero convincimento del giudice[138].

È necessario che l'evidenza digitale, quale fonte di prova nel processo penale, non venga in alcun modo alterata o modificata, proprio per facilitare la ricostruzione del reato commesso: affinché ciò possa avvenire è importante agire servendosi delle "*Best practices*", ossia le modalità tecniche previste per gli operatori del diritto[139].

I.4.1 Le *Best practices*.

Le c.d. "*Best Practices*" sono delle linee guida[140], non necessariamente formalizzate in dei documenti, che disciplinano le operazioni che devono essere svolte per la corretta acquisizione del dato informatico, in modo che esso possa essere considerato come una prova idonea nel processo penale.

---

[137] M. L. DI BITONTO, *L'accentramento investigativo delle indagini sui reati informatici*, in *Dir. dell'internet*, 2008.

[138] G. ZICCARDI, *L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in L. LUPARIA, *Sistema penale e criminalità informatica (...)*, cit., p. 171 ss.

[139] F. NOVARIO, *Le prove informatiche*, in P. FERRUA, E. MARZADURI, G. SPANGHER (a cura di), *La prova penale*, Giappichelli, Torino, 2013, p. 124 ss.

[140] Con il termine "linee guida" ci si riferisce ad un insieme di raccomandazioni sintetiche, sviluppate sulla base di conoscenze scientifiche valide e aggiornate, affinché un determinato comportamento possa essere appropriato e avere uno standard elevato di qualità. Esse costituiscono la base per l'impostazione del *modus operandi* in ogni organizzazione, nella società e in numerosi campi, tra cui quello giuridico.

L'efficacia delle *best practices* era stata precedentemente sottovalutata dall'ordinamento italiano[141], che ne ha riconosciuto la sua importanza, già affermata a livello sovranazionale (basti considerare le influenze delle legislazioni di *common law* inglesi e statunitensi, e alla Convenzione di Budapest del 2001), solo con la legge di ratifica della Convenzione che ha apportato modifiche ed integrazioni di tipo sostanziale e procedurale, e ha disciplinato gli standard minimi necessari affinché fosse garantita, un'adeguata tutela nella lotta ai *cybercrimes*, ma anche a favorire un maggior rigore nell'acquisizione processuale delle prove digitali e nella sicurezza dei sistemi informatici al pari delle altre nazioni all'avanguardia in questo settore[142].

Esse sono sviluppate dagli organi che si occupano delle investigazioni tecno-scientifiche, mediante elaborazioni teoriche o sulla base di esperienze pratiche: fondamentali sono quelle di Eoghan Casey[143], e nel nostro ordinamento, quelle di Cesare Maioli[144]; vi sono anche delle elaborazioni sviluppate a livello internazionale dalle organizzazioni investigative dell'*United State Secret Service*, dell'*International association of Chiefs of Police*, del *National Institute of Justice* e dell'*Association of Chief Police Officers* inglese[145].

---

[141] Le *best practices* erano paragonate alle linee guida in campo medico-chirurgico le quali, secondo la Suprema Corte di Cassazione, «*costituiscono sapere scientifico e tecnologico codificato, metabolizzato, reso disponibile in forma condensata, in modo che possa costituire un'utile guida per orientare agevolmente, in modo efficiente ed appropriato, le decisioni terapeutiche*» ed attraverso il quale «*si tenta di oggettivare, uniformare le valutazioni e le determinazioni e di sottrarle all'incontrollato soggettivismo del terapeuta*». Cosi, Cass., Sez. IV, 29/01/2013 (dep. 09/04/2013), n. 16237, *Cantore*, Rv. 255105.

[142] D. SHINDER LITTLEJOHN, *Scene of the Cybercrime. Computer Forensics Handbook* / Rockland, MA, Syngress Publishing, 2002.

[143] E. CASEY è un esperto nordamericano della *digital forenser* riconosciuto a livello internazionale grazie ai suoi approfondimenti in materia informatica forense; è autore del libro "*Digital evidence and computer crime*". Egli individua tre competenze specifiche ben distinte che dovrebbero avere i soggetti che compiono un'indagine digitale: *digital crime scene technicians*, ossia coloro che assicurano inizialmente le prove sul luogo del delitto; *digital evidence examiners*, ossia coloro che hanno competenze scientifiche che consentono di processare senza errori le prove rilevate; *digital investigators*, ossia i responsabili del processo di investigazione incaricati di creare un quadro generale della situazione. Cfr. G. ZICCARDI, *L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*", in L. LUPARIA, *Sistema penale e criminalità informatica (…)*, cit., p. 172 ss.

[144] C. MAIOLI è professore ordinario di informatica giuridica presso la facoltà di giurisprudenza di Bologna, autore di 16 monografie ed oltre 200 articoli scientifici e tecnici, ed esperto in materia di *computer science*.

[145] Per un approfondimento cfr. L. LUPARIA DONATI, G. ZICCARDI, *Investigazione penale e tecnologia informatica: l'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, Giuffrè, 2007.

Il legislatore italiano, con la legge di ratifica n. 48/2008, si è focalizzato più sul risultato finale che sulle metodologie tecnico-scientifiche opportune da utilizzare nel campo della *computer forensics*, indicando nelle definizioni i due aspetti fondamentali richiesti, ossia la corretta procedura di copia del dato originale, che deve essere adeguatamente conservato e di cui potrà esserne previsto il sequestro come *extrema ratio*, e la garanzia dell'integrità/non alterabilità del supporto usato nel procedimento di copia[146]. Infatti, la prova digitale è analizzata mediante un procedimento *step by step* in cui ogni passo è fondamentale ed è svolto con particolare cautela per la credibilità dell'intero caso: pertanto, è necessario che l'integrità del dato venga assicurata non solo in riferimento al *bit* informatico, ma anche attraverso quelle strutture logiche che convertono i dati in informazioni leggibili, compreso il *software* in cui questi dati sono visualizzati[147]. Inoltre, è necessario che l'analisi forense venga condotta solo da tecnici del settore, capaci di interpretare in modo chiaro i dati elettronici (parziali o semplici indizi) rilevati nel corso dell'attività: si distinguono le figure degli operatori forensi, che si limitano ad acquisire le prove digitali che verranno consegnate alle forze dell'ordine secondo regole stabilite, dagli investigatori forensi, ossia coloro che grazie alle capacità tecniche forniscono un valido supporto per l'indagine affinché questa abbia successo[148].

È possibile disciplinare un modello generico di *best practices*, articolato in tre fasi: la prima fase riguarda i c.d. "adempimenti preliminari", ossia la selezione accurata degli strumenti tecnici adatti a proteggere e ad isolare la scena del crimine nello stato in cui è stata trovata; successivamente si passa alla seconda fase riguardante la "ricerca dei materiali correlati", individuando ciò che possa essere considerato rilevante per la risoluzione del caso concreto mediante il controllo dei dispositivi e delle apparecchiature digitali, o parti ad esso collegate, e acquisendo le informazioni relative alle *password* degli *account*; l'ultima fase è quella della di "analisi e documentazione dello stato dei luoghi", in cui l'investigatore si accerta dello stato di attività dei

---

[146] G. ZICCARDI, *L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in L. LUPARIA, *Sistema penale e criminalità informatica (…)*, cit., p. 166 ss.

[147] *Ibidem*, 174 ss.

[148] G. CARIA, *Le quattro identificazioni dell'analisi forense: identificazione, acquisizione, analisi, reporting*, in M. IASELLI, *Investigazioni digitali*, Milano, Giuffrè, 2020, p. 4.

computer (del suo contenuto e delle sue componenti periferiche, tra cui *monitor* e memoria RAM) e della rete, rilevando le impronte digitali, salvando eventuali operazioni informatiche e repertando i materiali[149]: successivamente l'investigatore deciderà o di procedere all'eventuale sequestro del computer, oppure di copiare, tramite la funzione di Hash i dati originali che non potranno più essere modificati.

Le investigazioni e le analisi forensi possono essere effettuate secondo una varia selezione di strumenti e tecniche utilizzate per scoprire diverse attività[150]; tuttavia, il modello più comune per l'esecuzione dell'analisi forense è l'ADFM (*Abstract Digital Forensics Model*), composto da nove passaggi: identificazione del tipo di incidente; preparazione, ossia selezione dei metodi e supporti; approccio, ossia stabilire una procedura nella raccolta delle prove digitali che costituisca un minimo impatto sulla vittima; protezione e isolamento delle prove (siano esse fisiche o digitali); collezione, ossia catalogazione nei registri dei duplicati delle prove acquisiti mediante le procedure previste; esame dei dati raccolti; analisi e determinazione delle prove; presentazione e spiegazione delle conclusioni tratte; restituzione delle prove ai legittimi proprietari[151].

I.4.2 *Digital forenser* e attività di *forensics*: le fasi

La storia dell'informatica forense come scienza nasce come computer *forensics* poiché il fenomeno informatico ruotava essenzialmente intorno al *personal* computer; successivamente, con l'avvento di molteplici supporti elettronici in grado di eguagliare le prestazioni di un PC si è coniato il termine *digital forensics* che consiste nell'applicazione di tecniche specifiche idonee a garantire e assicurare la raccolta e la conservazione dei dati attraverso la corretta esecuzione della catena di custodia, nel e rispetto dei diritti individuali presenti nelle attività d'indagine[152].

---

[149] F. NOVARIO, *Le prove informatiche*, in P. FERRUA, E. MARZADURI, G. SPANGHER (a cura di), *La prova penale*, Giappichelli, Torino, 2013, p. 126 ss.

[150] La *digital forensics* può essere utile anche per monitorare e recuperare i dati, per decrittografarli, ma anche per identificare attività e operazioni sospette su diverse piattaforme.

[151] G. CARIA, *Le quattro identificazioni dell'analisi forense: identificazione, acquisizione, analisi, reporting*, in M. IASELLI, *Investigazioni digitali*, Milano, Giuffrè, 2020, p. 4.

[152] M. COPPOLA, *Perquisizioni informatiche e tutela del segreto industriale*, in G. CASSANO, S. PREVITI, *Il diritto di internet nell'era digitale*, Milano, Giuffrè Francis Lefebvre, 2020.

L'esecuzione di un'analisi forense è un tema molto discusso in quanto l'investigatore forense, a causa del continuo sviluppo della tecnologia, deve essere costantemente aggiornato sulle variazioni digitali che incidono sulla struttura dei sistemi operativi, in modo da scoraggiare le eventuali problematiche insorgenti nella validazione delle prove acquisite.

Il primo step del *digital forenser* consiste nell'individuazione dell'origine della *digital evidence*: è un'attività di osservazione, caratterizzata dalla constatazione preliminare delle condizioni in cui si presenta la scena del crimine che dovrà essere esaminata, al fine di documentare, con ogni mezzo, lo stato delle cose prima che l'investigatore possa intervenire. Questa operazione comporta alcune difficoltà[153], in quanto il dato dematerializzato da ricercare può essere contenuto su diversi supporti di tipo fisico, o su parti di questo (USB, *hard disk*, *file log* su *server*), che potrebbero essere nascosti e contenere elementi necessari nella risoluzione del caso. Pertanto, è necessario predisporre un "ordine di volatilità" (*order of volatility*) in cui si stabilisce l'ordine di catalogazione in cui i dati devono essere acquisiti, procedendo da quello più labile a quello più persistente, in modo da evitare la possibile cancellazione o sovrascrittura con altri dati.

La catalogazione avviene seguendo la *Chain of Custody*, ossia una documentazione cronologica e sequenziale che registra il controllo, il trasferimento, l'analisi e la disposizione delle prove fisiche o elettroniche, fondamentale per verificare che esse non siano state manomesse o alterate[154]. La *CoC* documenta in modo chiaro e non equivoco tutto ciò che riguarda la prova, da chi l'ha gestita, alla data e l'ora in cui è stata raccolta e lo scopo del suo trasferimento, preservandone l'integrità e impedendone qualsiasi alterazione che ne impedisca l'ammissibilità in tribunale. Infatti, è fondamentale fotografare, riportando luogo e orario, gli oggetti prima dell'acquisizione

---

[153] "In una realtà dove è difficile delimitare l'area geografica e logica del crimine, può diventare estremamente difficile discernere con precisione quali siano le possibili fonti di prova, quali le aree del sistema da analizzare, quali i dati da elaborare per primi, quali strumenti utilizzare per *il data mining* e per il filtraggio dei dati utili da quelli inutili o falsi o che possono creare confusione e ostacolare le indagini". Cfr., G. ZICCARDI, *Informatica giuridica. Privacy, sicurezza informatica, computer forensics e investigazioni digitali*, Tomo II, Seconda ed., Milano, 2012, p. 265.

[154] G. CARIA, *Le quattro identificazioni dell'analisi forense: identificazione, acquisizione, analisi, reporting*, in M. IASELLI, *Investigazioni digitali*, Milano, Giuffrè, 2020, p. 6.

affinché non possano sorgere dubbi sul percorso temporale degli oggetti precedente all'analisi. Il primo anello della catena di custodia è costituito dal c.d. DEFR - *Digital Evidence First Responder*, ossia colui che ha compiuto il primo sopralluogo nella scena del crimine, di cui si ha corretta e obbligatoria verbalizzazione: infatti, ogni volta che i supporti oggetto di indagini vengono affidati ad un nuovo investigatore, ad un perito, ad un consulente tecnico di parte o all'ufficio dei corpi di reato del Tribunale, nella catena di custodia dovrà essere aggiunta un'informazione.

La seconda fase riguarda l'acquisizione degli elementi di prova digitale: si tratta di uno step molto delicato, in quanto il dato analizzato, che dovrà essere repertato e conservato, dovrà presentare le garanzie dell'inalterabilità e se eseguito erroneamente, potrebbe compromettere l'intero lavoro degli investigatori. La procedura non consisterà in una semplice "copia" del dato ricercato, poiché un'operazione di questo tipo comporterebbe, oltre alla perdita dei c.d. metadati, anche la mancanza di un'esatta corrispondenza contenutistica tra dato originale e copia[155].

L'acquisizione forense avviene mediante copia dell'originale, da parte di persone autorizzate, su un supporto: il duplicato della prova è definito "copia forense", ossia un clone identico all'originale immodificabile, che diventerà la prova nel processo. Tecnicamente, l'integrità dei *files* originali è garantita mediante la c.d. *bit stream image*, ossia una copia-clone (*bit* a *bit*), *on site*, delle informazioni digitali; si tratta di una duplicazione esatta dell'intero supporto originale, contenuta su un disco o su una parte di esso, ricomprendendo anche i *files* cancellati, definitivamente rimossi o nascosti. La copia forense può essere realizzata con diverse modalità previste a seconda del metodo seguito[156], del sistema operativo da analizzare e del *software* utilizzato per l'acquisizione; è fondamentale però che, affinché venga preservata la fonte di prova originale, il supporto di destinazione su cui si effettua la copia dei dati deve essere "vergine" e il supporto sorgente non deve essere alterato durante la fase di acquisizione

---

[155] M. TORRE, *Aspetti giuridici e tecnici relativi al trattamento della prova digitale nel processo penale. La prova informatica nella legge 18 marzo 2008, n. 48*, cit., p. 77.

[156] Metodologicamente il *computer forenser* ha due possibilità: smontare il dispositivo di memorizzazione dal computer analizzato (nella *scena criminis* originale) e collegarlo ad una macchina forense per l'acquisizione, o acquisire l'immagine del disco utilizzando il computer analizzato come sorgente, salvando il risultato su un supporto esterno rimuovibile o su una macchina forense via rete.

dei dati (se così fosse, vi dovrebbe esserne documentazione completa redatta attraverso la *CoC*)[157]. Questo spesso non accade perché quando si collega un supporto di memorizzazione ad un dispositivo al fine di "copiare" dati digitali, si producono comunque delle modifiche ai dati in esso contenuti[158]; perciò per garantire la genuinità e l'integrità dell'evidenza digitale nelle operazioni di acquisizione forense dei dati, è fondamentale prevedere un "blocco" dell'accesso in scrittura sul supporto che contiene i dati da copiare[159].

È necessario che la copia forense non distrugga o alteri in nessun modo l'oggetto originale, come stabilito dalla L. n. 48/2008, nelle modifiche agli artt. 244, comma 2, c.p.p., in tema di ispezioni, con l'art. 254-*bis* riguardante il sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni, e all'art. 256, comma 1, c.p.p., in tema di dovere di esibizione e segreti.

In tema di *digital evidence*, l'acquisizione potrebbe comunque e inevitabilmente provocare modifiche irreversibili sui dati a prescindere dalla volontà e dalla competenza degli operatori, e pertanto, nel rispetto del principio del contraddittorio si rispetterà la regola degli accertamenti tecnici non ripetibili; tuttavia, in maniera eccezionale è consentito il ricorso all'art. 354 c.p.p. in ipotesi di urgenza dell'accertamento, garantendo il contraddittorio postumo sull'elemento di prova digitale acquisito[160].

L'attività di copia forense sarebbe, secondo la giurisprudenza di legittimità, un'attività sempre ripetibile in dibattimento, a patto che i dati originali non vengano in

---

[157] M. TORRE, *Aspetti giuridici e tecnici relativi al trattamento della prova digitale nel processo penale. La prova informatica nella legge 18 marzo 2008, n. 48*, cit., p. 79.

[158] Le modifiche riguardano alcuni elementi del dato, come l'ultima modifica di un *file* (informazioni contenute nel c.d. *file* di *log*), o l'ultimo accesso.

[159] Il c.d. *write blocking* è garantito sia a livello *software*, sia a livello *hardware*. Il blocco in scrittura a livello *software* si ottiene agendo sull'operazione di *mounting* dell'*hard disk* da parte del sistema operativo, ed è una scelta più economica poiché non richiede l'acquisto di particolari dispositivi; quando un *hard disk* viene collegato ad un elaboratore, il sistema operativo lo mette a disposizione dell'utente per effettuare operazioni di lettura e scrittura: a seconda del sistema operativo utilizzato sulla macchina forense di acquisizione, si adottano accorgimenti per impedire il flusso bidirezionale della comunicazione e consentire un accesso in modalità di sola lettura. Un *write blocker hardware* è invece un dispositivo fisico che viene interposto tra l'*hard disk* e la macchina di acquisizione forense; si tratta di dispositivi flessibili, facilmente trasportabili e semplici da utilizzare, e inoltre risultano più comprensibili per interlocutori non tecnici (es. giudice).

[160] M. TORRE, *Aspetti giuridici e tecnici relativi al trattamento della prova digitale nel processo penale. La prova informatica nella legge 18 marzo 2008, n. 48*, cit., p. 83.

nessun modo alterati[161]: sulla base di questa opinione vi è la convinzione che le attività tecniche di *forensics*, se fossero eseguite correttamente e professionalmente, non modificherebbero l'oggetto originale d'analisi dematerializzato[162]; tuttavia un orientamento dottrinale opposto riconosce comunque la natura non ripetibile delle operazioni tecniche di natura digitale a causa della possibilità di alterazione dei *files* ad opera di *software forensics* che non possono essere considerati completamente affidabili[163], e pertanto, nel rispetto del diritto di difesa, queste attività devono essere eseguite nelle forme previste dall'art. 360 c.p.p. dell'accertamento tecnico non ripetibile. Una terza teoria, più moderata, si basa sulla valutazione concreta delle circostanze del caso, ragionando in termini di urgenza piuttosto che di irripetibilità[164]: il compromesso deve basarsi sul fatto che ogni modificazione non è sempre concretamente rilevante e ogni azione accertativa non è sempre insuscettibile del differimento necessario ad assicurare la presenza del difensore; se non potesse realizzarsi il compromesso può soccorrere il controllo esercitabile *ex post* attraverso un'adeguata documentazione che possa verificare l'incidenza effettiva dell'attività accertativa sui risultati conseguiti.

L'acquisizione potrebbe essere critica nel caso in cui i supporti/oggetti da acquisire siano protetti da misure di sicurezza: infatti, anche se in materia di perquisizioni, all'art. 352 c.p.p., comma 1-*bis*, è stabilita la possibilità di perquisire sistemi informatici o telematici, ancorché protetti da misure di sicurezza, da parte degli ufficiali di polizia giudiziaria, potrebbero insorgere delle problematiche nello

---

[161] "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". Cfr. Cass., sez. I, 5 marzo 2009, n. 14511, in C.E.D. Cass., 243150; cfr., Cass., sez. I, 9 marzo 2011, in *Cass. pen.*, 2012, p. 440, con nota a sentenza di M. DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche*, 2012.

[162] Cfr., più chiaramente Cass. pen., sez. I, 26 febbraio 2009, n. 11863, in CED Cass., 2009, n. 243922, secondo cui "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".

[163] Cfr. L. LUPARIA DONATI, G. ZICCARDI, *Investigazione penale e tecnologia informatica: l'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, Giuffrè, 2007. pp. 154 ss.; E. M. MANCUSO, *L'acquisizione di contenuti e-mail*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, Giappichelli, 2019, pp. 531 ss.

[164] A. CHELO, *Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria*, Padova, CEDAM, 2014, p. 68 ss.

svolgimento delle operazioni, soprattutto a causa dell'impossibilità di decrittografare dati presenti in computer spenti, che senza la chiave di lettura, potrebbero essere letti dagli esaminatori forensi attraverso approcci di acquisizione forense *live*[165] o di virtualizzazione[166]. Spetta agli investigatori valutare se concretamente occorra disporre un sequestro materiale dei supporti, o compiere un'acquisizione dematerializzata dei dati, mediante *bit stream image*[167], la cui ammissibilità è soggetta a condizione che si assicuri l'inalterabilità dell'oggetto di analisi e in modo che le parti possano controllare e*x post* l'affidabilità della fonte e la genuinità dell'elemento di prova[168]. In ipotesi di *live data forensics*, questo fondamentale principio potrà ritenersi rispettato quando le procedure utilizzate siano poco invasive e quando le fisiologiche alterazioni prodotte siano documentate[169]; ergo, garanzia fondamentale sarà la controllabilità *ex post*, in

---

[165] La *Live data forensics* è una parte dell'informatica forense, una branca della scienza forense digitale relativa alle prove legali trovate nei computer, caratterizzato da attività di natura tecnica e temporale non ripetibili, in quanto non è possibile realizzare analisi e acquisizione dati *live* senza modificare una parte della memoria del sistema, e in quanto lo stato dell'apparecchiatura durante l'attività ha una complessità tale da non poter essere nuovamente riprodotta. Consultabile *online* su: https://www.marcomattiucci.it/informatica_digitalforensics_liveforensics.php.

[166] G. CARIA, *Le quattro identificazioni dell'analisi forense: identificazione, acquisizione, analisi, reporting*, in M. IASELLI, *Investigazioni digitali*, Milano, Giuffrè, 2020, p. 9.

[167] "L'ispezione informatica (volta alla ricerca di dati presenti su computer) da effettuarsi *on site* si impone, di regola: laddove il computer da acquisire non sia ben identificabile; quando interessino solamente dati intesi come informazioni utili per l'immediato proseguo delle indagini, senza che sia necessaria l'apprensione fisica dell'intera macchina che li contiene; quando, anche laddove ci interessi l'apprensione fisica dell'intera macchina tramite sequestro, essa sia di difficile realizzazione: penso all'ipotesi di scuola di ricercare dati - utili agli investigatori – sui grandi server di società. […]", in F. CAJANI, *La L. 48/2008 ed il reperimento delle fonti di prova da sistemi digitali*, gennaio 2010, consultabile *online* al sito: http://www.marcomattiucci.it/informatica_digitalforensics_l482008.php. Cfr., inoltre, F. NOVARIO, *Criminalità informatica e sequestro probatorio: le modifiche introdotte dalla l. 18 marzo 2008, n. 48 al codice di procedura penale*, in *Rivista di diritto processuale*, Padova, p. 1070.

[168] "Questo costituisce il nucleo insopprimibile del contraddittorio come metodo di accertamento. Al tempo stesso, il contraddittorio esercitabile *ex post* esprime il principio del bilanciamento degli interessi contrapposti, come è stato elaborato dalla giurisprudenza costituzionale in altre occasioni. L'esigenza di ammettere la prova quando vi è «accertata impossibilità di natura oggettiva» (art. 111, comma 5 Cost.) non esclude, ed anzi impone, che sia tutelato quanto meno il contraddittorio "sulla prova" come nucleo insopprimibile della garanzia costituzionale. Il contraddittorio sulla prova non è possibile quando un'acquisizione unilaterale ha modificato l'elemento di prova, o ha impedito di controllare l'affidabilità della fonte e la genuinità dell'elemento. In tal caso, la garanzia del contraddittorio sulla prova già assunta, ma in modo non corretto, risulta preclusa in radice". Così, P. TONINI, *Il documento informatico: problematiche civilistiche e penalistiche a confronto*, in *Corriere giuridico*, 2012, 3, p. 435.

[169] "Intervenire su un sistema *live* significa […] perturbarlo, e svolgere quindi un accertamento che non potrà in nessun caso considerarsi ripetibile. […] limitare l'inquinamento del reperto consentirà di acquisire più informazioni genuine. Le inevitabili alterazioni prodotte, infine, devono essere note e documentabili. […] Quando è possibile scegliere tra acquisizione e analisi, prima si acquisisce e poi si

quanto, “non importa provare ad ogni costo, ciò che conta è avere una prova controllabile, poiché il fine non giustifica i mezzi (la procedura), ma sono i mezzi a legittimare il fine”[170].

Terminata l'acquisizione, è importante provare che la copia forense sia l’esatto clone dell’originale: ciò viene garantito attraverso un "sigillo digitale", ossia la funzione di Hash[171]. Inoltre, l’attività di acquisizione deve poter essere controllabile a posteriori: tecnicamente questo è possibile utilizzando *software open-source*[172], che grazie alle loro caratteristiche permettono ad ulteriori tecnici di verificare la correttezza metodologica delle operazioni[173], considerando la mancanza di contraddittorio *ex ante* con la controparte[174].

La terza fase consiste nel garantire la conservazione dei dati digitali, intesi sia gli originali che le copie forensi. "Conservare" un elemento di natura digitale significa

---

analizza, non il contrario. Anche perché, solitamente, le procedure di acquisizione impattano sul sistema in misura minore rispetto ad operazioni di analisi”, in D. GABRINI, *La L. 48/2008 ed il reperimento delle fonti di prova da sistemi digitali*, http://www.marcomattiucci.it/l482008.php.

[170] M. TORRE, *Aspetti giuridici e tecnici relativi al trattamento della prova digitale nel processo penale. La prova informatica nella legge 18 marzo 2008, n. 48*, cit., p. 88.

[171] L’integrità dei dati oggetto di acquisizione può essere garantita e verificata attraverso l’applicazione di un algoritmo di Hash, che consente di “firmare” in maniera univoca un determinato agglomerato di dati. In particolare, applicando tale algoritmo al contenuto di un *file* o anche ad un intero dispositivo, si ottiene una sequenza alfanumerica di caratteri che rappresenterà l’impronta digitale dei dati memorizzati nel dispositivo; una minima modifica degli elementi acquisiti genererà un *digest* differente rispetto a quello prodotto in sede di acquisizione del contenuto del dispositivo originale, inficiandone il valore processuale. Cfr., G. ZICCARDI, *Manuale breve di informatica giuridica*, Milano, Giuffrè, 2008, pp. 206 e 207.

[172] A differenza dei *software* a “codice chiuso” che non permettevano la valutazione ex post alle parti, dal momento che “non essendo possibile analizzare i codici-sorgente di questi programmi, la validità dei report da loro generati è fondata su un vero e proprio atto di fede”, così Monti, A., *Attendibilità dei sistemi di computer forensic*, in *ICT-Security*, 2003, 9 (disponibile on line: http://www.ictlex.net/?p=287), “i *software open-source* rappresentano un ottimo strumento a basso costo, ed in ambito forense forniscono una grande opportunità perché permettono di trattare il reperto informatico con trasparenza operativa e garanzia, ed offrendo la possibilità di consultare il codice sorgente e conseguentemente di documentare i metodi e le tecniche utilizzate nella acquisizione dei reperti digitali. Tuttavia, non è sempre possibile utilizzare programmi *open-source* per tutte le problematiche.”, così, D. E. CACCAVELLA, *La L. 48/2008 ed il reperimento delle fonti di prova da sistemi digitali*, http://www.marcomattiucci.it/l482008.php.

[173] La controllabilità delle operazioni dipende dalla natura “proprietaria” o “aperta” del *software* utilizzato dall’esperto. Cfr. G. ZICCARDI, *Manuale breve di informatica giuridica*, Milano, Giuffrè, 2008, 51 ss.

[174] M. TORRE, *Aspetti giuridici e tecnici relativi al trattamento della prova digitale nel processo penale. La prova informatica nella legge 18 marzo 2008, n. 48*, in *Informatica e diritto*, 2015, 1-2, p. 81.

garantirne l'integrità[175] (assenza di alterazioni) e documentarne la vita post acquisizione (mediante la c.d. *CoC*).

La conservazione è disciplinata dall'art. 259, comma 2, c.p.p., in tema di custodia delle cose sequestrate, o all'art. 260 c.p.p. riguardante l'apposizione dei sigilli alle cose sequestrate, cose deperibili e distruzione delle cose sequestrate[176]: secondo quanto previsto, l'esaminatore forense che ottiene il mandato di custodia delle copie forensi deve adoperarsi affinché le copie siano protette da manomissioni o visioni da parte di terzi non autorizzati, cercando di usare supporti innovativi e mai utilizzati[177]. Giuridicamente, conservazione e documentazione sono imposte dal principio del contraddittorio nella formazione della prova: l'evidenza digitale deve essere conservata in modo tale da essere preservata da qualsiasi possibile alterazione, per consentire alla controparte di esperire le relative indagini, perizie e valutazioni su un quid identico all'originale[178].

Nel caso in cui sia disposto il sequestro fisico del dispositivo *hardware*, per l'analisi del suo contenuto *post mortem*, l'operatore dovrà imballare il dispositivo ed etichettarlo in modo che la rimozione, anche parziale, segnali una violazione di sicurezza dei sigilli; durante il periodo di custodia è necessario evitare pericoli di inquinamento[179]. Gli archivi dovrebbero prevedere sistemi di protezione fisici con accesso limitato al personale, che dovrà usare abiti idonei alla repertazione, e registrato

---

[175] L'integrità dipende dalle precauzioni adottate in concreto per evitare il danneggiamento dei dati, anche accidentale. I principali problemi di un laboratorio forense sono: la grande quantità di dati; la necessità di trasferimento dei dati; la necessità di conservazione dei dati integri per lungo tempo; la necessità di garantire un accesso riservato ai dati. Per soddisfare queste esigenze è necessario attuare un'accurata strategia di *Data Management*.

[176] All'art. 260 c.p.p, comma 2, è stabilito che "Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria."

[177] G. CARIA, *Le quattro identificazioni dell'analisi forense: identificazione, acquisizione, analisi, reporting*, in M. IASELLI, *Investigazioni digitali*, Milano, Giuffrè Francis Lefebvre, 2020, p. 10.

[178] M. TORRE, *Aspetti giuridici e tecnici relativi al trattamento della prova digitale nel processo penale*, cit., p. 90 ss.

[179] I pericoli possono consistere in un'esposizione a temperature estreme, umidità, raggi UV, vibrazioni durante l'uso od il trasporto, cadute anche accidentali, campi elettromagnetici, cfr. *U.S. Department of Justice, Electronic crime scene investigation: a guide to First Responder*, sul sito https://www.ncjrs.gov/pdffiles1/nij/219941.pdf.

ad ogni apertura. Quando è possibile acquisire i dati *on site* in sicurezza, la conservazione deve essere realizzata a livello *software*, con memorizzazione del clone all'interno di un c.d. *forensic container*[180] e validazione del suo contenuto informativo attraverso un doppio codice Hash.

Esiste una *timeline* di conservazione specifica delle copie forensi, stabilita dal codice in materia di protezione dei dati personali all'art. 132 del d.lgs. n. 196 del 2003, che agli artt. 4-*ter*, 4-*quater* e 4-*quinquies* dispone l'ordine di conservazione, ai fornitori e agli operatori di servizi informatici o telematici, per un periodo non superiore a novanta giorni, dei dati relativi al traffico telematico, escludendo i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive, o per finalità di accertamento e repressione di specifici reati, con possibilità di proroga, per motivate esigenze, per una durata complessiva non superiore a sei mesi; il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-*ter* deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento ed è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità, la cui violazione comporta, salvo che il fatto costituisca più grave reato, l'applicazione delle disposizioni previste dall'art. 326 c.p.; i provvedimenti adottati ai sensi del comma 4-*ter* sono comunicati per iscritto e senza ritardo entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione che, se ne ricorrono i presupposti, li convalida, o in caso contrario i provvedimenti assunti perdono efficacia[181].

Acquisiti i dati, il *digital forenser* deve occuparsi della loro analisi, ricercando ciò che è rilevante ai fini del processo. L'analisi digitale forense è l'esame delle informazioni archiviate elettronicamente (ESI) al fine di individuare i materiali che vengono raccolti durante la fase di identificazione del processo forense digitale.

---

[180] Un *forensic container* è caratterizzato da: controlli interni sulla consistenza dei dati (integrità, indicizzazione, ecc.); informazioni sul caso investigativo (numero del caso, descrizione del supporto, nominativo dell'operatore, ecc.); sistemi di compressione; sistemi di cifratura.

[181] G. CARIA, *Le quattro identificazioni dell'analisi forense: identificazione, acquisizione, analisi, reporting*, in M. IASELLI, *Investigazioni digitali*, Milano, Giuffrè, 2020, p.10 ss.

Attraverso specifici *software* è possibile estrapolare dai *files* delle informazioni utili ai fini delle strategie processuali delle parti. Le norme di riferimento sono diverse a seconda della fase procedimentale in si presenta l'analisi: "in sede di indagine preliminare sarà possibile, alternativamente, procedere ad accertamenti tecnici (artt. 359 e 360 c.p.p.) o ad incidente probatorio (artt. 392 e ss. c.p.p.); in sede dibattimentale, invece, sarà possibile utilizzare lo strumento della perizia (artt. 220 e ss. c.p.p.)"[182].

Nell'analisi di un dispositivo digitale si dovrà procedere partendo dal generale al particolare, fino a ricavare gli elementi utili. Si inizierà con una descrizione sommaria del sistema[183] fino ad arrivare al singolo *file* oggetto di ricerca[184].

Le principali attività che si possono compiere sui dispositivi digitali sono: *text searching*, ossia ricerche di tipo testuale all'interno dei *file* o delle *directory*; *image searching*, riguardante la ricerca delle immagini digitali nei diversi formati possibili; *data recovery*, *data discovery* e *data carving*, consistenti nel dalla memoria del dispositivo di dati cancellati o danneggiati, dati nascosti, cifrati o protetti in altro modo[185]; *metadata recovery*, ossia recupero delle informazioni di sistema poste a corredo della struttura del *file system*, dei *file*, delle cartelle o delle partizioni.

La documentazione prodotta durante l'analisi riporterà: lo scopo dell'esame, persone o oggetti coinvolti; la natura generale dell'analisi; l'intervallo temporale della catena degli eventi, necessario per individuare chiaramente la *timeline* degli eventi su cui si indaga; dati logici e/o cancellati: i dati logici sono quelli presenti e visibili, ma si deve analizzare approfonditamente ciò che è stato cancellato; perdita di dati e/o *unauthorized transfer*: nei casi di furto di informazioni è importante capire se i dati

---

[182] G. VACIAGO, *Profili processuali delle indagini informatiche*, in G. CASSANO, G. SCORZA, G. VACIAGO, *Diritto Dell'Internet: Manuale Operativo: Casi, Legislazione, Giurisprudenza*, CEDAM, Padova, 2013, p. 651.

[183] Sistema operativo, programmi o applicativi presenti, date di installazione, di utilizzo, ultimo accesso e ultimo spegnimento del dispositivo, utenti presenti e relativi privilegi di accesso, ecc. Occorrerà poi verificare la presenza di sistemi ad accesso condizionato o l'uso di *password*, l'eventuale stato di aggiornamento del sistema, nonché il livello di sicurezza presente (*antivirus, firewall* ecc.).

[184] Anche alle aree cancellate, non più utilizzate, non allocate, fino allo *slack space*, ecc.

[185] Sul problema relativo al delicato rapporto esistente tra la crittografia e le garanzie dell'indagato, cfr. G. VACIAGO, *Profili processuali delle indagini informatiche*, cit., 654 ss.

aziendali sono stati caricati su supporti esterni e/o su drive *online*; parole chiave: occorre capire quali sono le parole chiave inerenti a quanto si sta cercando[186].

La fase di *reporting* è l'ultima fase che compie il *digital forenser* e avviene con la presentazione delle prove digitali attraverso delle relazioni tecniche: "questo documento deve descrivere tutte le operazioni compiute per il raggiungimento del risultato dell'analisi del dato digitale; in tale sede, sarà necessario operare uno sforzo di sintesi e di semplificazione, tale da abbattere ogni potenziale *digital divide* tra inquirenti e giudicanti"[187]. Infatti, nonostante i tecnicismi della materia informatica, la relazione deve risultare sintetica, riportando solo ciò che interessa nel giudizio, semplice, in modo da essere compresa anche da coloro che non sono esperti informatici, e asettica, evitando l'inserimento di considerazioni o valutazioni di tipo legale che non siano state espressamente richieste.

Una relazione tecnica forense, affinché possa essere considerata completa e valida dovrebbe contenere: i principi scientifici su cui l'analisi e il repertamento si basano, la catena di custodia dei reperti (formata dai verbali che ne assicurano prelievi, trasferimenti e luoghi di permanenza) e la loro descrizione, le richieste dell'autorità giudiziaria con le autorizzazioni della procura legittimata, la descrizione delle operazioni tecniche svolte in laboratorio e l'esito finale; esito finale e richieste dell'autorità giudiziaria sono gli elementi considerati dai giuristi al fine di trarre conclusioni di ordine legale, mentre le altre semplificano lo studio e l'eventuale ripetizione delle analisi da parte di ulteriori organi tecnici forensi[188].

I.5 La *Mobile Forensics.*

La *mobile device forensics* si occupa del recupero delle prove digitali, durante le indagini tecnico-scientifiche, sui dispositivi digitali dotati di memoria interna e capacità di comunicazione, come telefoni cellulari e *smartphone*.

---

[186] G. CARIA, *Le quattro identificazioni dell'analisi forense: identificazione, acquisizione, analisi, reporting*, in M. IASELLI, Milano, Giuffrè Francis Lefebvre, 2020, p. 17.

[187] G. VACIAGO, *Profili processuali delle indagini informatiche*, cit., p. 653.

[188] G. CARIA, *Le quattro identificazioni dell'analisi forense: identificazione, acquisizione, analisi, reporting*, in M. IASELLI, Milano, Giuffrè Francis Lefebvre, 2020, p. 24.

Se a carattere internazionale vi sono delle linee guida relative alla corretta analisi dei dispositivi mobili, in Italia l'unico punto di riferimento normativo è la L. 48/2008; pertanto, è necessario basarsi sui criteri sovranazionali elaborati dall'ISO (*International Organization for Standardization*) e dall' IEC (*International Electro technical Commission*) n. 27037/2012 e 27042/2015, che stabiliscono i criteri per ricavare la *digital evidence*.

È necessario occuparsi dell'analisi dei dispositivi mobili, in considerazione del loro uso sempre più frequente nella popolazione, e soprattutto perché sono ricchi di documenti utili ai fini dell'indagine[189]: infatti, le tracce digitali rinvenibili sui dispositivi mobili sono molteplici e possono essere differenziate in tre gruppi: dati di comunicazione, che possono includere registri delle chiamate, messaggi sms e altri messaggi del servizio di messaggistica; *file* multimediali contenenti informazioni (*geo-tag*, o dati utili ad esso incorporati sull'identificazione o posizione) oltre alla rappresentazione del *file*; altri dati[190]. Inoltre, le informazioni possono essere recuperate

[189] "Basta porre lo sguardo ai dati che descrivono la diffusione e l'uso di dispositivi mobili in Italia e all'estero per comprendere la centralità della *mobile forensics* nel panorama investigativo. Nel nostro Paese, secondo il Rapporto Italia diffuso da Eurispes, lo *smartphone* si conferma lo strumento tecnologico più diffuso […]. L'utilizzo più frequente resta chiamare ed essere chiamati (99,3%), seguono inviare e ricevere *sms* (85,1%); è elevatissimo l'uso di applicazioni di messaggistica (75,2%), l'abitudine a scattare foto e registrare filmati (69%), a navigare in Internet (66,8%) e a utilizzare i *Social Network* (51,1%). Su scala globale, i dati sono ancora più significativi; il *Global Digital Report* 2019 ha registrato 5,11 miliardi di utenti mobile al mondo, con un incremento di oltre 100 milioni (+2%) rispetto all'anno precedente; 4,39 miliardi di utenti Internet, con un incremento di oltre 366 milioni (+9% rispetto all'anno precedente); 3,48 miliardi di utenti *social*, dei quali 3,26 miliardi accedono alle piattaforme social da mobile, con un incremento di 297 milioni (+10% rispetto all'anno precedente). Questi dati testimoniano inequivocabilmente come la quotidianità di ogni individuo sia costantemente scandita dalla continua interazione con molteplici dispositivi mobili i quali, anche a prescindere dal più o meno specifico carattere informatico di un fenomeno criminale, possono rappresentare preziosi depositari di informazioni di interesse investigativo", cfr. K. LA REGINA, *Le indagini su dispositivi digitali*, in M. IASELLI, *Investigazioni digitali*, cit., 27 ss.

[190] Nello specifico, secondo la classificazione predisposta dalle linee guida dall'Interpol (*Global Guidelines for Digital Forensics Laboratories*), si potranno rinvenire: la cronologia delle chiamate; l'elenco dei contatti; messaggi di testo ed e-mail; *file* multimediali (immagini, video, audio), che possiedono una potenzialità probatoria notevole, in quanto molti *smartphone* incorporano le coordinate GPS della posizione (ma anche data e luogo e *software* utilizzato per modificare l'immagine) nei metadati, c.d. *Exif* (*Exchangeable File Format*); cronologia di navigazione in *Internet* e ricerca di parole chiave; registri di *chat* e *app* di messaggistica (ad esempio, *WhatsApp*, *Telegram*, *Skype*, ecc.), dove è possibile eseguire il *backup* nel *cloud* o nell'archiviazione locale come un computer, e inoltre, rilevano anche le chiamate eseguite attraverso tali applicazioni che permettono al proprietario dello *smartphone* di comunicare con il protocollo IP, senza lasciare traccia nella cronologia delle chiamate del dispositivo; *account* dei *social network* (come *Instagram*, *Facebook*, *Twitter*, ecc.); calendario e note; connessioni (rete mobile, *Wi-Fi*, *Bluetooth*); le mappe (luoghi, indicazioni stradali), e le coordinate GPS dei

anche analizzando la scheda SIM (*Subscriber Identity module*)[191], sulla memoria rimovibile esterna[192] e su quella interna del telefono. La scheda SIM e i dati in essa contenuti sono protetti dal codice PIN, un codice di 4/8 cifre che, se composto erroneamente per tre volte, può bloccare temporaneamente la scheda e rende necessario l'inserimento di un codice PUK (*Personal Unlocking Key*), il cui erroneo inserimento per dieci volte blocca la SIM definitivamente; l'estrazione dei dati avviene attraverso la rimozione della scheda dal telefono e viene effettuata mediante un lettore di SIM *Card*. La memoria esterna rimovibile espande la capienza dello spazio di salvataggio dei dati nei cellulari; l'estrazione e l'analisi sarà compiuta attraverso dei dispositivi come il *write blocker* che consentono l'accesso ai dati digitali del supporto di memorizzazione, prevenendo alterazioni e scritture. Lo spazio di maggiore interesse e difficoltà è rappresentato dalla memoria interna del dispositivo, in quanto i dispositivi mobili sono caratterizzati da differenti tipologie di memoria con caratteristiche diverse in termini di volatilità o non volatilità del contenuto[193]; l'analisi è subordinata alla tipologia del sistema operativo del dispositivo mobile (attualmente sono cinque quali *Android*, *iOS*, *Blackberry OS*, *Windows Mobile*, *Windows Phone*, ma spesso vi sono dispositivi cloni di natura cinese che richiedono particolari procedure per l'estrazione dei dati), e avviene attraverso un pc su cui è installato un *software* per l'estrazione dei dati o con un dispositivo *hardware* dedicato, mediante una connessione sicura tra il dispositivo e lo strumento acquisitivo, preferibilmente via cavo[194].

---

movimenti dell'utente che possono essere acquisite analizzando le applicazioni (*Google Maps*, *Bings Maps* e *Apple Maps*); *software* (elaborazione dei documenti, PDF ecc.), *Ibidem*, 31 ss.

[191] La scheda SIM (*Subscriber Identity module*) è una componente rimovibile del dispositivo da cui è possibile ricavare le principali informazioni relative al sottoscrittore del servizio mobile, tra cui il codice ICCID (*Integrated Circuit Card Identification*) che identifica in modo univo la SIM; il codice IMSI (*International Mobile Subscriber Identity*), che identifica il numero univoco dell'utente nella rete del suo operatore; o le informazioni sulla localizzazione relative alle comunicazioni vocali (*Location Area Information*) o alle trasmissioni di dati (*Routing Area Information*), *Ibidem*, 34 ss.

[192] "Si tratta di schede generalmente utilizzate per la memorizzazione di *file* multimediali, come ad esempio audio, video, immagini e documenti che, anche in ragione delle dimensioni ridotte, possono costituire uno strumento privilegiato per l'occultamento, il trasferimento e lo stoccaggio di dati", *ivi*.

[193] "Un esempio di memoria volatile è la RAM, considerata la componente che crea le maggiori difficoltà di analisi, che può contenere importanti informazioni ai fini investigativi; la ROM, invece, è una memoria non volatile che possiede caratteristiche di maggiore persistenza e i dati in essa contenuti permangono anche in mancanza di alimentazione", *Ibidem*, 35 ss.

[194] Cfr. K. LA REGINA, *Le indagini su dispositivi digitali*, in M. IASELLI, *Investigazioni digitali*, 2020.

Le fasi di repertazione della prova digitale sono simili a quelle previste per la *digital* e *computer forensics* e si dividono in: individuazione; acquisizione e preservazione; analisi; *reporting*.

La *mobile forensics analysis* presenta alcune criticità, in quanto attualmente non si può parlare di una vera e propria analisi forense, ma ci si riferisce ad analisi di tipo *forensically sound*[195]. Tali dispositivi non permettono di effettuare analisi di tipo *post mortem*: in considerazione dei principi di non alterabilità e cristallizzazione dell'evidenza digitale, non risulta possibile acquisire prove informatiche senza interagire, anche limitatamente, con il loro sistema operativo. Le metodiche utilizzate per tali dispositivi minimizzano le interazioni dell'operatore, anche se per tali attività, non essendo garantita la ripetibilità dell'atto, si deve operare in base ai dettati dell'art. 360 c.p.p.[196]

[195] La letteratura americana individua il concetto di *foreniscally sound*, per indicare le procedure di *computer forensics* che, per varie motivazioni, legate sia all'urgenza di compiere determinati atti, o alla tipologia di evidenze da repertare, tendono alla corretta applicazione delle *best praticies*, pur non potendo garantire l'assoluta ripetibilità ed integrità. È questo il caso, ad esempio, della *mobile forensics* o delle attività di ricerca della prova su dispositivi *embedded* (ossia sistemi elettronici a microprocessore progettati per una determinata applicazione o non riprogrammabili dall'utente per altri scopi, spesso con una piattaforma *hardware* ad hoc, integrati nel sistema che controllano e in grado di gestirne tutte o parte delle funzionalità).

[196] M. TONELLOTTO, *Evidenza informatica, computer forensics e best practices*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, 8.2, (2014), p. 93 ss.

CAPITOLO II

LE INDAGINI INFORMATICHE E I MEZZI DI RICERCA DELLA PROVA

SOMMARIO: II.1 Il documento informatico tra prova scientifica e processo penale. - II.2 I mezzi di ricerca della prova nel codice di procedura penale. - II.3 Le ispezioni informatiche. - II.3.1 Il labile confine tra l'ispezione informatica e la perquisizione digitale. - II.3.2 L'ispezione informatica tramite virus, e i relativi profili problematici. – II.4 Le perquisizioni informatiche. - II.5 Il sequestro probatorio informatico. – II.6 Le intercettazioni di conversazioni o comunicazioni. II.6 Le intercettazioni di conversazioni o comunicazioni. - II.6.1 Principi costituzionali e definizioni. - II.6.2 La normativa delle intercettazioni comune alle vecchie e alle nuove riforme. - II.6.3 Le riforme. - II.6.3.1 La riforma Orlando, non entrata in vigore. - II.6.3.2 Gli aspetti essenziali della riforma c.d. Bonafede. – II.6.3.3 Le norme sulle intercettazioni mediante captatore informatico.

II.1 Il documento informatico tra prova scientifica e processo penale.

La formazione del libero convincimento del giudice e la ricostruzione della "verità processuale"[197] possono essere esperite solo con mezzi conformi alla legge, ossia le prove, disciplinate dal terzo libro del codice di procedura penale, che vi ricomprende la disciplina dei "mezzi di prova" nel titolo II e dei "mezzi di ricerca della prova" nel titolo III. Nel sistema attuale processual-penalistico, la formazione della prova avviene attraverso un procedimento costituito da tre fasi importanti, talvolta distinguibili, altre volte strette da una consequenzialità cronologica tale da poterle confonderle tra loro, quali: ammissione (attraverso una prima deliberazione del giudice sulla scelta dei mezzi da ammettere), acquisizione (accertamento della verità materiale attraverso una sequenza di atti giuridicamente regolata) e valutazione della prova (momento del convincimento del giudice)[198].

---

[197] "La verità formale o processuale che emerge dal processo, si costruisce attraverso un percorso conoscitivo irto di regole che riguardano l'ammissione, l'assunzione e la valutazione delle prove che fatalmente ne condizionano la ricerca. A ben guardare i limiti che regolano l'ammissibilità delle prove nel processo rappresentano, a livello epistemologico, un ostacolo alla conoscenza della verità. Inoltre, la regola processuale dell'autorità della cosa giudicata pone fine alla ricerca della verità processuale e le attribuisce la qualità di verità "assoluta". Viceversa, la verità storica non può avere l'autorità della cosa giudicata.", cfr. Rosoni, I., "*Verità Storica e Verità Processuale. Lo Storico Diventa Perito*." *Acta Histriae*, vol. 19, no. 1-2, 2011, p. 129 ss. Inoltre, con l'art. 187 c.p.p. il legislatore ha definito l'oggetto della prova, in modo da evitare che "l'attività probatoria possa arbitrariamente orientarsi verso qualunque obiettivo di ricostruzione della "verità storica" (secondo una logica inquisitoria estranea all'ispirazione del codice), circoscrivendone, invece la destinazione verso temi coessenziali all'oggetto stesso del procedimento, inteso nella sua complessità." in G. CONSO, V. GREVI, M. BARGIS (a cura di), *Compendio di procedura penale*, X ed., Torino, 2020, p. 265 ss.

[198] P. MOSCARINI, *Lineamenti Del Sistema Istruttorio Penale*, Giappichelli, Torino, 2017, p. 26 ss.

Le prove possono dividersi in differenti classificazioni, una tra queste è la distinzione tra prove rappresentative (come testimonianza e documenti), e prove critiche o indiziarie[199]. Spesso si ritiene che, nonostante l'importanza del principio di oralità tale da permettere il massimo della dialettica processuale, i documenti e le registrazioni "forniscano prove più sicure delle parole parlate, specie in tribunale"[200], in quanto "il sapere scritto è anche il sapere per eccellenza"[201]; tuttavia, anche il documento può presentare degli errori, causati sia dall'essere umano, sia dagli stessi dispositivi, problematiche che riecheggiano nel rapporto complicato tra scienza e processo[202].

Infatti, il legislatore del codice di procedura penale si è occupato di dare omogeneità alla disciplina della prova documentale, prevista dal capo VII, tra i mezzi di prova, inserendo nel 2008 il "documento informatico", proprio perché il progresso tecnologico ha dato al documento, e in particolar modo al documento informatico, un ruolo centrale, in considerazione dell'evoluzione dei rapporti sociali che nascono e si sviluppano attraverso i dispositivi digitali, e attraverso cui si acquisiscono le *digital evidence*. È importante, quindi, in considerazione dei principi stabiliti dall'art. 111 Cost., chiarire il concetto di documento informatico, affinché venga riconosciuto all'imputato "il diritto di essere messo a confronto con il dato informatico nel suo aspetto genuino, senza alterazioni"[203].

L'art. 234, comma 1, del codice di procedura penale, stabilisce "l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo". In altre parole, il codice riunisce nella nozione di documento, inteso come la «rappresentazione di un fatto che è incorporata su di una base materiale con un metodo analogico o digitale»[204],

---

[199] Per un approfondimento sulle classificazioni delle prove e la distinzione tra prova rappresentativa e prova indiziaria o critica, si rinvia a P. MOSCARINI, *Lineamenti Del Sistema Istruttorio Penale*, Giappichelli, Torino, 2017, p. 10 ss.

[200] W. J. ONG, *Oralità e scrittura. Le tecnologie della parola*, Bologna, 1986, p. 139.

[201] G. R. CARDONA, *Antropologia della scrittura*, Torino, 2009, p. 102.

[202] Cfr. O. DOMINONI, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Milano, 2005, p. 11; P. TONINI, *Dalla perizia "prova neutra" al contraddittorio sulla scienza*, in *Dir. pen. proc*., 2011.

[203] Così, P. TONINI, *Documento informatico e giusto processo*, cit., p. 406.

[204] P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 365.

diverse tipologie dalla comune funzione rappresentativa[205]. Infatti, il documento informatico «può essere definito come quella rappresentazione di un fatto che è incorporata in una base materiale con un metodo digitale (es., un *file word* o MP3, un messaggio *WhatsApp*, una pagina di *internet*)»[206]. Il fatto rappresentato che sarà ricostruito nel processo, e che costituirà oggetto della prova, verrà incorporato su una base materiale, tale da poterne garantire la conservazione «al fine di riprodurla quando occorra»[207]; l'incorporazione può essere compiuta attraverso il metodo analogico o digitale, differenziati tra loro per la caratteristiche del metodo digitale di essere "dematerializzato"[208] e quindi di essere, a differenza del metodo analogico, staccato dal supporto fisico in cui è incorporato, rendendo più agevole il trasferimento su vari dispositivi dei dati informatici, rendendoli unici[209] e in alcun modo intaccati[210].

Inoltre, il metodo di incorporamento digitale che distingue e costituisce il documento informatico può essere considerato una prova scientifica[211]; infatti, essendo

---

[205] Cfr. F. ZACCHÈ, *La prova documentale*, in G. UBERTIS, G. P. VOENA, (diretto da), *Trattato di procedura penale*, XIX, Milano, 2012, p. 20.

[206] Così P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 367.

[207] "La base materiale sulla quale è incorporata la rappresentazione può essere la più varia. È sufficiente l'idoneità a conservare la rappresentazione al fine di riprodurla quando occorra.", *Ibidem*, p. 367.

[208] La dottrina preferisce la dematerialità, piuttosto che l'immaterialità, in quanto il documento digitale è caratterizzato da una autonomia, essendo legato al supporto soltanto in modo ideale. A riguardo cfr. nel paragrafo dedicato da P. TONINI, *L'evoluzione delle categorie tradizionali: il documento informatico*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, cit., p. 1312 ss.

[209] In tema di "unicità", F. M. MOLINARI, *Questioni in tema di perquisizioni e sequestro di materiale informatico*, in *Cass. pen*., 2012, n. 2, pp. 696-716.

[210] «Noi sosteniamo che l'incorporamento su di una base materiale può avvenire sia con modalità analogiche, sia con modalità digitali. Quando avviene con modalità analogiche, l'incorporamento di una rappresentazione utilizza grandezze fisiche che sono variabili con continuità e che, ci dicono gli scienziati, sono proporzionali all'intensità del fenomeno da riprodurre. L'incorporamento analogico è definito "materiale" perché la rappresentazione esiste soltanto se è incorporata su quella determinata base materiale. La rappresentazione non può essere trasferita indipendentemente dal supporto; altrimenti, occorre farne una fotocopia, che si distingue dall'originale perché è incorporata su una differente base materiale. Se l'originale o la copia sono falsificati, lo si accerta con una perizia, perché resta una traccia sul supporto. Tutto questo avviene per il documento tradizionale, di tipo analogico. Viceversa, quando la rappresentazione di un fatto è incorporata con modalità digitali, l'incorporamento utilizza entità variabili con discontinuità, e cioè numeri in forma binaria. Con la conseguenza che la rappresentazione è percepibile soltanto ed unicamente con l'uso di uno strumento digitale, dal computer al riproduttore di un CD. La novità è che la rappresentazione è trasferibile, da un supporto ad un altro, "identica": questo il pregio e la singolarità del documento informatico.» in P. TONINI, *L'evoluzione delle categorie tradizionali: il documento informatico* cit., p. 1311 ss.

[211] Scientifica è "quel tipo di conoscenza che ha le seguenti caratteristiche: ha per oggetto i fatti della natura; è ordinata secondo un insieme di regole generali che sono denominate leggi scientifiche e che

un genere di prova a carattere trasversale, che ricomprende la categoria delle prove critiche o indiziarie e delle prove rappresentative, come il documento informatico in questione, è necessario che l'incorporamento digitale avvenga attraverso una corretta applicazione delle leggi scientifiche. Pertanto, considerando la natura volatile e alterabile dei dati digitali, è necessario procedere all'acquisizione dei documenti informatici con strumenti di *computer forensics*, seguendo le c.d. *best practices*, la cui inosservanza, sebbene siano prive «di valore giuridico e di vincolatività», potrebbe «compromettere il valore probatorio dell'elemento raccolto con un pericoloso effetto domino sugli esiti processuali»[212].

Il documento informatico sarà acquisito attraverso i mezzi di ricerca della prova, di cui la legge 18 marzo 2008, n. 48 (esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica) ha imposto l'adozione di cautele che assicurino la conservazione genuina del documento informatico e ne impediscano l'alterazione[213].

II.2 I mezzi di ricerca della prova nel codice di procedura penale.

Il codice di procedura penale definisce "mezzi di ricerca della prova" le ispezioni, le perquisizioni, i sequestri e le intercettazioni di comunicazioni. La relazione al progetto preliminare inquadra la differenza tra i mezzi di prova, che si caratterizzano per l'attitudine ad offrire al giudice prove direttamente utilizzabili in sede di decisione, e i mezzi di ricerca della prova, che non integrano di per sé una fonte del convincimento giudiziale, ma facilitano l'acquisizione di cose materiali, tracce o dichiarazioni dotate di

---

sono collegate tra loro in modo sistematico; accoglie un metodo controllabile dagli studiosi nella formulazione delle regole, nella verifica e nella falsificabilità delle stesse." Così, P. TONINI, *Progresso tecnologico, prova scientifica e contradditorio*, in L. DE CATALDO NEUBURGER (a cura di), *La prova scientifica nel processo penale*, Padova, 2007, p. 49 ss. Per ulteriori riferimenti sulla prova scientifica, cfr. C. CONTI, *La prova scientifica alle soglie dei vent'anni dalla sentenza Franzese: vette e vertigini in epoca di pandemia*, in *ww.sistemapenale.it*., 9 febbraio 2021.

[212] C. CONTI, *La prova informatica e il mancato rispetto della best practice: lineamenti sistematici sulle conseguenze processuali*", in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, cit., p. 1330 ss.

[213] P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 368.

attitudine probatoria[214]. Attraverso questi strumenti è possibile l'acquisizione al dibattimento della fonte di prova e, in fase dibattimentale, della prova vera e propria.

I mezzi di ricerca della prova operano già prima della formazione della prova, in quanto la fase di ricerca può essere disposta, con decreto motivato, anche durante le indagini dal giudice, dal pubblico ministero, e talvolta anche dalla polizia giudiziaria (artt. 352-354), non consentendo il preventivo avviso al difensore dell'indagato[215]; inoltre, a differenza dei mezzi di prova che formano l'elemento di prova attraverso il loro esperimento processuale, con l'attuazione del principio del contraddittorio per la formazione della prova stabilito all'art. 111 Cost., l'elemento probatorio rilevato mediante i mezzi di ricerca della prova è preesistente allo svolgimento dello stesso.

Lo sviluppo della tecnologia ha avuto un impatto anche nella materia dei mezzi di ricerca della prova digitale, in quanto il supporto informatico e le sue varie componenti (come *pen drive*, *hard disk*, *floppy disk*, CD, DVD), sono ritenuti autonomi rispetto al documento digitale dematerializzato da analizzare, oggetto dei mezzi di ricerca della prova. La L. n. 48/2008 ha introdotto una normativa specifica sull'ispezione, la perquisizione e il sequestro di un sistema informatico, prevedendo cinque garanzie fondamentali[216], e inquadrandoli nei mezzi "tipici" di ricerca della prova, ed escludendo definitivamente l'atipicità[217]. Tuttavia, la stessa legge presenta delle lacune[218] che dovranno essere colmate dal lavoro interpretativo della dottrina e della giurisprudenza.

I mezzi di ricerca della prova disciplinati dal codice di rito sono:

---

[214] *Ivi*, p. 384.

[215] Sono definiti anche atti a "sorpresa".

[216] *Infra*, § I.3.4.

[217] Prima della legge di ratifica della Convenzione di Budapest sulla criminalità informatica, "l'art. 189 c.p.p., in coerenza con l'art. 190, comma 1, c.p.p. – che impone al giudice di escludere le prove "vietate dalla legge" –, presuppone logicamente la formazione lecita della prova e soltanto in questo caso la rende ammissibile". cfr. S. COLAIOCCO, *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *Archivio penale*, 1, 2014, p. 195.

[218] «Le lacune non trovano una giustificazione logica se non nella sommarietà dell'approccio alla problematica del documento informatico», v. P. TONINI, *Documento informatico e giusto processo*, in *Dir. pen. proc.*, 2009, n. 4.

- l'ispezione (artt. 244 – 246 c.p.p.) che consiste nell'attività di osservare e descrivere persone, luoghi e cose allo scopo di accertare le tracce e gli altri effetti materiali del reato; ispezionare significa "cercare qualcosa", per questo il presupposto che legittima l'adozione di questo mezzo è cercare la traccia appartenente al reato. Ispezionare significa proprio cercare qualcosa, per questo il presupposto che legittima l'adozione di questo mezzo è cercare la traccia appartenente al reato. le ispezioni sono disposte con decreto motivato caratterizzato dai connotati di urgenza, perché si tratta di un atto da svolgere tempestivamente, e motivato in quanto incide su diritti costituzionalmente garantiti. Nel comma 2 dell'art. 244 si prescrive che nel caso in cui non vengano trovate tracce o cose appartenenti al reato, l'autorità giudiziaria descrive lo stato attuale, e provvede nel caso ad usare apparecchiature che consentano di conservare lo stato di quelle cose soggette a possibili cambiamenti (e ciò rileva anche riguardo ai dati informatici). L'ispezione personale (art.245) è un atto che va ad incidere su norme costituzionalmente garantite (art.13 Cost.), per questo deve essere svolta nel rispetto della dignità e del pudore del soggetto sottoposto, il quale ha la facoltà di farsi assistere da persona di fiducia o dal difensore, o può essere eseguita da un medico. Circa l'ispezione di luoghi o di cose (anche del domicilio, a norma dell'art. 614 c.p.) viene estesa la garanzia della consegna del decreto motivato prima dell'inizio delle operazioni, annunciando i motivi del provvedimento, e nel verbale l'autorità giudiziaria potrà richiedere il non allontanamento di soggetti, riconducendo coattivamente l'eventuale trasgressore. Durante l'udienza preliminare o del dibattimento, l'ispezione di persone, di luoghi o di cose è disposta dal giudice, mentre nella fase delle indagini preliminari l'ispezione è compiuta ad iniziativa della polizia, se in urgenza, attraverso gli "accertamenti e rilievi sulle persone" (art. 354, comma 2). Occorre sottolineare che la polizia giudiziaria in casi del genere può disporre di sua iniziativa soltanto quei "rilievi sulle persone", che sono diversi dall'ispezione personale (art. 354, comma 3)[219]. Nei casi di assoluta

[219] Le ipotesi "speciali" sono previste in materia di prevenzione e repressione della criminalità organizzata

urgenza, quando si ritiene che il ritardo possa pregiudicare la ricerca o l'assicurazione della prova, il pubblico ministero può procedere prima delle 24 ore previste dal termine fissato.

- la perquisizione (artt. 247 – 252 c.p.p.) è l'attività volta ad acquisire al processo il corpo del reato e le cose pertinenti al reato, ossia le cose sulle quali o a mezzo delle quali il reato è stato commesso, e quelle che ne costituiscono il profitto, il prezzo, il prodotto. Si distinguono vari tipi di perquisizione, a seconda di ciò che dovrà essere cercato, come: perquisizioni personali, quando si ritiene che il corpo o le cose pertinenti al reato (intese come le cose che hanno la funzione di provare il reato o la responsabilità del suo autore[220]) siano occulti sulla persona, e occorre consegnare a questa una copia del decreto con l'avviso della facoltà di farsi assistere da persona di fiducia, purché prontamente reperibile e idonea[221]; di tipo locale, quando vi è fondato motivo di ritenere che le cose si trovino in un luogo determinato luogo, o che nello stesso possa eseguirsi l'arresto dell'imputato o dell'evaso (art. 247, comma 1), per cui si procede con la consegna della copia del decreto all'interessato o a colui che abbia la disponibilità del luogo; perquisizioni informatiche, introdotte dalla L. n. 48 del 2008, e le controverse perquisizioni *online* oggetto della trattazione. Rispetto alle ispezioni, il difensore ha sempre diritto di assistere ai vari tipi di perquisizione (e di rappresentarlo durante la perquisizione locale). La perquisizione avviene d'iniziativa del pubblico ministero, che con decreto motivato la dispone prevedendo se eseguirla personalmente o delegarla agli ufficiali della Polizia Giudiziaria; tuttavia, può però accadere che in sede d'indagini preliminari, la P.G. possa dar luogo di propria iniziativa, a perquisizione locale o personale nei casi di flagranza del reato o evasione

---

(art. 27 l. 19 marzo 1990, n. 55) e del traffico di stupefacenti (art. 103 d.p.r. 9 ottobre 1990, n. 309) o sono volte al contrasto dell'immigrazione clandestina (art.12, comma 7, d.lgs. 25 luglio 1998, n. 286, mod. dalla l. 30 luglio 2002, n. 189). Si ricordino gli interventi della polizia in materia di armi chimiche (art. 8 l. 18 novembre 1995, n. 496) e di sicurezza stradale (art. 192 codice della strada).

[220] P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 388.

[221] La persona deve avere almeno quattordici anni e non essere inferma di mente, oltre ad altri requisiti imposti dall'art. 120.

(art. 352 c.p.p.) e tali atti necessitano di convalida da parte del P.M. entro le 48 ore successive per accertarne il fondamento, altrimenti i risultati ottenuti saranno inutilizzabili; nelle fasi dell'udienza preliminare e del dibattimento la perquisizione è disposta dal giudice. Inoltre, l'autorità giudiziaria può "invitare" taluno a consegnare una cosa spontaneamente, ed è prevista una modalità meno invasiva della perquisizione per la ricerca di una cosa determinata (art. 248, comma 1).

- il sequestro probatorio (artt. 253 – 265 c.p.p.), spesso consequenziale agli altri mezzi di ricerca della prova, è quel mezzo attraverso cui l'autorità giudiziaria con decreto motivato, e mediante una procedura coattiva di spossessamento, dispone l'acquisizione del corpo del reato o delle cose ad esso attinenti ai fini dell'indagine, in modo che possano essere conservate e immutate fino all'accertamento dei fatti nel processo penale. All'interessato deve essere consegnata copia del decreto di sequestro emanato nel corso delle indagini preliminari dal pubblico ministero, mentre nelle fasi dell'udienza preliminare e del dibattimento il sequestro probatorio è disposto dal giudice. Poiché il sequestro è un "atto a sorpresa", il difensore dell'indagato (o uno designato d'ufficio) ha il diritto di assistere senza preavviso. Le cose saranno sequestrate fino a quando sussistono le esigenze probatorie, tranne se non vi sia sentenza irrevocabile, dopodiché le cose dovranno essere restituite, salvo che ne sia stata ordinata la confisca. Inoltre, la polizia giudiziaria, durante le indagini preliminari e in casi di urgenza, potrà intervenire al sequestro (art. 354 c.p.p.), che dovrà essere convalidato entro i termini previsti. Contro la convalida e il decreto di sequestro è previsto il riesame. Le cose sequestrate saranno custodite presso la cancelleria o la segreteria e se ciò non è possibile viene nominato un custode che si occuperà di tale elemento. Il codice disciplina alcune fattispecie peculiari di sequestro, come quello di documenti coperti dal segreto professionale o d'ufficio, il sequestro presso banche, di corrispondenza, e quello di telecomunicazioni e dati informatici. Sul sequestro probatorio di dati informatici, vi sono contrasti tra giurisprudenza e dottrina, in quanto,

secondo quest'ultima, il sequestro non sarebbe conciliabile con la "natura immateriale delle tracce informatiche"[222].

- le intercettazioni (artt. 266 – 271 c.p.p.) sono state definite dalla Corte di Cassazione come un'attività di "captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti che agiscano con l'intenzione di escludere altri e con modalità oggettivamente idonee allo scopo, attuata da soggetto estraneo alla stessa mediante strumenti tecnici di percezione tali da vanificare le cautele ordinariamente poste a protezione del suo carattere riservato"[223]. La poliedricità del captatore informatico, utilizzato come strumento intercettivo, ha prospettato nuove ipotesi di mezzi di ricerca della prova, dal labile confine tra tipicità e atipicità.

Il legislatore si è occupato di novellare, all'interno del codice di rito, un *corpus* normativo omogeneo in tema di criminalità informatica, riconoscendo la specificità della materia tecnologica, caratterizzata dalla natura volatile del dato digitale su cui incidono "condotte involontarie atte a ingenerare fenomeni di inquinamento e la conseguente necessità di impiegare *standard operating*, ossia procedure idonee a garantire la genuinità dell'accertamento"[224]. La L. n. 48/2008 ha integrato e modificato il testo degli articoli relativi ai mezzi di ricerca della prova compiuti su sistemi informatici e telematici, prevedendo l'adozione di "misure tecniche idonee dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione", in modo che sia prestata particolare attenzione alla "salvaguardia dell'integrità dei dati digitali", finalità imprescindibile per la verifica che gli inquirenti effettueranno sul corretto utilizzo delle procedure acquisitive degli elementi probatori, che avranno valenza di prova nel processo.

---

[222] G. COSTABILE, *Scena criminis, documento informatico e formazione della prova penale*, in *Dir. inf.*, 2005, p. 533 ss.

[223] Cass. Sez. VI, n. 12189, 29 marzo 2005.

[224] L. LUPARIA, *La ratifica della Convezione Cybercrime del Consiglio d'Europa.*, cit., p. 719.

II.3 Le ispezioni informatiche.

L'istituto dell'ispezione ha sollevato diverse problematiche relative alla necessità di conciliazione tra l'accertamento del fatto e il diritto di difesa, trattandosi l'ispezione di un atto che si realizza durante la fase delle indagini preliminari, e dunque, non ripetibile nel processo. Tali problematiche sono incrementate con l'introduzione nel 2008 della c.d. "ispezione informatica" inserita nel comma 2 dell'art. 244 c.p.p., a causa della natura volatile del dato digitale.

L'ispezione, etimologicamente dal latino *inspiciens* ossia guardare in qualcosa, si riferisce ad una osservazione visiva e sensoriale di una cosa, di un luogo o di una persona, finalizzata a ricercare elementi rilevanti e attinenti al reato, come prove materiali, tracce o dichiarazioni che sono dotate di attitudine probatoria. In altre parole, si ricercano "prove precostituite al processo"[225] tramite una constatazione "di una situazione di fatto attuale, come essa cade sotto i sensi dell'organo procedente"[226]. La mera osservazione è una caratteristica distintiva dell'ispezione, che la differenzia dalla perquisizione per la mancanza di una vera e propria ricerca.

L'ispezione (art. 244 c.p.p.) è un mezzo di ricerca della prova che ha la finalità "descrittiva" in quanto l'autorità giudiziaria la dispone per compiere la descrizione di persone, luoghi e cose allo scopo di "accertare le tracce e gli altri effetti materiali del reato" (art. 244, comma 1); l'autorità giudiziaria, se il reato non ha lasciato tracce o effetti materiali (es. sono scomparsi), cerca il come (modo, tempo e cause) è avvenuta la modificazione, e può disporre rilievi o operazioni tecniche su sistemi informatici o telematici attraverso misure tecniche atte ad assicurare la conservazione dei dati originali e ad impedirne la loro alterazione (art. 244, comma 2, c.p.p.)[227].

Il secondo comma dell'art. 244 c.p.p. non specifica quali misure tecniche debbano essere utilizzate, limitandosi a prevedere solo la *ratio* della prescrizione, che appare come una "norma processuale in bianco" che lascia libera scelta al *digital*

---

[225] Così, F. SIRACUSANO, *Manuale di procedura penale*, Milano, Giuffrè, 1990, p. 373.

[226] C. PEYRON, *L'ispezione giudiziale*, in *En. Dir, vol*. XXII, Giuffrè, Milano, 1972, p 962.

[227] P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 386.

forenser, professionista del settore, capace di individuare la *best practices* più adatta al caso concreto.

La legge 18 marzo 2008, n. 48, è intervenuta sull'ultima parte del 2 comma dell'art. 244, specificando che l'autorità giudiziaria può disporre rilievi "anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione". Pertanto, l'ispezione può avere ad oggetto anche i dati digitali, consistendo in un'osservazione finalizzata esclusivamente ad accertare la presenza di dati, informazioni e programmi all'interno di un determinato supporto[228], a cui non segue l'acquisizione.

II.3.1 Il labile confine tra l'ispezione e la perquisizione digitale.

Gli istituti tradizionali, però, sono difficilmente adattabili nel contesto digitale, tanto da sostanziarsi spesso in procedure analoghe che rischiano di sovrapporsi e confondersi tra loro, assottigliando la linea di demarcazione che le distingue. In particolar modo, è necessario capire in cosa consiste e come può svolgersi l'ispezione informatica, tenendo presente che, anche la sola osservazione delle tracce o degli effetti materiali del reato, ossia l'attività ispettiva, comporterebbe comunque l'irrimediabile alterazione dei dati di sistema o, comunque, la modifica dei metadati[229].

A riguardo, una parte della dottrina[230] afferma che l'ispezione informatica dovrebbe consistere in una mera osservazione e descrizione specifica del sistema e dei *file* nel suo insieme (considerando le periferiche, descrivendone i sistemi *hardware* o i *software* presenti, elencando le periferiche collegate e il sistema di connessione ad Internet[231]), poiché solo attraverso l'attività ispettiva si può effettuare una corretta

---

[228] G. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici"*, in L. LUPARIA, *Sistema penale e criminalità informatica (…)*, p. 192.

[229] Un metadato è un'informazione che descrive un insieme di dati. In informatica, ciascun *file* è portatore di dati (il suo contenuto) e metadati, come la sua data di creazione, la data di ultimo accesso e di modifica, il nome del suo autore, ecc.

[230] G. CORASANITI, G. CORRIAS LUCENTE, S. ATERNO, *Cybercrime, responsabilità degli enti e prova digitale: (…)*., cit., p. 206 ss.

[231] "L'attività ispettiva in ambiente informatico dovrebbe limitarsi ad osservare il sistema descrivendolo nei suoi particolari, ad esempio rilevando la presenza di periferiche collegate, accesso alla rete attivo, presenza di *software* in funzione, partizioni logiche nascoste e rese visibili da meccanismi di

esaminazione della scena del crimine informatica, anche attraverso i rilievi video-fotografici dei luoghi in cui sono allocati il sistema informatico o il *server*.

Un secondo orientamento[232], invece, ne incoraggia l'utilizzo nella determinazione di reati di lieve entità, per cui è necessario acquisire un'esigua quantità del materiale da sequestrare; tuttavia questa evenienza è limitata temporalmente, in quanto la sommaria visualizzazione di alcuni dati comporterebbe il tralascio di altri, mancando così di accuratezza e completezza investigativa; il secondo limite riguarda le garanzie difensive, in quanto le operazioni ispettive rientrerebbero nella categoria degli accertamenti tecnici non ripetibili e non controllabili *ex post* (art. 360 c.p.p.), ma sembra essere una scelta non praticabile, in considerazione delle finalità descrittive fisiologiche dell'ispezione stessa.

Per altri[233], la differenza tra ispezione e perquisizione si riscontrerebbe nei sistemi informatici, in cui rilevano dati protetti da sistemi di autenticazione che per essere acquisiti necessitano dell'inserimento di una *password* (e ciò necessita una perquisizione), e dati "liberi", fruibili da qualsiasi utente che potrebbero essere osservati (ispezione); questa distinzione si assottiglia ulteriormente nel caso di utilizzo della c.d. "*preview* dei reperti"[234]: attraverso l'utilizzo di *software* specifici gli inquirenti possono visualizzare in modo preliminare una parte del contenuto di un documento protetto dai sistemi di sicurezza, al fine di scegliere il materiale rilevante da poter eventualmente

---

autorizzazione connessi allo status dell'utilizzatore (ad esempio amministratore di sistema e chiavi di cifratura)". Così, C, MAIOLI, E. SANGUEDOLCE, *I "nuovi" mezzi di ricerca della prova fra informatica forense e L. 48/2008*, https://www.altalex.com/documents/news/2012/05/03/i-nuovi-mezzi-di-ricerca-della-prova-fra-informatica-forense-e-l-48-2008, 2012. Cfr., inoltre, G. CORASANITI, G. CORRIAS LUCENTE, S. ATERNO, *Cybercrime, responsabilità degli enti e prova digitale: (...)*., cit., p. 206 ss.

[232] G. COSTABILE, *Scena criminis, documento informatico e formazione della prova penale*, in *Dir. inf.*, 2005, p. 531.

[233] Così, C. MAIOLI, E. SANGUEDOLCE, *I "nuovi" mezzi di ricerca della prova fra informatica forense e L. 48/2008*, cit.

[234] «Il panorama si complica ulteriormente nel caso di utilizzo delle c.d. *preview*: attraverso l'utilizzo di *software* ad hoc viene permesso agli inquirenti in sede d'ispezione, ma anche di perquisizione (fattore, questo, che alimenta ulteriormente la "confusione applicativa" fra i due istituti), di poter analizzare in maniera grossolana il contenuto di un dispositivo per poi scegliere il materiale interessante e, se del caso, procedere a sequestro del dato. Si osserva, tuttavia, come tale operazione debba essere condotta da personale altamente qualificato, stante l'alto rischio di alterazione dei contenuti con conseguente dispersione di una possibile prova e, altresì, debba essere valutata caso per caso non rappresentando ad oggi operazione di routine applicabile indiscriminatamente a qualsiasi fattispecie concreta», *Ivi*.

sequestrare. Questo procedimento può avvenire in sede sia di ispezione che di perquisizione, e ciò suscita ulteriore "confusione applicativa" tra i due istituti. Si tratta di un'attività che può essere svolta solo da professionisti del settore, in considerazione della facilità di alterazione e dispersione dei dati digitali, attraverso una procedura diversa per ogni situazione concreta: ad esempio, rileva l'uso della *preview* nel reato di pedopornografia *online*, in cui durante l'acquisizione del materiale da sequestrare si dovrà procedere ad una cernita del contenuto doloso; o nel caso delle indagini digitali, la *preview* sarà utile al fine di stabilire un c.d. "alibi informatico"[235] tale da ricostruire le attività che l'indagato ha realizzato sullo stesso, esaminando anche i file cancellati o di sistema.

II.3.2 L'ispezione informatica tramite virus, e i relativi profili problematici.

In base a quanto previsto dalla relazione di accompagnamento alla legge del 23 dicembre 1993, n. 547[236], il concetto di sistema informatico o telematico ricomprende un'accezione ampia, caratterizzata sia dai sistemi di elaborazione e di scrittura ad uso individuale o ad un alto tasso di utenti, sia dai collegamenti tra computer e reti di ogni genere[237]. In considerazione di tale normativa e delle evoluzioni delle *best practices*, la disciplina di cui all'art. 244 potrebbe essere estesa alle condotte prodotte dall'uso del captatore informatico, come accadeva prima della legge di ratifica alla Convenzione di Budapest, in cui si cercava di adattare la normativa esistente ai casi riguardanti i reati informatici; l'estensione potrebbe concretizzarsi come una sorta di "ispezione

---

[235] Il termine "alibi" non ha una definizione specifica: si tratta di un avverbio latino il cui significato è "altrove", ed è utilizzato dall'indiziato per chiarire l'arco temporale in cui si trovava in un altro posto rispetto a quello di commissione del reato. Nel corso delle indagini si potranno raccogliere elementi coerenti e ragionevoli, tali da far assurgere l'alibi a valore di prova contro-deduttiva: affinché ciò avvenga è necessario che l'alibi informatico sia "direttamente" riferibile all'imputato che lo fornisce a sua difesa. Tuttavia, l'alibi informatico potrebbe anche essere falso, e pertanto, dovrà essere verificata ed adeguata soprattutto in fase di indagini preliminari, rispetto alle singole esigenze indiziarie e probatorie. Cfr. V. CALABRÒ, G. COSTABILE, S. FRATEPIETRO, M. INAULARDO, G. NICOSIA, *L'alibi informatico. Aspetti tecnici e giuridici*, in IISFA Memberbook 2010, Forlì, Experta.

[236] La legge, pubblicata in G. U. n. 305 del 30 dicembre 1993, reca Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica.

[237] G. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici"*, in L. LUPARIA, *Sistema penale e criminalità informatica (…)*, p. 194. Per ulteriori approfondimenti sulla nozione di sistema informatico, vedi Cass. pen., Sez. VI, 4 ottobre 1999, n. 3067.

personale", poiché, nonostante l'oggetto di controllo sia lo "spazio virtuale" di un dispositivo, lo stesso dispositivo è costituito dal contenuto di informazioni personali e riservate. Tuttavia, tale operazione non sembrerebbe essere ammessa, a causa di obiezioni e contrasti costituzionali: in primo luogo, l'art. 244 c.p.p. non fa nessun riferimento ai mezzi con cui l'attività ispettiva debba essere espletata, ma concerne solo l'oggetto di questa; in secondo luogo, la ratio della legge di ratifica n. 48/2008 è il contrasto alla criminalità informatica attraverso misure efficaci disposte per l'acquisizione dei dati digitali, che siano conformi alle garanzie e tutele previste dalla Convenzione del Consiglio d'Europa del 1950 e dalla Convenzione internazionale delle Nazioni Unite sui diritti civili e politici del 1966, e ciò limita l'uso del captatore informatico che può estendersi a qualunque reato, seppur con il divieto di indagini informatiche *ad explorandum*; infine, vi sono contrasti nel diritto nazionale (Artt. 2 e 13, 14 e 15 della Costituzione) e sovranazionale (art. 8 CEDU), a causa del carattere occulto e invasivo del captatore che incide sul c.d. "domicilio informatico"[238] e sulla riservatezza informatica, diritti fondamentali dell'individuo[239].

II.4 Le perquisizioni informatiche.

La perquisizione, disciplinata dagli artt. 247 e ss. c.p.p., consiste nel ricercare una cosa da assicurare al procedimento o una persona da arrestare[240]. L'attività del *perquirere* si caratterizza nell'individuazione e acquisizione del corpo del reato o delle cose ad esso pertinenti, qualificandosi spesso come attività prodromica rispetto al sequestro probatorio (art. 247, comma 1°). La perquisizione si caratterizza per tre elementi fondamentali: le modalità di espletamento, consistenti nella ricerca di una cosa materiale attinente al reato che sia preesistente al processo, intervenendo sullo stato dei

[238] Il concetto di domicilio informatico è stato elaborato con l'introduzione dei reati informatici nella legge del 23 dicembre 1993, n. 574, inteso come bene giuridico tutelato dagli artt. 615-bis e 615-ter c.p., collocati tra i delitti contro l'inviolabilità del domicilio. L'introduzione delle due condotte incriminate ha lo scopo di tutelare i sistemi informatici o telematici, in quanto "espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'articolo 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli articoli 614 e 615 del codice penale".

[239] La problematica relativa all'incidenza dei diritti fondamentali riguarda principalmente la riserva di legge stabilita in materia, a riguardo cfr. C. CONTI, *Sicurezza e riservatezza*, in *Dir. Pen. e proc*., 2019, 11, p. 1572.

[240] P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 388.

luoghi[241]; le sue duplici finalità di acquisizione degli elementi probatori, o di esecuzione di provvedimenti coercitivi; la coercizione, strumento che grazie alle deroghe costituzionali risulta strumentale per la ricerca (artt. 13 e 14 Cost.).

La perquisizione informatica è stata introdotta dalla legge 48/2008, che ha aggiunto il comma 1-*bis* all'art. 247, e la dispone "quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico", anche quando esso sia protetto da misure di sicurezza[242]; inoltre, devono essere sempre adottate "misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione".

Inoltre, per i casi di urgenza, è stata prevista la modifica dell'art. 352 in materia di perquisizioni, e dell'art. 354 c.p.p. in tema di accertamenti urgenti sui luoghi, sulle cose e sulle persone e sequestro da parte degli ufficiali della polizia giudiziaria: tali norme stabiliscono che gli ufficiali in questione adottino misure tecniche o le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso ai dati originali contenuti nei sistemi informatico-telematici (352), prevedendo, ove possibile, alla duplicazione immediata dell'originale su adeguati supporti, attraverso una procedura che ne garantisca la sua immodificabilità (354)[243].

In ambito informatico, l'attività di ricerca avviene nei dispositivi digitali contenenti *file* di interesse investigativo: tale attività perquisiva è potenzialmente idonea a modificare il dato originale, e pertanto è necessario che all'attività di ricerca consegua necessariamente il sequestro, non potendo essere considerato quest'ultimo come un procedimento strumentale alla perquisizione informatica[244]; ciò che sarà sequestrato

---

[241] Ciò la differenzia dall'ispezione in quanto "l'investigatore non si limita alla mera osservazione delle particolarità di una persona, di un luogo o di un oggetto, ma si puntualizza in una ricerca accurata volta al rinvenimento del corpo del reato o delle cose ad esso pertinenti" così P. FELICIONI, *Le ispezioni e le perquisizioni*, Milano, Giuffrè, 2004, p. 96.

[242] Per approfondimenti sulle misure di sicurezza e tutela del domicilio informatico cfr. S. ATERNO, *Aspetti giuridici comuni delle indagini informatiche*, in S. ATERNO, F. CAJANI, G. COSTABILE, M. MATTIUCCI, G. MAZZARCO, *Computer Forensics e Indagini digitali*, vol.1, Experta, 2011. Inoltre, A. VITALE, *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico*, in *Dir. dell'Internet*, 2008, p. 503.

[243] Cfr. S. ATERNO, *Digital forensics (investigazioni informatiche)*, in *Dig. disc. pen.* (agg.), 2014, p. 217.

[244] Così, L. LUPARIA, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa* (l. 18 marzo 2008, n. 48). *Profili di diritto processuale*, in *Dir. pen. proc*., 6/2008, p. 720., ed anche, E. LORENZETTO,

sarà la copia forense, accuratamente acquisita secondo i procedimenti già descritti, e non il *file* originale, pena la violazione degli artt. 247 e 352 c.p.p., modificati dalla legge 48/2008.

È stata fortemente dibattuta in dottrina e giurisprudenza l'utilizzabilità del sequestro effettuato successivamente a perquisizione illegittima: le Sezioni unite della Cassazione, si sono espresse affermando che tale forma di invalidità della perquisizione non si trasmette al sequestro quando questo ha per oggetto il corpo del reato e le cose ad esso pertinenti, perché in tal caso si tratta di un atto dovuto ai sensi dell'art. 253[245]; analogamente la pronuncia della sentenza costituzionale n. 219 del 2019[246].

È necessario però che la perquisizione sia giustificata e legata all'oggetto della prova[247]: ciò può avvenire mediante l'individuazione del fatto storico penalmente rilevante, rispetto a cui sussiste un rapporto di pertinenzialità dell'elemento informatico da ricercare; tale individuazione può essere semplificata attraverso la *preview* dei reperti, condotte con particolari cautele a seconda dello stato del dispositivo, rinvenuto in modalità accesa o spenta, in considerazione del fatto che i dispositivi accesi e collegati alla rete[248] sono più vulnerabili rispetto ad una ricerca e successivo sequestro compiuti sui dispositivi *offline*, oltre a rappresentare problematiche a livello processuale sulla loro eventuale a/tipicità, in quanto attività occulta che coinvolge diritti costituzionalmente garantiti.

Le attività urgenti di investigazione informatica e telematica, in L. LUPARIA, *Sistema penale e criminalità informatica (…)*, cit., p. 154.

[245] Cass., sez. un., 27 marzo 1996, n. 5021, *Sala*, in *Cass. pen.*, 1996, 3268.

[246] La Consulta ha precisato che l'invalidità derivata è prevista soltanto dalle norme sulle nullità e non può essere estesa all'inutilizzabilità a causa del principio di tassatività nella disciplina dei divieti probatori. Il principio è stato ribadito dalla successiva sentenza n. 252 del 2020.

[247] Secondo Cass., sez. II, 10 settembre 1997, n. 84, in *Arch. n. proc. pen*., 1998, 297, può farsi ricorso alla perquisizione come mezzo coattivo di ricerca della prova, solo se sia stato individuato il tema nel cui ambito tale ricerca ha un suo contenuto di concretezza e specificità, posto che, diversamente, la perquisizione si trasformerebbe in un mezzo di acquisizione della *notitia criminis*.

[248] Sull'analisi delle "perquisizioni *online*" si rimanda al capitolo III di questa trattazione.

II.5 Il sequestro probatorio informatico.

Il sequestro probatorio (art. 253 c.p.p.) consiste nel conservare in modo immutato una cosa mobile o immobile[249] al fine dell'accertamento dei fatti[250], attraverso lo spossessamento coattivo della cosa e la creazione di un vincolo di indisponibilità sulla medesima.

La legge n. 48 del 2008 è intervenuta anche in tema di sequestro probatorio, modificando e integrando diverse norme del codice di rito al fine di adeguarle alla nuova realtà dematerializzata.

Riguardo al sequestro probatorio informatico, l'art.19 della Convenzione di Budapest sul *Cybercrime* afferma che il sequestro di strumenti informatici può avere ad oggetto sia l'*hardware* (sistema informatico o supporto di memorizzazione), sia i *file* in esso contenuti e presenti nel territorio nazionale. Secondo la legge n. 48 del 2008 ciò che è posto sotto sequestro probatorio, non è la sua componente mobile (come computer o l'*hard disk,* in ragione del fatto che gli accessori non possono ritenersi rientranti nel concetto di corpo del reato, non essendo cose mediante le quali è stato commesso il reato"[251]), ma il documento informatico, poiché nel momento in cui l'oggetto fisico (*hardware*) sarà restituito, ciò che sarà conservata sarà la copia-clone dell'originale (tanto che la copia-clone del dato rilevato all'esito dell'espletamento dei mezzi di ricerca rende superfluo il sequestro del dato originale, ed è per questo che in dottrina si afferma la mancanza di attualità del sequestro, in relazione al dato digitale[252]), attraverso la *bit stream image*, di cui l'imputato potrà contestarne il trattenimento

---

[249] È necessario che la cosa sia un bene materiale (requisito "naturalistico"), e che si tratti del corpo del reato o di una cosa pertinente al reato (requisito "giuridico") necessaria per l'accertamento dei fatti. Cfr. P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 392.

[250] Cass., sez. un., 28 gennaio - 13 febbraio 2004 n. 2, Ferrazzi, in *Cass. pen.*, 2004, 1913: «anche per le cose che costituiscono corpo di reato il decreto di sequestro a fini di prova deve essere sorretto, a pena di nullità, da idonea motivazione in ordine al presupposto della finalità perseguita, in concreto, per l'accertamento dei fatti».

[251] Tribunale Riesame, Venezia, ord. 6 ottobre 2000. In dottrina, cfr. A. MONTI, *No ai sequestri indiscriminati di computer*, in *Diritto dell'Internet*, 3, 2007, pag. 268.

[252] E. LORENZETTO, *Utilizzabilità dei dati informatici incorporati su computer in sequestro: dal contenuto al contenitore, passando per la copia*, in *Cass. pen.*, 2010, p. 1533.

mediante il riesame[253]: credere l'opposto, significherebbe accettare l'idea che un vincolo reale possa discendere da un provvedimento inoppugnabile, cosa, chiaramente al di là di ogni possibile sostenibilità.

La legge 28/2008 ha innovato la disciplina del sequestro di corrispondenza prevista dall'art. 254 c.p.p. sotto tre aspetti: in primis è stato ampliato l'elenco tassativo dei soggetti destinatari del provvedimento di sequestro, ricomprendendo quei fornitori di servizi postali, telegrafici e telematici che consentono, oltre ai servizi tradizionali, la possibilità di ricevere comunicazioni elettroniche *online*; in secondo luogo è stata aggiunta alle varie tipologie di corrispondenza quella telematica, sempre che sussista un rapporto di pertinenza tra la cosa sequestrata e il reato (ciò è possibile circoscrivendo il sequestro attraverso la peculiare indicazione del bene da requisire, scongiurando sequestri "sovrabbondanti" non idonei per le esigenze probatorie previste[254]); infine, è stato stabilito il criterio della "non alterabilità" del reperto, che obbliga la polizia giudiziaria sequestrante a garantire la conservazione genuina del materiale appreso.

Tra gli interventi riformatori della legge di ratifica, spicca la creazione dell'art. 254-*bis* c.p.p. sul sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni: tale norma stabilisce che l'autorità giudiziaria può disporre il sequestro dei dati da costoro detenuti (compresi quelli di traffico o di ubicazione) e può stabilire "che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità"; è ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali[255]. L'articolo in esame ha suscitato criticità in relazione alla locuzione sul sequestro di "dati di traffico o di ubicazione" che sembrava sovrapporsi alla disciplina prevista dall' art. 132 del "Codice della *privacy*" sulla c.d. *data retention* e l'acquisizione dei tabulati anche per finalità di

---

[253] "Pertanto, vi è interesse dell'imputato ad impugnare il trattenimento della copia clone, mediante riesame, al fine di verificare la pertinenza del dato, o di chiedere la restituzione qualora difettino i presupposti del trattenimento" in P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 396.

[254] F. CAJANI, *La rete internet e "dintorni", parte I - Aspetti tecnici ed investigazioni di base*., in S. ATERNO, F. CAJANI, G. COSTABILE, M. MATTIUCCI, G. MAZZARCO, *Computer Forensics e Indagini digitali*, vol.1, Experta, 2011.

[255] P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 397.

accertamento dei reati nel processo penale (d.lgs. n. 196/2003); tuttavia, l'istituto del sequestro stabilito dall'art. 254-*bis*, va tenuto distinto dall'attività "preventiva" disciplinata dall'art. 132 d.lgs. 196/2003, in quanto i risultati ottenuti non sono utilizzabili nel procedimento penale, in base a quanto previsto dall'art. 226 co. 5 d.lgs. 28 luglio 1989, n. 271[256]. Infatti, per evitare contrasti normativi, è stata proposta un'interpretazione restrittiva per cui l'art. 254-*bis* c.p.p. rappresenterebbe una specificazione dell'art. 254 c.p.p., precisando sia le modalità di acquisizione e di copia dei dati su supporti adeguati, attraverso una procedura tale da assicurarne conformità e immodificabilità dei dati acquisiti, sia imponendo ai fornitori dei servizi di telefonia e di connessione internet una conservazione e protezione adeguata dei dati originali. Inoltre, attraverso l'applicazione dell'art. 254-*bis* c.p.p è possibile sequestrare i *file* di "log"[257] di navigazione Internet, rilevanti per l'indagine: ciò permette sia lo svolgimento regolare della fornitura del sevizio di *Internet Service Provider* (che continua nonostante il provvedimento di sequestro), sia che possano adempirsi gli obblighi previsti dalla data retention (nelle normative previste d.lgs. n. 109 del 2008 e art.132 del d.lgs.196 del 2003), riguardanti la cancellazione dei dati prevista dalla legge e la conservazione e protezione dei questi fino ai termini stabiliti dall'art.132 del d.lgs.n.196/2003.

L'ordinamento italiano nel prevedere che l'autorità giudiziaria "può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità", non chiarisce quali siano le *best practices* da seguire per effettuare correttamente il sequestro dei dati informatici, e ciò ha suscitato contrasti sovranazionali, in particolar modo con la Raccomandazione n. 3 del 7 settembre 1999, che disciplina il trattamento dei dati personali per la conservazione dei dati sulle comunicazioni da parte dei fornitori di servizi Internet a fini giudiziari. Pertanto, nel rispetto delle normative sopracitate, è auspicabile eseguire il sequestro mediante la *bit stream image*, *best practice* capace di

[256] V. anche, per il rapporto tra i vari istituti, G. DI PAOLO, la voce *Prova informatica*, in *Enc. giur.*, Giuffrè, p. 753 ss.

[257] Il Log è un registro. Piccolo *file* o memoria ad alta velocità in grado di memorizzare dati, normalmente in formato testo, con lo scopo preciso di storicizzare gli eventi. Le registrazioni sono memorizzate sui *file*.

produrre una copia-clone del dato originale, punto d'incontro tra gli standard europei e la salvaguardia delle libertà costituzionalmente garantite[258].

Tra le ulteriori introduzioni, occorre segnalare quelle riguardanti la tutela degli oggetti digitali posti a sequestro, in considerazione del carattere dispersivo del materiale informatico: nel comma 2 dell'art. 259 c.p.p., rubricato "custodia delle cose sequestrate", si precisa che «quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria» e ciò può avvenire predisponendo la *Chain of custody*[259], già ampliamente descritta. Nell'art. 260 c.p.p. relativo all'apposizione di sigilli, si introducono al comma 1 sigilli informatici ed elettronici, come la funzione di Hash[260], che criptando i dati originali acquisiti in copia permette la loro immodificabilità e garantisce che non vi siano rischi di inquinamento delle prove; inoltre, la criptazione renderebbe superfluo l'obbligo che ha il custode nei confronti dei terzi, che potrebbero accedere e alterare i dati sequestrati, necessario solo se si debba scongiurare la distruzione del supporto di memorizzazione[261], che non influirebbe sulle indagini, ma configurerebbe solo reato stabilito dall'art. 388, comma 3, c.p., "Mancata esecuzione dolosa di un provvedimento del giudice". Al comma 2 dell'art. 260 c.p.p. è previsto che l'eventuale copia dell'evidenza digitale deve essere realizzata su adeguati supporti attraverso una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità.

---

[258] S. VENTURINI, *Sequestro probatorio e fornitori di servizi telematici*, da L. LUPARIA, *Internet provider*, Milano, Giuffrè, 2009.

[259] *Infra*, § I.4.2.

[260] *Ivi*.

[261] F. NOVARIO, *Le prove informatiche*, in P. FERRUA, E. MARZADURI, G. SPANGHER (a cura di), *La prova penale*, Giappichelli, Torino, 2013.

II.6 Le intercettazioni di conversazioni o comunicazioni.

II.6.1 Principi costituzionali e definizioni.

Nel codice di procedura penale non è presente la definizione di intercettazione. Tale silenzio normativo deve essere necessariamente colmato in ragione del fatto che l'attività intercettiva, prevista dagli artt. 266 e ss., incide su diritti costituzionalmente garantiti, come l'art. 15 Cost. che tutela l'inviolabilità della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione, e la loro limitazione "può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge"; inoltre, le intercettazioni possono incidere sul rispetto dell'inviolabilità del domicilio, tutelato dall'art. 14 Cost., e sul diritto alla *privacy* di ogni cittadino, costituzionalmente garantito dall'art. 2 Cost., attraverso interventi normativi della Corte Costituzionale[262] che hanno fatto rientrare il diritto alla riservatezza nel novero dei diritti inviolabili dell'uomo. Infatti, la Convenzione europea dei diritti dell'uomo stabilisce all'art. 8 che "ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della corrispondenza" da cui discende la tutela del diritto alla riservatezza della vita privata.

La problematica relativa alla definizione di intercettazione è stata ampliamente risolta dalla giurisprudenza nella storica sentenza a Sezioni Unite n° 36747 del 24 settembre 2003 "Torcasio", in cui si è affermato che è intercettazione quella «captazione, ottenuta mediante strumenti tecnici di registrazione, del contenuto di una conversazione o di una comunicazione segreta in corso tra due o più persone, quando l'apprensione medesima è operata da parte di un soggetto che nasconde la sua presenza agli interlocutori»[263].

I requisiti che distinguono l'attività intercettiva dagli altri mezzi di ricerca della prova sono molteplici: innanzitutto, si tratta di una captazione "segreta" di una comunicazione o conversazione, che viene realizzata da un soggetto terzo totalmente estraneo al contenuto e alla relazione intercorrente tra i comunicanti, e pertanto, non può

[262] Si veda, C. cost., 26 marzo 1990, n. 139; C. cost., 23 giugno 2005, n. 271; C. cost., 21 febbraio 2019, n. 20. Inoltre, si veda CEDU, 10 febbraio 2009, *Iordachi c. Moldavia*, in *Cass. pen*., 2009, 4021.

[263] La definizione è tratta dalla sentenza della Cass., sez. un., 28 maggio-24 settembre 2003, *Torcasio*, in *Guida dir*., 2003, 42, 49.

considerarsi intercettazione l'espressione pubblica di un pensiero, sia pure rivolta a terzi estranei[264]; la captazione deve essere realizzata mediante strumenti tecnici di registrazione (elettronici o digitali) che siano idonei a superare le cautele elementari, che dovrebbero garantire la libertà e segretezza del colloquio, e a captarne i contenuti[265], con la possibilità di attuare intercettazioni "differite" caratterizzate da un ascolto compiuto non in tempo reale, ma attraverso un'apparecchiatura di registrazione nascosta che sarà poi recuperata e riprodotta successivamente[266]; l'intercettazione è un'attività "occulta", e questo requisito fondamentale permette un ascolto clandestino che garantisce la terzietà del captante al colloquio tra soggetti, poiché se la registrazione fosse effettuata da uno degli interlocutori si tratterebbe di un "documento" che potrà essere ammesso nel processo, salvo che vi osti un divieto probatorio[267] (inoltre, anche il pedinamento elettronico mediante apparecchiatura satellitare G.P.S. non può essere considerata intercettazione perché non ha per oggetto una "comunicazione", e può essere disposto dalla polizia giudiziaria come attività atipica[268]).

---

[264] "L'intercettazione di conversazioni realizzate per mezzo di un apparecchio ricetrasmittente privo di concessione non è soggetta ad autorizzazione alcuna da parte dell'autorità giudiziaria, perché relativa a comunicazioni non costituzionalmente garantite in quanto effettuate con mezzo illegale, il cui uso costituisce reato, ed in quanto prive del requisito della riservatezza, essendo liberamente captabili da chiunque, nel raggio di irradiazione, si avvalga di un apparecchio ricevente sintonizzato sulla stessa lunghezza d'onda". In tal senso, Cass., sez. II, 12 novembre 1994, in *Cass. pen*., 1996, 861. Così in P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 398.

[265] Ivi.

[266] Così Cass., sez. un., 24 settembre 2003, *Torcasio*, cit.

[267] "La registrazione di una conversazione telefonica compiuta da uno degli stessi interlocutori è documento della conversazione in questione e perciò ne è prova idonea ed utilizzabile in giudizio". Così, Cass., sez. II, 8 aprile 1994, in Giust. pen., 1995, III, 67; Cass., sez. un., 24 settembre 2003, *Torcasio*, cit. Il documento fonografico così formato è utilizzabile solo se non viola specifiche regole di acquisizione della prova, quali gli artt. 63 comma 2, 195 comma 4 e 203 c.p.p. Il Supremo collegio ha prospettato una sorta di "inutilizzabilità sistematica" (C. CONTI) che consegue all'impiego di un mezzo di prova allo scopo di aggirare i limiti ricavabili dagli schemi legali delineati dal codice. Con la sentenza 4 dicembre 2009, n. 320, la Corte costituzionale ha precisato che non costituisce documento, bensì documentazione, la registrazione effettuata dalla polizia giudiziaria nell'ambito di un atto di indagine.

[268] In modo analogo la giurisprudenza tratta il c.d. *positioning* (che sfrutta il sistema di geolocalizzazione presente nei dispositivi cellulari) a proposito del quale afferma che la "localizzazione dei soggetti compiuta attraverso l'apparecchio cellulare di cui abbiano il possesso, mediante la tecnica cosiddetta "*positioning*", non necessita di autorizzazione giudiziale, risolvendosi in una sorta di pedinamento satellitare e non interferendo sulla libertà e segretezza delle comunicazioni". Così Cass., sez. I, 13 maggio 2008, n. 21366, *Stefanini*, in CED n. 240092; Cass., sez. IV, 12 giugno 2018, n. 41385, *Chirico e altro*, in CED n. 273929.

Il codice di rito ha previsto che l'applicazione delle intercettazioni sia soggetta ad una doppia riserva, di giurisdizione e di legge. Riguardo alla riserva di giurisdizione, la giurisprudenza costituzionale ritiene che soltanto con un provvedimento del giudice possa essere autorizzata l'intercettazione: infatti, il giudice per le indagini preliminari dovrà figurare come il garante dei diritti del soggetto indagato, e sarà l'unico che potrà autorizzare, con decreto motivato[269] che specificherà i presupposti e le modalità dell'operazione (art. 267 c.p.p.), la richiesta effettuata dal pubblico ministero, o convalidarla nelle 48 ore successive, nel caso in cui venga disposta dal P.M. in situazioni d'urgenza. In relazione alla riserva di legge, si parla di una riserva di legge "rinforzata" in quanto l'art. 15 Cost. prevede che siano stabilite delle "garanzie" con le norme che prevedono le limitazioni alla libertà e segretezza della corrispondenza e delle comunicazioni[270]: le intercettazioni possono essere disposte solo quando vi siano gravi indizi di reato (a differenza dei gravi indizi di colpevolezza delle misure cautelari), intesi come un'elevata probabilità e non una mera possibilità che sia stato commesso o si stia commettendo un reato, ed è lo stesso art. 266 c.p.p., oggetto di costanti riforme, che dispone l'elenco tassativo[271] per l'ammissione delle intercettazioni; infatti, le

[269] "Purtroppo, nella prassi, la giurisprudenza ha svalutato l'importanza della motivazione e ha consentito al giudice di riferirsi ai motivi contenuti nella richiesta del pubblico ministero; sono dovute intervenire le Sezioni unite della Cassazione per indicare i limiti nei quali è accettabile la motivazione redatta attraverso un riferimento c.d. per *relationem* ad altri provvedimenti", Cfr. P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 400, in cui fa riferimento a Cass., sez. un. 21 giugno 2000, Primavera, in Cass. pen., 2001, 69, ha precisato che «la motivazione per relationem di un provvedimento giudiziale è da considerare legittima quando: 1) faccia riferimento (...) a un legittimo atto del procedimento, la cui motivazione risulti congrua rispetto all'esigenza di giustificazione propria del provvedimento di destinazione; 2) fornisca la dimostrazione che il giudice ha preso cognizione del contenuto sostanziale delle ragioni del provvedimento di riferimento e le abbia meditate e ritenute coerenti con la sua decisione; 3) l'atto di riferimento, quando non venga allegato o trascritto nel provvedimento da motivare, sia conosciuto dall'interessato o almeno ostensibile, quanto meno al momento in cui si renda attuale l'esercizio della facoltà di valutazione, di critica ed, eventualmente, di gravame e, conseguentemente, di controllo dell'organo della valutazione o dell'impugnazione».

[270] P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 401.

[271] Art. 266 c.p.p.: "1. L'intercettazione di conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazione è consentita nei procedimenti relativi ai seguenti reati:
a) delitti non colposi per i quali è prevista la pena dell'ergastolo o della reclusione superiore nel massimo a cinque anni determinata a norma dell'articolo 4; b) delitti contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni determinata a norma dell'articolo 4; c) delitti concernenti sostanze stupefacenti o psicotrope; d) delitti concernenti le armi e le sostanze esplosive; e) delitti di contrabbando; f) reati di ingiuria, minaccia, usura, abusiva attività finanziaria, abuso di informazioni privilegiate, manipolazione del mercato, molestia o disturbo alle persone col mezzo del telefono; f-*bis*) delitti previsti dall'articolo 600 ter, terzo comma, del codice penale, anche se relativi al materiale pornografico di cui all'articolo 600 quater 1 del medesimo codice, nonché

intercettazioni possono avere ad oggetto le conversazioni o comunicazioni telefoniche e altre forme di telecomunicazione (art. 266), le comunicazioni o conversazioni tra presenti (cd. intercettazioni ambientali); art. 266, comma 2 e il "flusso di comunicazioni relativo a sistemi informatici o telematici o intercorrente tra più sistemi" (art. 266-*bis*); inoltre, le intercettazioni potranno essere utilizzate solo come *extrema ratio*, ossia se siano ritenute assolutamente indispensabili ai fini della prosecuzione delle indagini.

II.6.2 La normativa delle intercettazioni comune alle vecchie e alle nuove riforme.

Nonostante le modifiche normative che hanno intaccato per diversi aspetti l'assetto delle intercettazioni, la disciplina relativa ai requisiti necessari per disporre le intercettazioni è rimasta invariata per i procedimenti iscritti prima del 31 agosto 2020, mentre per quelli iscritti dopo tale data si osserveranno le disposizioni stabilite dalla L. n. 70 del 2020. I requisiti per disporre le intercettazioni sono riferiti al titolo di reato su cui il P.M. sta svolgendo le indagini; si è soliti distinguere i procedimenti per i reati comuni (elencati nell'art. 266 c.p.p.) e i procedimenti per reati di criminalità organizzata o ad essa equiparati[272].

Riguardo ai procedimenti per i reati comuni, essi sono previsti nell'art. 266, comma 1: tra questi, occorre segnalare l'introduzione dei delitti commessi avvalendosi delle condizioni tipiche dell'associazione mafiosa o commessi al fine di agevolare l'attività di queste associazioni (art. 416-*bis* c.p.; art. 266, lett. f-*quinquies*, con effetto

---

dall'art. 609 *undecies*; f-*ter*) delitti previsti dagli articoli 444, 473, 474, 515, 516, 517 *quater* e 633, secondo comma, del codice penale; f-*quater*) delitto previsto dall'articolo 612 *bis* del codice penale; f-*quinquies*) delitti commessi avvalendosi delle condizioni previste dall'articolo 416 *bis* del codice penale ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo. 2. Negli stessi casi è consentita l'intercettazione di comunicazioni tra presenti che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile. Tuttavia, qualora queste avvengano nei luoghi indicati dall'articolo 614 del codice penale, l'intercettazione è consentita solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa. 2-*bis*. L'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile è sempre consentita nei procedimenti per i delitti di cui all'articolo 51, commi 3-*bis* e 3-*quater*, e, previa indicazione delle ragioni che ne giustificano l'utilizzo anche nei luoghi indicati dall'articolo 614 del codice penale, per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'articolo 4.

[272] P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 402 ss.

per i procedimenti iscritti dopo il 31 agosto 2020), secondo quanto previsto dalla legge di conversione 28 febbraio 2020, n. 7; inoltre le intercettazioni possono essere disposte per i reati commessi attraverso l'impego di tecnologie telematiche o informatiche, ai sensi dell'art. 266-*bis*; e infine, le intercettazioni potranno anche essere disposte per semplificare la ricerca del latitante (art. 295, commi 3 e 3-*bis*). È necessario che dagli atti di indagine risultino gravi indizi di reato, in cui viene applicata la disciplina prevista dall'art. 203 c.p.p. relativa agli indizi riguardanti le dichiarazioni ottenute dagli informatori della polizia giudiziaria e dei servizi di sicurezza, che dovranno essere esaminati come testimoni o come persone informate sui fatti, pena inutilizzabilità delle stesse ai fini della valutazione dei gravi indizi di reato (art. 267, comma 1-*bis*). L'intercettazione deve rispettare dei termini specifici di durata pari a quindici giorni, ma può essere prevista una proroga richiesta dal P.M. e motivata nel decreto del giudice, nel caso in cui sussistano i presupposti indicati nel comma 3 dell'art. 267 c.p.p. In questi casi il codice può consentire le intercettazioni di comunicazioni tra presenti (c.d. ambientali), anche nel domicilio privato, ma solo se si ritenga, con fondato motivo, che nello stesso si stia compiendo l'attività criminosa (art. 614 c.p.).

La disciplina risulta più attenuata in relazione ai procedimenti per i delitti di criminalità organizzata, o ad essa equiparati. In questo caso, i reati che potranno essere soggetti ad intercettazione sono previsti dall'art. 13 d.l. 1991 n. 152 che ricomprende: i delitti di "criminalità organizzata"[273]; la "minaccia col mezzo del telefono" (art. 13 d.l. 1991 n. 152); il terrorismo anche internazionale (art. 407, comma 2, lett. a, n. 4 c.p.p.; art. 3 d.l. 2001 n. 374, e inoltre gli artt. 270-*ter* e 280-*bis* c.p.); i delitti contro la libertà individuale (art. 9, legge 2003 n. 228; artt. 600-604 c.p.); i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione di almeno cinque anni nel massimo, determinata a norma dell'articolo 4 c.p.p.[274]. Per tali reati,

[273] Si intende "l'associazione di più di due persone, stabilita da tempo, che agisce in modo concertato allo scopo di commettere reati"; così Cass., sez. un. 11 maggio 2005, *Petrarca*, in *Cass. pen*., 2005, 2916: la nozione di "criminalità organizzata" è riferibile ai reati di criminalità mafiosa e a qualsiasi tipo di associazione a delinquere ex art. 416 c.p. con esclusione del mero concorso di persone nel reato.

[274] La legge n. 3 del 2019 ha equiparato tali delitti a quelli di criminalità organizzata, mentre la legge n. 7 del 2020, ha aggiunto alla categoria i delitti degli incaricati di pubblico servizio, con efficacia differita ai procedimenti iscritti dopo il 31 agosto 2020. Tale estensione è rilevante in considerazione della sproporzione tra i delitti compiuti dalla criminalità organizzata, rispetto ai reati contro la pubblica

l'intercettazione è richiesta, sempre se necessaria alla prosecuzione delle indagini, ma anche con "sufficienti" indizi di reato, e sono previsti termini di durata più dilatati, consentendo l'intercettazione in termini non superiori ai quaranta giorni, con eventuale proroga di venti giorni; se vi è urgenza, alla proroga provvede il pubblico ministero con successiva convalida del giudice (art. 13 d.l. 1991 n. 152). Anche le intercettazioni ambientali hanno più ampio respiro, potendo essere disposte nel domicilio sempre, anche quando si ritenga che nei luoghi menzionati si sta svolgendo l'attività criminosa (art. 13 d.l. 1991 n. 152)[275].

Le intercettazioni dovranno essere sempre autorizzate dal giudice attraverso un decreto succintamente motivato, anche quando queste saranno disposte con urgenza dal pubblico ministero, poiché a norma dell'art. 267 c.p.p. il giudice dovrà decidere sulla convalida entro le quarantotto ore successive, altrimenti i risultati non potranno essere utilizzati (art. 267, comma 2). Successivamente all'autorizzazione, il pubblico ministero emana un decreto esecutivo che regola le modalità e la durata delle operazioni (art. 267, comma 3), procedendo personalmente o coadiuvandosi di un ufficiale di polizia giudiziaria (art. 267, comma 4). L'attività intercettiva potrà essere svolta mediante l'uso di determinati apparecchi previsti dalla procura o in dotazione alla P.G., o se motivate nel decreto, attraverso impianti di pubblico servizio o presso la polizia giudiziaria (art. 268, comma 3).

Le utenze intercettabili sono molteplici, poiché, secondo quanto previsto dal codice possono estendersi alle utenze degli indagati, dei testimoni, e delle persone estranee ai fatti, quando queste ultime siano destinatarie di comunicazioni provenienti da indagati o da testimoni. Tuttavia, l'attività intercettiva può subire delle limitazioni: essa può essere subordinata ad un'autorizzazione a procedere, nel caso in cui debba essere disposta nei confronti di determinate persone che rivestono profili costituzionali (c.d. intercettazioni nei confronti dei parlamentari[276]), e può essere vietata nei confronti

---

amministrazione, non solo dai pubblici ufficiali, ma anche degli incaricati di pubblico servizio, categoria ampia comprendenti anche soggetti privati che svolgono servizi concessi dagli enti pubblici.

[275] Tale requisito occorre per i reati di minaccia per mezzo del telefono.

[276] "Le intercettazioni che riguardano i membri del parlamento sono disciplinate dalla legge 20 giugno 2003, n. 140, modificata da varie sentenze della Corte costituzionale. Si dividono in tre categorie: intercettazioni dirette, quando sono sottoposti ad intercettazione utenze o luoghi appartenenti al

di figure processuali, come il difensore, consulenti tecnici e dei loro ausiliari, in modo che sia tutelato il segreto professionale; nel caso in cui tali divieti vengano violati, le intercettazioni saranno inutilizzabili. Sono previste diverse ipotesi di inutilizzabilità delle intercettazioni previste dall'art. 271, comma 1: quando le intercettazioni sono state eseguite al di "fuori dei casi consentiti dalla legge"; quando le intercettazioni sono state compiute non osservando i presupposti e le forme stabilite dai provvedimenti, secondo quanto previsto dall'art. 267 c.p.p.; quando non siano stati osservati i commi 1 e 3 dell'art. 268 c.p.p., relativi alla mancata registrazione e redazione del verbale sommario delle operazioni, o per intercettazioni compiute al di fuori degli impianti installati nella procura della Repubblica, senza che siano motivate le ragioni di urgenza[277]. Inoltre, vi sono delle ipotesi eccezionali per cui vige un divieto di intercettazione assoluto, poiché secondo la Corte Costituzionale[278], vi sono "ragioni di ordine sostanziale, espressive di un'esigenza di tutela "rafforzata" di determinati colloqui in funzione di salvaguardia di valori e diritti di rilievo costituzionale che si affiancano al generale interesse alla segretezza delle comunicazioni": si tratta delle intercettazioni riguardanti le conversazioni del Presidente della Repubblica, e delle comunicazioni tra soggetti appartenenti ai servizi segreti, le quali, se acquisite, devono essere distrutte dal giudice.

Il legislatore prevede, al fine di contrastare reati gravissimi, l'uso di intercettazioni che, per la loro funzione, non rientrano nelle finalità del processo penale; tuttavia, mantiene sullo svolgimento delle stesse un controllo ad opera del pubblico ministero in ragione dell'indipendenza che l'ordinamento costituzionale garantisce a tale organo (226, comma 1, disp. att. c.p.p.).

---

parlamentare o nella sua disponibilità; intercettazioni indirette, quando l'attività di captazione interessa utenze intestate a differenti soggetti che, tuttavia, possono ritenersi interlocutori abituali del parlamentare, o concerne luoghi a lui non appartenenti, ma che possono presumersi dal medesimo frequentati (C. cost. n. 114 del 2010); intercettazioni casuali, quando l'ascolto è del tutto accidentale e se il giudice delle indagini preliminari le ritenga irrilevanti, ne decide in camera di consiglio la distruzione ai sensi dell'art. 269, commi 2 e 3; viceversa, se il giudice considera rilevanti tali intercettazioni, egli deve chiedere un'autorizzazione alla Camera cui il parlamentare appartiene che se non concessa, le rende inutilizzabili nei confronti del parlamentare coinvolto", in P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 425.

[277] *Ibdem*, p. 408.

[278] Si veda, sent. Corte Cost. n. 1 del 2013.

II.6.3 Le riforme.

La disciplina delle intercettazioni negli ultimi anni ha subito numerosi interventi riformatori riguardanti principalmente il bilanciamento da un lato, della compressione per fini processuali della segretezza delle comunicazioni, e dall'altro, la tutela alla riservatezza delle conversazioni private, non attinenti alle indagini, dei soggetti non indagati. Il decreto legislativo n. 216 del 2017 (c.d. riforma Orlando) aveva cercato di disciplinare i due interessi in conflitto, ma a causa dei continui rinvii, nella legge approvata risultavano assenti i punti focali più importanti. Con la successiva conversione con modifiche nella legge 28 febbraio 2020, n. 7, si è dato luogo ad una controriforma, ulteriormente differita dall'entrata in vigore del decreto-legge n. 28 del 2020, conv. in legge n. 70 del 2020.

Gli interventi in questione hanno diviso la disciplina delle intercettazioni, prevedendo un regime normativo differente per i procedimenti iscritti nel registro delle notizie di reato fino al 31 agosto 2020, che continuano a seguire la disciplina originaria del codice, e i procedimenti iscritti dopo tale data, che seguiranno le nuove regole.

II.6.3.1 La riforma Orlando, non entrata in vigore.

La disciplina originaria delle intercettazioni era stata profondamente modificata dal d.lgs. n. 216 del 2017, emanato dal Governo sulla base della delega contenuta nella legge n. 103 del 2017 (c.d. riforma Orlando). L'entrata in vigore della riforma sulle intercettazioni era stata posticipata dal Governo dal 26 luglio 2018 al 1° aprile 2019[279], e poi nuovamente al 1° agosto 2019[280], e ancora al 1° gennaio 2020[281].

La *ratio* della legge delega consisteva nel tutelare l'efficienza delle indagini e la riservatezza delle persone intercettate occasionalmente, e dei destinatari delle intercettazioni quando fossero state captate conversazioni riguardanti a fatti privati non

[279] Decreto - legge n. 91 del 2018, convertito nella legge n. 108 del 2018.

[280] Legge 31 dicembre 2018, n. 145 (legge di bilancio), art. 1, comma 1139, lett a.

[281] Decreto - legge 14 giugno 2019, n. 53, conv. nella legge n. 77 del 2019.

rilevanti per le indagini[282]. Ciò, in ragione della mancata introduzione di una sanzione più severa riguardante la pubblicazione arbitraria di atti processuali segreti oblazionabile con una somma pari a 129 euro (art. 684 c.p.). Ed è per questo motivo che la riforma Orlando (d.lgs. n. 216 del 2017) aveva imposto alla polizia giudiziaria e al pubblico ministero, il compito di sviluppare una selezione immediata delle dichiarazioni non rilevanti: l'acquisizione delle dichiarazioni, custodite in archivio con accesso limitato e coperte da segreto, avrebbe tardato fino al momento in cui il giudice avesse valutato, in contraddittorio tra le parti, rilevanti o meno le conversazioni captate. Tale riforma, oltre ad essere per certi versi di complicata attuazione, poneva un veto sulle informazioni acquisite che non potevano essere selezionate e controllate dagli interessati in ragione della segretezza di queste: ciò ha comportato un ostacolo al diritto di stampa, che attraverso la conoscenza delle dichiarazioni captate avrebbe potuto sortire effetti economici e politici eccezionali, ed è per questo che il Ministro della giustizia in carica aveva definito la riforma Orlando come «un bavaglio all'informazione».

I continui rinvii hanno portato il Governo ad operare una scelta particolare, in quanto il decreto-legge 30 dicembre 2019, n. 161 è stato formulato dal Ministero della Giustizia senza che vi sia stata convocazione o considerazioni di esperti del settore giuridico; inoltre, la conversione in legge n. 7 del 2020, è avvenuta senza nessun dibattito parlamentare.

A causa dell'improvvisa pandemia mondiale da Covid19, l'entrata in vigore delle nuove norme è stata ulteriormente rinviata al 1° settembre 2020 dal decreto-legge 30 aprile 2020, n. 28, conv. nella legge n. 70 del 2020[283]. Tale riforma ha distinto i procedimenti in base alla data in cui sono stati iscritti nel registro delle notizie di reato: quelli iscritti fino al 31 agosto 2020 seguono la disciplina originaria delle intercettazioni anteriore alla riforma Orlando, considerando che il d.lgs. n. 216 del 2017 non è mai entrato in vigore; i procedimenti iscritti dopo tale data seguiranno la normativa prevista dalla riforma c.d. Bonafede, che discostandosi dalla riforma Orlando, ha apportato modifiche legislative che mantengono l'assetto originale delle intercettazioni, anche in

[282] Nel dettaglio, C. CONTI, *Le nuove norme sulla riservatezza delle intercettazioni: anatomia di una riforma discussa*, in *Giur. it. Speciale*, 2018, 1754.

[283] P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 410 ss.

relazione all'uso del captatore informatico, intervenendo però sulla problematica disciplina dell'utilizzabilità delle intercettazioni in procedimenti diversi, e di cui saranno trattati gli aspetti più essenziali.

II.6.3.2 Gli aspetti essenziali della riforma c.d. Bonafede.

Il pregio della controriforma risiede nel controllo, precedentemente assente a livello normativo, sulle trascrizioni delle intercettazioni, svincolandolo da superflui formalismi procedurali. La nuova disciplina si presenta come il giusto compromesso tra esigenze investigative, dove non sempre la celerità delle operazioni è proporzionale alla fruttuosità dei risultati, e finalità di riservatezza[284].

La polizia redige un verbale del contenuto delle intercettazioni, che dovrà essere controllato successivamente dal pubblico ministero affinché non vengano riportate le espressioni lesive della reputazione delle persone, e le espressioni che riguardano dati personali sensibili[285]; tuttavia, tale norma è soggetta ad eccezione nel caso in cui tali espressioni siano rilevanti ai fini delle indagini (art. 268, comma 2-bis). Inoltre, è stato previsto un divieto delle intercettazioni, casualmente ottenute, delle conversazioni dei difensori e consulenti tecnici svoltesi tra di loro e con i loro assistiti (art. 103, commi 5 - 7), per cui il loro contenuto non sarà trascritto nel verbale delle operazioni, ma saranno indicati solo "la data, l'ora e il dispositivo su cui la registrazione è intervenuta" (art. 103, comma 7). I verbali trascritti saranno trasmessi al pubblico ministero, e il procuratore della Repubblica disporrà e assicurerà la conservazione nell'archivio

---

[284] D. PRETTI, *La metamorfosi delle intercettazioni: la contro-riforma Bonafede e l'inarrestabile mito della segretezza delle comunicazioni*, in *Sist. pen*., 2/2020, p. 75 ss. V. anche, a titolo esemplificativo, come ulteriori contributi sul tema: M. GIALUZ (a cura di), *Le nuove intercettazioni. Legge 28 febbraio 2020, n. 7*, in Diritto dell'internet, Supplemento al fascicolo, 2020, 3; T. BENE, *Intercettazioni. Intrecci e discordanza di idee nella stagione delle riforme processuali*, in *Diritto penale e processo*, 2020, fasc. 12, pp. 1641-1647; A. CAMON, *Il nuovo procedimento di spoglio dei risultati delle intercettazioni*, in La *Legislazione penale*, 2020, fasc. 11, pp. 32; F. CAPRIOLI, *La procedura di filtro delle comunicazioni rilevanti nella legge di riforma della disciplina delle intercettazioni (The Filtering Procedure of the Relevant Communications in the New Wiretap Law)*, in *Cassazione penale*, 2020, fasc. 3, pp. 1384-1416; L. FILIPPI, *Intercettazioni: "habemus legem"!*, in Diritto penale e processo, 2020, fasc. 4, pp. 453-466, 2020; M. GIALUZ, *Riservatezza e nuova disciplina delle intercettazioni*, in *Rivista penale*, 2020, fasc. 7-8, pp. 667-677.

[285] Si tratta dei dati personali in grado di rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza.

digitale, ritenuto più sicuro della segreteria del P.M. (art. 269, comma 1 e art. 89-*bis*, comma 2 disp. att.); tale deposito potrà essere differito dal pubblico ministero quando da esso può derivare un grave pregiudizio per le indagini, che dovrà essere autorizzato dal g.i.p. e che non può protrarsi oltre la chiusura delle indagini (art. 268, comma 5). I verbali e le registrazioni dovranno essere depositati entro cinque giorni dalla conclusione delle operazioni (o dalla data in cui è scaduto il differimento), presso l'archivio digitale insieme ai decreti riguardanti le intercettazioni medesime (art. 268, commi 4 e 5), di cui è dato immediato avviso ai difensori delle parti. Il materiale contenuto nell'archivio è coperto da segreto e non è pubblicabile, nemmeno parzialmente come notizia generica, fino all'acquisizione delle intercettazioni, secondo i meccanismi normativamente stabiliti; una simile ricostruzione si ricava dall'interpretazione dell'art. 269, comma 1, confermata dal nuovo comma 2-*bis* dell'art. 114 per cui «è sempre vietata la pubblicazione, anche parziale, del contenuto delle intercettazioni non acquisite ai sensi degli artt. 268, 415-*bis* o 454». Inoltre, i difensori avranno la facoltà, entro il termine fissato dal pubblico ministero, di indicare i verbali e le registrazioni che ritengono rilevanti, irrilevanti o inutilizzabili. Scaduto il termine, il pubblico ministero e i difensori sono avvisati della data e del luogo dell'udienza di stralcio, almeno ventiquattro ore prima[286].

Durante l'udienza di stralcio il g.i.p. potrà emettere diversi provvedimenti relativi alla rilevanza o meno dei verbali e delle registrazioni (art. 268, commi 6 e 7). Ciò sarà ritenuto irrilevante sarà restituito al procuratore della Repubblica, che collocherà le intercettazioni nell'archivio digitale protetto da segreto e saranno conservate fino a quando la sentenza non sarà più soggetta a impugnazione (art. 269, comma 1 e art. 89-*bis*, comma 2, disp. att.), mentre le intercettazioni inutilizzabili o dal contenuto riservato dovranno essere distrutte. Il giudice, anche nel corso delle attività di formazione del fascicolo del dibattimento ai sensi dell'art. 431, disporrà la trascrizione integrale delle registrazioni, di cui i difensori possono estrarne copia. Successivamente all'acquisizione nel fascicolo dibattimentale, le intercettazioni potranno essere pubblicate come notizia generica.

[286] P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 414 ss.

Le nuove disposizioni lasciano dubbi interpretativi sulla possibilità di rinvio dell'udienza di stralcio, che potrebbe svolgersi non in fase di indagini[287]. Proprio per superare tali inconvenienti, il legislatore ha introdotto, per il procedimento ordinario, il comma 2-*bis* all'art. 415-*bis* c.p.p. e, parallelamente, il comma 2-*bis* all'art. 454 c.p.p. per il caso di giudizio immediato: il comma 2-*bis* dell'art. 415-*bis* stabilisce l'ipotesi in cui, durante le indagini, il pubblico ministero sia stato autorizzato dal giudice al deposito differito e, pertanto, l'avviso di conclusione delle indagini dovrà contenere l'avvertimento che il difensore dell'indagato potrà esaminare gli atti depositati relativi alle intercettazioni, depositando eventualmente, tramite istanza sottoposta a decisione del P.M. con decreto motivato, l'elenco delle ulteriori registrazioni rilevanti e di cui ne chiede copia; se l'istanza sarà rigettata, il difensore potrà chiedere al giudice di procedere nelle forme dell'udienza di stralcio ordinaria.

La riforma c.d. Bonafede ha inciso anche sulla questione relativa all'uso delle intercettazioni in procedimenti diversi da quelli autorizzati[288]: la regola stabilita dall'art. 270, comma 1, c.p.p. prevede che i risultati delle intercettazioni non possano essere utilizzati in procedimenti diversi da quelli nei quali sono state disposte, salvo che siano indispensabili per l'accertamento dei delitti per i quali è obbligatorio l'arresto in flagranza. La questione è stata oggetto della sentenza a Sezioni unite della Corte di Cassazione[289], che, in senso in parte correttivo degli orientamenti giurisprudenziali formatisi in precedenza, ha ritenuto che non ci si troverebbe davanti ad un "altro procedimento", se questo ha ad oggetto quei reati «che risultino connessi (art. 12 c.p.p.)

---

[287] Il comma 7 dell'art. 268 dà per scontato che la trascrizione delle intercettazioni, non effettuata in precedenza, possa avvenire «nel corso delle attività di formazione del fascicolo per il dibattimento. In tal caso, il giudice deve disporre (se non disposto in precedenza) la trascrizione integrale delle registrazioni delle intercettazioni che sono depositate nel fascicolo delle indagini in quanto sono state ritenute rilevanti. Devono essere osservate le forme, i modi e le garanzie previsti per l'espletamento delle perizie. Il risultato deve essere inserito nel fascicolo per il dibattimento.

[288] P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 424 ss.

[289] Cass., Sez. Un., 25 giugno 2020, in CED n. 20127. «In altre parole, una volta che l'intercettazione sia stata legittimamente autorizzata all'origine, i suoi risultati potrebbero valere per qualunque reato successivamente emerso nel corso delle operazioni, a prescindere dalla specifica presenza dei presupposti per una intercettazione. Si deve rilevare che se invece il divieto fosse applicato l'intercettazione potrebbe essere utilizzata solo come *notitia criminis*, in base alla quale aprire un'indagine alla ricerca di elementi utili per l'accertamento del diverso reato.», così G. ILLUMINATI, *Osservazioni a margine di Cass., Sez. un., 28 novembre 2019 (dep. 2 gennaio 2020), n. 50, Pres. Carcano, est. Caputo*, in *Sistema Penale*, 30 gennaio 2020.

a quelli in relazione ai quali l'autorizzazione era stata disposta, sempreché rientrino nei limiti di ammissibilità previsti dalla legge»: pertanto, le intercettazioni potranno essere utilizzate per la prova di fatti diversi da quelli per cui erano state autorizzate solo se vi sarà «un preciso collegamento tra i fatti per i quali erano state mano a mano autorizzate e prorogate le operazioni di intercettazione e quelli per i quali, anche sulla base delle conversazioni intercettate, è stata confermata la condanna»[290]. Riguardo ai procedimenti iscritti dopo il 31 agosto 2020 il divieto posto dall'art. 270, comma 1 resterà valido; tuttavia, i limiti tracciati dalle Sezioni unite sono stati superati dalla legge di conversione n. 7 del 2020, che ha permesso l'utilizzo delle nuove intercettazioni non autorizzate che risultino "rilevanti e indispensabili" anche per l'accertamento dei reati per cui è ammesso il ricorso alle intercettazioni. Per i procedimenti iscritti dopo il 31 agosto 2020, inoltre, l'uso delle intercettazioni per reati diversi da quelli autorizzati è stato ampliato con l'introduzione del comma 1-*bis* dell'art. 270 c.p.p., per cui i risultati delle intercettazioni operate con captatore informatico su dispositivo elettronico portatile possono essere utilizzate per la prova di reati diversi da quelli autorizzati con decreto, se compresi tra quelli indicati dall'art. 266, comma 2-*bis*, riguardanti anche i delitti contro la pubblica amministrazione commessi da pubblici ufficiali e incaricati di pubblico servizio.

II.6.3.3 Le norme sulle intercettazioni mediante captatore informatico.

Il captatore informatico[291] è uno strumento ormai indispensabile, in ragione delle nuove modalità operative di elusione dei reati che la criminalità realizza, tali da mettere fuori gioco le intercettazioni tradizionali di tipo passivo, più limitate nel collegamento comunicativo tra gli interlocutori. Ed è per questo motivo che sono stati previsti dal codice casi in cui potrà compiersi l'intercettazione ambientale[292] attraverso

[290] Ciò nel rispetto delle riserve di legge e di giurisdizione imposte dall'art. 15 della Costituzione. In tal senso, Cass., Sez. un., 28 novembre 2019 - 2 gennaio 2020, n. 51, *Cavallo*, in CED, n. 277395.

[291] *Infra*, § III.1.

[292] "L'oggetto delle nuove disposizioni sul captatore informatico è circoscritto: esse regolano soltanto l'ipotesi in cui il virus viene usato per mettere in funzione di nascosto il microfono dell'apparecchio portatile infettato; curiosamente, non disciplinano nemmeno il caso – pur contiguo – in cui si voglia eseguire un'intercettazione ambientale mandando il *trojan* in un computer fisso; benché si tratti d'una

l'installazione del captatore informatico su dispositivi elettronici portatili, attraverso l'impiego di programmi conformi ai requisiti tecnici stabiliti dal decreto del Ministro della giustizia (art. 89, comma 2 disp. att.)[293].

Dopo la storica sentenza delle Sezioni Unite "Scurato", che ha enunciato diversi princìpi di diritto in relazione all'utilizzo del captatore a fini intercettivi[294], si sono susseguite diverse riforme che hanno trasformato per certi versi l'assetto normativo delle intercettazioni, modificando anche i procedimenti riguardanti l'attività di captazione. In particolar modo, il decreto-legge n. 161 del 2019, conv. nella legge n. 7 del 2020, ha introdotto una normativa sull'uso del captatore e che si applica ai procedimenti iscritti dopo il 31 agosto 2020.

I requisiti per utilizzare il captatore informatico cambiano a seconda che si tratti di delitti comuni (art. 266, comma 2), o delitti di criminalità organizzata e assimilati (art. 266, comma 2-*bis*)[295]: nel primo caso, il giudice autorizza l'intercettazione captativa attraverso un decreto motivato che dia conto dell'esistenza di gravi indizi di reato e dell'assoluta indispensabilità di tale strumento eccezionale per il proseguo delle indagini, e delle modalità operative del captatore, attraverso espresse indicazioni dei luoghi e del tempo in cui dovrà essere attivato il microfono; nel secondo caso, il giudice dovrà autorizzare l'intercettazione con un decreto motivato più sintetico, contenente, a differenza del primo, i sufficienti indizi di reato che rendono indispensabile l'uso dell'intercettazione "attiva", le modalità operative, senza ulteriori precisazioni sui tempi e luoghi in cui è consentita l'accensione del microfono. Con riferimento alla possibilità di impiego del captatore per le intercettazioni nel domicilio, viene in rilievo la distinzione tra i gravi reati per cui si procede (per i delitti previsti dall'art. 51, commi 3-*bis* e 3-*quater*, l'intercettazione tra presenti è sempre consentita, per i delitti dei pubblici

---

lacuna gratuita, si deve ritenere che l'operazione sia vietata", A. CAMON, *Fondamenti di procedura penale*, Assago, Wolters Kluwer, 2021.

[293] Requisiti fissati con D.M. 20 aprile 2018, pubblicato sul Bollettino Ufficiale del Ministero della Giustizia il 31 maggio. Manca un espresso riferimento alle limitazioni imposte ai *software* per l'effettuazione delle sole operazioni autorizzate. In rilievo, le osservazioni del Garante Privacy, nella Segnalazione al Parlamento e al Governo sulle intercettazioni con captatore informatico (30 aprile 2019).

[294] *Infra*, § III.1, riguardo a Cass., Sez. un., 28 aprile - 1° luglio 2016, n. 26889, *Scurato*, in Cass. pen., 2016, 3536.

[295] P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 423.

ufficiali e degli incaricati di pubblico servizio contro la pubblica amministrazione, l'intercettazione è consentita nei luoghi domiciliari, previa indicazione delle ragioni che ne giustificano l'utilizzo[296]).

L'ufficiale di polizia giudiziaria potrà avvalersi di ausiliari, di cui all'art. 348, comma 4, per lo svolgimento delle operazioni riguardanti le registrazioni effettuate attraverso il captatore, relative alle conversazioni tra presenti. Di tali registrazioni, che saranno conferite esclusivamente negli impianti della procura della Repubblica, sarà redatto un verbale delle operazioni, che indicherà sia il tipo di programma impiegato e, nei casi in cui è stabilito, i luoghi in cui si svolgono le comunicazioni o conversazioni, sia il termine delle attività intercettive, caratterizzate dalla disattivazione del captatore in modo che non possa dar luogo a successivi impieghi (art. 89, disp. att.). Inoltre, è prevista la sanzione dell'inutilizzabilità per i dati acquisiti nel corso delle attività preliminari all'installazione del captatore informatico sul dispositivo elettronico portatile e per i dati acquisiti al di fuori dei limiti di tempo e di luogo indicati nel decreto autorizzativo (art. 271, comma 1-*bis*)[297].

Occorre sottolineare come la sentenza "Scurato" abbia esaltato le caratteristiche del captatore informatico, mettendo in luce anche i diversi utilizzi dello stesso, come la possibilità di effettuare le c.d. perquisizioni *online*, oggetto del prossimo capitolo.

[296] Per tali delitti, è previsto che, nei casi di urgenza, il p.m. possa disporre, con decreto motivato che indichi l'impossibilità di attendere il provvedimento del giudice, l'intercettazione mediante il captatore, previa successiva convalida del giudice entro quarantotto ore (art. 267, comma 2-*bis*).

[297] P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 423.

CAPITOLO III

LA c.d. PERQUISIZIONE *ONLINE*, IN BILICO TRA DISCIPLINA DELLE INTERCETTAZIONI E REGIME DELLE PERQUISIZIONI

SOMMARIO: III.1 La poliedricità del captatore informatico. - III.1.2 La sentenza "Scurato". – III.2 Il pendolarismo tra le "intercettazioni" e le "perquisizioni *online*". – III.2.2 Le *Online-Durchsuchung*: le incertezze e le evoluzioni giurisprudenziali del diritto costituzionale tedesco. – III.3 Il bilanciamento tra le garanzie costituzionali e le esigenze investigative nel diritto italiano. – III.4 L'inquadramento giurisprudenziale delle perquisizioni *online*. – III.4.1 I profili di atipicità delle perquisizioni *online*. – III.4.2 Il "documento informatico" come soluzione interpretativa. – III.5 Perquisizioni *online* e finalità preventive. – III.5.1 Il caso "*Ryanair*" e il divieto di perquisizioni *ad explorandum*. – III.6.1 L'inammissibilità delle perquisizioni occulte: un punto di partenza per il futuro.

III.1 La poliedricità del captatore informatico.

Tra le tecniche investigative più diffuse nel processo penale, spicca per la sua potenzialità e per la capacità di incidere sui diritti costituzionalmente garantiti, l'uso del captatore informatico. Il captatore informatico[298] è un *software* facente parte della categoria dei *malicious software* (c.d. *malware*)[299], ossia un virus informatico, che una volta installato, in modo furtivo, all'interno del dispositivo digitale *target* (es. cellulare, *tablet*, computer), è in grado di svolgere attività di ricerca e di sorveglianza *online* molto invasive, e di seguirne l'attività mediante una sorta di *shadowing*[300] ossia, attraverso un controllo dell'apparecchiatura occulto effettuato da remoto. Il programma in questione è composto da due moduli, *server* (programma infettivo installato) e *client* (virus che consente la captazione), collegati tra loro.

L'inoculazione del captatore nel dispositivo bersaglio può avvenire da vicino o da remoto: l'installazione fisica è un'ipotesi molto rara, caratterizzata dall'inserimento

---

[298] Vedi, S., MARCOLINI, *Le cosiddette perquisizioni on-line (o perquisizioni elettroniche)*, in *Cass. pen*., 07/08, 2010, p. 2855 ss.; inoltre, S. ATERNO, *Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto e la soluzione per la lotta contro l'utilizzo del cloud criminal*, in G. COSTABILE – A. ATTANASIO (a cura di), IISFA Memberbook, 2012, *Digital Forensics.* Condivisione della conoscenza tra i membri dell'IISFA Italian Chapter, Forlì, 2013, pp. 1 ss.; S. COLAIOCCO, *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *Arch. Pen*., 1, 2014; M. TROGU, *Intrusioni segrete nel domicilio informatico*, in A. SCALFATI (a cura di), *Le indagini atipiche*, cit., 2019; E. APRILE, *voce Captazioni atipiche (suoni, immagini, segnali)*, in A. SCALFATI (diretto da), in *Dig. proc. pen. online*, Giappichelli, Torino, 2013.

[299] *Malware* è concetto che comprende diverse *species* di virus conosciuti, *infra*, § I.2.

[300] Tradotto dall'inglese "ombra", si intende "la puntuale osservazione e rilevazione delle micro-attività quotidiane della persona sottoposta ad indagine".

di un programma (c.d. *backdoor*), capace di bypassare le autenticazioni richieste per l'accesso al sistema, effettuato direttamente sull'*hardware* del dispositivo da controllare; l'installazione da remoto è, invece, l'ipotesi più frequente e più semplice, in quanto, l'inoculazione del virus è mascherata in un allegato e-mail che induce l'utente all'apertura, in un SMS[301], o nella richiesta di aggiornamento di un'applicazione, e richiede l'ignara "collaborazione" dell'indagato che dovrà credere all'inganno (è per questo motivo che spesso si tratta di *malware* di tipo c.d. *trojan horses*[302], "cavallo di Troia", che come richiama il nome stesso, hanno la capacità di fingersi una cosa, come ad esempio un documento o un programma innocuo, pur essendone un'altra). Tuttavia, l'espansione delle conoscenze della materia tecnologica può rendere questa "ignara collaborazione" non sempre realizzabile, per cui spesso l'unica alternativa auspicabile per effettuare un controllo da remoto consisterebbe in una "intercettazione telematica"[303], in cui il fornitore di servizi informatico-telematici consegnerà agli inquirenti una serie di dati digitali che ruotano attorno all'indagato. Inoltre, numerosi sono gli sviluppi di carattere difensivo, che attraverso i *firewall* e ai *software antivirus* proteggono il dispositivo dagli attacchi in questione.

Il captatore è uno strumento poliedrico dalle ampie potenzialità applicative: grazie a tale virus, è possibile realizzare attività di *online search* e di *online surveillance*[304] (non escludendo un possibile ampliamento delle stesse in futuro); inoltre, secondo alcuni rientrerebbero nella categoria delle *online surveillance*, anche le ipotesi di gestione in tempo reale delle periferiche del dispositivo *target*[305] come la

---

[301] A. CAMON, *Cavalli di Troia in Cassazione*, in *Arch. nuova proc. pen.*, 2017, p. 91; R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuschung. La prospettiva delle investigazioni ad alto contenuto tecnologico ed il bilanciamento con i diritti inviolabili della persona*, in *Riv. trim. dir. pen. economia*, 2009, p. 698. Per una classificazione dei programmi da installare da remoto, «in base al numero di *click* che l'utente deve fare sul proprio dispositivo per infettarsi», A. MIRIELLO, L. GOVERNATORI, *Captatore informatico: aspetti tecnici e criticità. I nostri dati sono in buone mani?*, in www.scienzeforensi.org, 30 maggio 2020.

[302] Sulle funzioni del *trojan horse* si veda M. ZONARO, *Il Trojan - Aspetti tecnici e operativi per l'utilizzo di un innovativo strumento di intercettazione*, in *Parole alla difesa*, 2016, n. 1, p. 164.

[303] Art. 266-*bis* c.p.p.

[304] Tradotte rispettivamente come "copiatore informatico" e "appostamento informatico", vedi, M. TROGU, *Intrusioni segrete nel domicilio informatico*, cit., pp. 584 ss.

[305] P. FELICIONI, *L'acquisizione da remoto dei dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Processo penale e giustizia*, n. 5, 2016, p. 124.

tastiera, microfono, schermo e *webcam*[306] , dunque, le operazioni consistenti nel far funzionare il captatore come una microspia idonea ad eseguire intercettazioni tra presenti[307]; diversamente, si potrebbe ipotizzare ad una sorta di *tertium genus*, con caratteristiche miste all'*online search* e all'*online surveillance*.

III.1.2 La sentenza "Scurato".

Le Sezioni unite si sono pronunciate su un caso relativo ad un procedimento per criminalità organizzata, in cui il g.i.p. aveva autorizzato una intercettazione che doveva avvenire nel luogo "nel quale era ubicato in quel momento il portatile"[308] su cui era installato il captatore informatico. In particolar modo, la sentenza del 28 aprile 2016 "Scurato"[309] oltre a stabilire l'uso del captatore informatico nei soli procedimenti per delitti di criminalità organizzata[310], chiarisce quali siano le funzioni ulteriori, rispetto alle tradizionali intercettazioni di conversazioni tra presenti, costituite: dalla captazione di tutto il traffico dei dati in entrata e in partenza del dispositivo *target* (navigazione in Internet, accesso alla posta elettronica); dalla decifrazione di tutto ciò che viene digitato sulla tastiera collegata al sistema, compresi *password* e numeri di carte di credito,

---

[306] Un esempio sono i *keylogger software*, che permettono la creazione dei *file* di *log*, acquisibili anche successivamente, contenenti ciò che viene digitato sulla tastiera (fisica o virtuale) del dispositivo. Così, R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online durchsuschung*, in *Riv. trim. dir. pen. ec*., 3, 2009, p. 697.

[307] M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali, Milano*, 2017. Inoltre, P. FELICIONI, *Le fattispecie "atipiche" e l'impiego processuale*, in T. BENE (a cura di), *L'intercettazione di comunicazioni*, Bari, Cacucci Editore, 2018, p. 303.

[308] La Cassazione ha dato per scontato che il captatore non permettesse di azionare il microfono da remoto e non fosse in grado di distinguere tra i luoghi (domiciliari o meno) nei quali la captazione era in atto. Di conseguenza, la S.C. ha ritenuto non utilizzabile il captatore nei casi ordinari in cui l'intercettazione domiciliare richiede il presupposto specifico che in quel luogo si stia svolgendo l'attività delittuosa. Viceversa, ha permesso l'uso del captatore soltanto per i delitti di criminalità organizzata per i quali, appunto, è consentita sempre la captazione tra presenti anche nel domicilio. Cfr. C. CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Dir. Pen e processo*, 2018, p. 1218.

[309] L. GIORDANO, *Dopo le sezioni unite sul "captatore informatico: avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*. *Osservazioni a seguito di Cass., SSUU, sent. 28 aprile 2016 (dep. 1° luglio 2016), n. 26889, Pres. Canzio, Rel. Romis, ric. Scurato*, in *Diritto penale contemporaneo*, 2017, 3, pp. 177-195.

[310] Per reati di criminalità organizzata devono intendersi non solo quelli elencati nell'art. 51, commi 3-*bis* e 3-*quater* c.p.p., ma anche quelli comunque facenti capo a un'associazione per delinquere, (art. 416 c.p.), correlata alle attività criminose più diverse, con esclusione del mero concorso di persone nel reato.

(*keylogger*) e visualizzato sullo schermo (*screenshot* e *screencast*); dall'attivazione da remoto di microfono e *webcam*, tale da poter spiare l'indagato, registrando suoni e le conversazioni e acquisendo immagini; inoltre, è possibile effettuare attività di perquisizione nell'*hard disk*, potendo copiare, totalmente o parzialmente, le unità di memoria del sistema informatico bersaglio[311]. Si riesce, altresì, a "tracciare" gli spostamenti dell'utente, normalmente associati al dispositivo mobile, geolocalizzando il dispositivo attraverso il processo di c.d. *positioning* in un raggio inferiore a 20 metri[312], nonché, attraverso l'attivazione di microfono e telecamera, realizzare intercettazioni audio, fotografie e videoriprese[313], oltre a poter inserire nuovi *files*, modificarli o cancellare quelli esistenti.

La sentenza Scurato ha limitato intenzionalmente la propria pronuncia alle sole intercettazioni svolte a mezzo captatore, lasciando impregiudicata ogni questione relativa alle ulteriori attività potenzialmente lesiva dei diritti fondamentali. In assenza di una normativa specifica, si ritiene che tali operazioni atipiche vengano precluse in base al "principio di non sostituibilità", enunciato dalle Sezioni unite nella storica sentenza

---

311 La sentenza Cass., sez. V, 30 maggio - 20 ottobre 2017, n. 48370, *Occhionero*, in CED, n. 271412, sostiene che i flussi unidirezionali di dati captati rientrano nel concetto di "intercettazione telematica" di cui all'art. 266-*bis*. Questa sentenza, oltre a riaffermare il principio espresso dalla sentenza Scurato, secondo cui «l'intercettazione di comunicazioni tra presenti con l'installazione di un captatore informatico che segue i movimenti di chi usa un dispositivo elettronico è consentita nei soli procedimenti per delitti di criminalità organizzata, senza una necessità di indicazione dei luoghi, a prescindere dal compimento ivi dell'attività criminosa», ha precisato che in tale sentenza non si esclude l'utilizzo del captatore informatico per eseguire una captazione di flussi telematici, sebbene non espressamente menzionata, ritenendo legittima l'intercettazione telematica realizzata attraverso captatore informatico, e ricompresa nell'alveo dell'art. 266-*bis*. In precedenza, Cass., sez. V, 14 ottobre 2009, n. 16556, *Virruso*, in CED, n. 246954, ha affermato che si tratta di un atto atipico che è legittimo se autorizzato con decreto del pubblico ministero.

312 La Corte di Cassazione (Cass., Sez. I, 28 maggio 2008, n. 21366, in C.E.D. Cass., n. 240092) ha ricondotto la tecnica del *positioning* ad un'attività da cui trarre tracce e elementi di prova, che «può farsi rientrare negli atti urgenti demandati agli organi di Polizia Giudiziaria, ai sensi degli artt. 55 e 348 c.p.p. e, come tale, non è subordinata alla preventiva autorizzazione da parte dell'autorità giudiziaria, consistendo l'operazione in una sorta di pedinamento a distanza», anche se sarebbe preferibile l'adozione di un decreto autorizzativo del P.M. Cfr. G. DI PAOLO, *Acquisizione dinamica dei dati relativi all'ubicazione del cellulare ed altre forme di localizzazione tecnologicamente assistita. Riflessioni a margine dell'esperienza statunitense*, in *Cass. pen*., n. 3, 2008, p. 1227.

313 L. PARLATO, *Le perquisizioni on-line: un tema che resta un tabù*, in G. GIOSTRA, R. ORLANDI (a cura di), *Revisioni Normative in Tema Di Intercettazioni: Riservatezza, Garanzie Difensive e Nuove Tecnologie Informatiche*, Giappichelli, Torino, 2021, p. 342.

Torcasio[314], e che è stato così riformulato dalla V Sezione nel noto caso di Garlasco[315]: «*quando il codice stabilisce un divieto probatorio oppure un'inutilizzabilità espressa, è vietato il ricorso ad altri strumenti processuali, tipici od atipici, finalizzati ad aggirare surrettiziamente un simile sbarramento*»[316].

III.2 Il pendolarismo tra le "intercettazioni" e le "perquisizioni *online*".

La problematica principale che investe la disciplina delle perquisizioni *online* riguarda la sua qualificazione giuridica, in considerazione delle sue peculiarità capaci di abbracciare numerose risultanze probatorie che potrebbero essere verosimilmente ricondotte alle operazioni tipiche dei mezzi di prova già previsti dalla legge, ossia le ispezioni, le perquisizioni e soprattutto le intercettazioni, che attualmente non sono in grado di poterne fornire una "copertura normativa"; pertanto, è necessario appurare quali siano le affinità e le differenze fondamentali con la disciplina tradizionale, in modo da limitare il campo operativo di queste ultime.

La tradizionale distinzione tra l'ispezione e la perquisizione è valida anche per i nuovi mezzi di ricerca della prova digitale: infatti, come è stato già sottolineato[317], l'attività ispettiva consiste in una sola osservazione esterna allo scopo di accertare le tracce e gli altri effetti materiali del reato, mentre la perquisizione *online* è una vera e propria attività di ricerca, che tuttavia, differisce dalle perquisizioni tradizionali, basate sulla ricerca del corpo o delle cose attinenti al reato, in quanto essa è finalizzata all'acquisizione occulta (l'attività svolta è completamente ignota all'indagato che non potrà esercitare nessun diritto difensivo, rispetto alle classiche perquisizioni che, pur essendo considerate un atto a "sorpresa", sono conoscibili da parte di quest'ultimo attraverso la consegna del decreto motivato e il successivo deposito degli atti nella

---

[314] Cass., Sez. un., 28 maggio 2003, *Torcasio*, in *Cass. pen*., 2004, 30 e in CED225467; Cass., Sez. un., 19 aprile 2012, *Pasqua*, in CED n. 252893. Nello stesso senso, Corte cost. n. 20 del 2017.

[315] Cass. pen., sez. V, 27 marzo - 7 settembre 2015, n. 36080, *Sollecito*, in www.giurisprudenzapenale.com, pag. 27 della motivazione in diritto (n. 4.3.2).

[316] P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 423.

[317] *Infra*, § II.3 Le ispezioni informatiche.

segreteria del p.m.) di elementi utili ai fini investigativi in un contesto spaziale e temporale indefinito.

Sembrerebbe più opportuno tentare di ricondurre tale materia nell'alveo degli articoli dedicati alle intercettazioni svolte attraverso il captatore. La nozione di intercettazione sancita dalla sentenza "Torcasio", che la inquadrava come una «captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti»[318], sembra essere ormai superata, a causa dell'evoluzione tecnologica degli strumenti captatativi che hanno indebolito i criteri su cui era basata tale definizione[319]. I nuovi dubbi emersi, che parte della giurisprudenza aveva già sollevato in passato[320] nel tentativo di regolare indagini "atipiche" diverse dall'intercettazione, si basano sulla confusione investigativa che potrebbe derivare dall'ampio utilizzo di un virus *trojan* all'interno di un dispositivo digitale, tale da rendere difficoltosa la distinzione tra le attività che rientrerebbero nel novero dell'art. 266, e quelle che dovrebbero rimanerne distinte.

Infatti, con l'espressione "perquisizioni *online*" si fa riferimento a tutte quelle altre attività di ricerca più aggressive, effettuate all'insaputa dell'interessato e volte sia ad esplorare un sistema informatico per trarne utili elementi probatori, sia a monitorarlo con costanza: sono proprio la segretezza, la durata prolungata e la possibilità di copiare una molteplicità diversi tipi di informazioni utili alle indagini, a rendere la perquisizione *online* un particolare mezzo di ricerca della prova[321].

Non essendovi una definizione univoca che possa ricomprendere tutte le attività realizzabili attraverso le perquisizioni *online*, si è soliti distinguere tra le attività principali di *online search* e *online surveillance*: le prime consistono nell'acquisire una copia di tutti gli elementi precostituiti e salvati nella memoria del dispositivo *target* (definita anche *one time copy*), trasmettendo via *web* (attraverso una connessione *wi-fi*)

---

[318] Cass., Sez. Un., 28 maggio 2003, *Torcasio*, in CED, n. 225465.

[319] «A vacillare sono soprattutto i criteri basati sulla necessaria concomitanza tra attività captativa segreta e interlocuzione tra i soggetti coinvolti nella comunicazione/conversazione, nonché lo stesso inquadramento di quest'ultima»: così, L. PARLATO, *Le perquisizioni on-line,* cit., p. 344.

[320] Cfr. per tutte Cass., 9 febbraio 2005, Rosi, in *Cass. pen.*, 2006, p. 606; Cass., Sez. Un., 23 febbraio 2000, *D'Amuri*, ivi, 2000, p. 2595.

[321] Così, L. PARLATO, *Le perquisizioni on-line,* cit., p. 344.

dati e informazioni agli organi inquirenti; le seconde consistono nel controllare in modo immediato e continuativo, come una sorta di "spia invisibile" il flusso informativo di un sistema digitale (e delle periferiche dello stesso), o intercorrente tra più sistemi informatici o telematici, anche attraverso Internet[322].

La collocazione sistematica delle attività appena descritte suscita delle criticità, relative al fatto che queste operazioni non potrebbero collocarsi nell'alveo delle c.d. intercettazioni ambientali, in quanto più invasive delle attività tradizionali che, dal punto di vista investigativo, non hanno dei confini delimitativi netti, potendo essere contaminate da ulteriori procedimenti istruttori fruibili con l'introduzione del *trojan*[323]; nemmeno scorporare l'ambito applicativo delle perquisizioni *online* al netto delle "intercettazioni vere e proprie" sembrerebbe un'operazione semplice, in ragione della mancanza di un loro inquadramento stabile[324]: in conclusione, si può affermare che l'oggetto di analisi di queste ultime riguarderebbe la ricerca e l'estrazione occulta di dati informatici, con la conseguente acquisizione delle prove digitali "statiche", differenti dalla captazione di elementi istruttori "dinamici"[325].

Pertanto, le due discipline, nonostante presentino numerosi profili di ambiguità, si differenziano in termini di intrusività, in considerazione del fatto che spesso l'oggetto di investigazione è lo *smartphone*, strumento che, essendo costantemente accanto all'utente, permetterebbe la captazione ininterrotta di ogni suono, rumore e conversazione che il soggetto sorvegliato o persone limitrofe potrebbero emettere, anche nei luoghi domiciliari[326]; pertanto, saranno ricompresi nella captazione elementi "non comunicativi" suscettibili di transitare in altri procedimenti nei limiti indicati dalla riformulazione dell'art. 270 c.p.p., secondo quanto previsto dalla riforma c.d. Bonafede

---

[322] A. BALSAMO, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*, in *Cass. pen.*, 2015, p. 2274 e nota 3; S. MARCOLINI, *Le cosiddette perquisizioni* on-line, cit., p. 2855 s.

[323] Il problema era rilevato dalla Corte costituzionale tedesca nel 2016: BVerfG, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09.

[324] L. PARLATO, *Le perquisizioni on-line,* cit., p. 345.

[325] Cfr. A. PAOLETTI, *La ricerca della prova penale nell'era delle nuove tecnologie informative*, Key, 2020, p. 6 s. e 413 ss.

[326] Cfr. Cass., Sez. Un., 28 aprile 2016, *Scurato*.

del 2020[327]; la disciplina delle perquisizioni *online*, pertanto, implica una maggiore compressione del sistema delle tutele individuali rispetto alle classiche intercettazioni, a causa soprattutto dell'ingente presenza di risultati probatori molto ampi e articolati, a tal punto da non essere distinguibili tra loro, che potrebbero vanificare le esigenze investigative e difensive, rendendo impossibile l'applicazione delle nuove contromisure stabilite dalla riforma del 2020, riguardanti lo stralcio e l'archiviazione digitale[328].

Così delimitata l'area delle perquisizioni *online*, possiamo trovare ulteriori analogie con la fattispecie tedesca della *Online-Durchsuchung*[329], ammessa in ambiti marginali nell'ordinamento tedesco per finalità preventive, a causa delle stesse difficoltà inquadrative che ha tale disciplina rispetto alle classiche intercettazioni stabilite *ex* § 100a StPO.

III.2.2 Le *Online-Durchsuchung*: le incertezze e le evoluzioni giurisprudenziali del diritto costituzionale tedesco.

Prima delle recenti riforme, la Corte costituzionale federale (*BVerfG)*, si era già occupata della c.d. *Online-Durchsuchung*, delineandone il perimetro dei principi costituzionali da rispettare, le attività stabilite nella legge federale[330], gli aspetti tecnici del codice di rito e i profili pratici.

Seguendo le evoluzioni giurisprudenziali degli altri Stati relative alle garanzie sulla libertà della persona[331], l'ordinamento tedesco, nella pronuncia del 27 febbraio

---

[327] Cass., Sez. Un., 26 giugno 2014, *Floris* e altri, in *Cass. pen.*, 2014, p. 4046.

[328] L. PARLATO, *Le perquisizioni on-line*, cit., p. 338.

[329] Per la definizione, R. FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d. Online Durchsuschung. La prospettiva delle investigazioni ad alto contenuto tecnologico ed il bilanciamento con i diritti inviolabili della persona*, in *Riv. trim. dir. pen. ec.*, 2009, p. 696.

[330] F. IOVENE, *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in Riv. trim. *dir. pen. cont.* 2014, 3-4, p. 329 ss.

[331] A. CAMON, *Cavalli di Troia*, cit., p. 91; A. BALSAMO, *Intercettazioni ambientali mobili e cooperazione giudiziaria internazionale: le indicazioni desumibili dalla giurisprudenza della Corte di Strasburgo*, in *Cass. pen.*, 2016, p. 4241 s. Cfr. il progetto di studio della Commissione Libertà civili, giustizia e affari interni (LIBE) del Parlamento europeo, *Legal Framework for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, 2017; G. ZICCARDI, *Parlamento europeo, captatore informatico e attività di* hacking *delle Forze dell'Ordine: alcune riflessioni informatico giuridiche*, in *Arch. pen.*, 2017 (1), p. 1 s.

2008, ha promosso un'evoluzione dei propri principi costituzionali, fornendo indicazioni dettagliate sull'utilizzo della *Online-Durchsuchung*, nel rispetto degli artt. 10 e 13 GG (sulla tutela delle comunicazioni e del domicilio) in relazione gli artt. 1 comma 1 e 2 comma 1 GG, riguardanti la tutela della dignità umana e il libero sviluppo della personalità. Le innovative argomentazioni della sentenza possono essere riassunte in tre prospettive: innanzitutto, in base al "diritto di autodeterminazione informativa" ognuno potrà decidere sulla divulgazione e sull'utilizzo dei propri dati informatici, prescindendo dalla natura dei contenuti; se la condotta abusiva ha inciso sui dati personali dell'individuo, può essere invocato il "diritto fondamentale alla garanzia dell'integrità e della riservatezza dei sistemi informatici" (c.d. *Computer-grundrecht*); infine, maggior salvaguardia è stata riservata all'area riguardante il "nucleo essenziale della vita privata" (concetto ripreso dalla riforma del 2016[332] che ha suscitato perplessità dottrinali in relazione sia all'attuale impossibilità di poter escludere informazioni digitali meritevoli di una protezione più intensa, sia alla necessità di un controllo sulle attività di indagine, da parte di un organo in posizione di neutralità e di indipendenza[333]).

Una terza sentenza del 2016[334] ha accolto una prassi relativa al c.d. *surfen*, ossia la navigazione *web* effettuata sui motori di ricerca, ritenuti analoghi alle "telecomunicazioni", in ragione del dialogo dell'informazione tra tastiera e *server*; tale decisione ha dato vita a dubbi interpretativi sull'acquisizione dei contenuti memorizzati sul *Cloud*, poiché, secondo alcuni tali operazioni rientrerebbero nell'area delle intercettazioni, mentre un altro orientamento, sulla scorta delle indicazioni espresse dal *BVerfG*, riteneva errata questa ipotesi, affermando che il "salvataggio" su *Cloud* può

[332] BVerfG, 20 aprile 2016, sulle norme relative alla «Prevenzione delle minacce terroristiche internazionali».

[333] S. GLESS, *Wenn das Haus mithör: Beweisverbote im digitalen Zeitalter*, in StV, 2018, p. 677.

[334] BVerfG, 6 luglio 2016, 2 BvR 1454/13; cfr. M. HIÉRAMENTE, *Surfen im Internet doch Telekommunikation im Sinne des § 100a StPO*, in HRRS, 2016, p. 448 s.; in tema, da ultimo, M. HEINRICH, *Surfen im Internet und Cloud Computing zwischen Telekommunikationsüberwachung und Online Durchsuchung*, in ZIS, 2020, p. 421.

avvenire anche in modo automatico, non essendoci una comunicazione tra soggetto e dispositivo digitale[335].

Tuttavia, anche nell'ordinamento tedesco si sono riscontrate delle problematiche relative alla netta distinzione tra le intercettazioni e le perquisizioni *online*, ragione per cui spesso queste ultime sono state ricondotte alle attività intercettive, in modo da consentirne l'utilizzo dei risultati investigativi altrimenti non fruibili[336]. Solo nel 2017 è stato varato un intervento riformatore[337] che, nell'occuparsi delle indagini svolte nel processo penale attraverso *trojan*, le ha tipizzate prevedendo il loro utilizzo oltre le sole finalità preventive, per cui erano precedentemente adottate. Il legislatore tedesco ha così distinto la c.d. *Quellen-TKÜ* (*Quellen-Telekommunikationsüberwachung*), ossia l'intercettazione di ogni tipo telecomunicazioni[338], ricondotta alle garanzie costituzionali previste dall'art. 10 *Grundgesetz*, e l'*Online-Durchsuchung* (§100b StPO), paragonabile alle perquisizioni *online*, che incide su un elevato livello di garanzie individuali espressamente richieste, secondo quanto emerso dalla sentenza della Consulta del BVerfG nel 27 febbraio 2008, e in cui sono state assimilate anche le operazioni relative alle c.d. intercettazioni ambientali[339]. Tuttavia, numerosi sono i dibattiti legati alle attività effettuate mediante captatore[340]: la *Online-Durchsuchung* consente l'acquisizione dei dati custoditi attraverso intrusioni occulte nel sistema informatico, purché si rispetti il principio di proporzionalità dell'ingerenza rispetto ai

---

335 F. ROGGAN, *Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung: Elektronische Überwachungsmaßnahmen mit Risiken für Beschuldigte und die Allge meinheit*, in StV, 2017, p. 821, richiamando BVerfG, 20 aprile 2016, cit.

336 Così, L. PARLATO, *Le perquisizioni on-line*, cit., p. 346.

337 BGBl., I, 3202, *Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens*: la riforma, approvata il 18 agosto 2017, è entrata in vigore il 24 agosto 2017. Tra gli altri, L. BLECHSCHNITT, *Zur Einführung von Quellen-TKÜ und Online Durchsuchung*, in *StraFo*, 2017, p. 361. Sulla novella v. altresì K. LEIPOLD, S. BEUKELMANN, *Online-Durchsuchung und Quellen-TKÜ*, in *NJW*-Spezial, 2017, p. 440; ampiamente, F. ROGGAN, *Die strafprozessuale Quellen-TKÜ*, p. 821; sulle modifiche complessivamente introdotte, anche su altri temi, T. SINGELNSTEIN, B. DERIN,, *Das Gesetz zur effektiven und praxistauglicheren Ausgestaltung des Strafverfahrens*, in NJW, 2017, p. 2646 s., inoltre, L. PARLATO, *Il legislatore tedesco approfitta di una più ampia riforma per disciplinare le perquisizioni online*, in *Cass. pen*., 2019, p. 854 s.

338 Per la definizione di *Quellen-TKÜ*, tra le altre, LG Hamburg, 13 settembre 2010, 608 Qs 17/10.

339 K. LEIPOLD, S. BEUKELMANN, *Online-Durchsuchung und Quellen-TKÜ*, cit., p. 440.

340 In senso critico, L. BLECHSCHNITT, *Zur Einführung*, cit., p. 364 s.; F. ROGGAN, *Die strafprozessuale Quellen-TKÜ*, cit., p. 824.

suoi scopi, basato sulla gravità del reato commesso contro beni giuridici di particolare rilevanza[341], e sulla chiara necessità di utilizzo di queste particolari tecniche investigative "surrogate" rispetto ai tradizionali strumenti di indagine[342].

L'ultima pronuncia del 2020 della Corte costituzionale federale tedesca[343] si è soffermata sulle informazioni che l'*Internet Service Provider* dovrà cedere all'autorità giudiziaria, riferendosi specificatamente non hai dati di traffico, ma a quelli inerenti all'utente e agli indirizzi IP (c.d. dati di inventario), che incidono nella sfera di riservatezza del singolo, sollecitando il legislatore a introdurre una norma che rispetti il principio di proporzione.

Inoltre, nel dimostrare i contrasti tra l'uso del *trojan* e il quadro complessivo delle garanzie individuali, si è aggiunta una pronuncia della Corte costituzionale austriaca, la cui decisione si è mostrata severa riguardo all'utilizzo investigativo del *trojan*, anche rispetto al principio della proporzionalità[344]: il giudice delle leggi austriaco ha considerato la captazione occulta di un sistema informatico attraverso il *virus* spia come una "grave intrusione nella sfera privata", riconoscendo una violazione dell'art. 8 CEDU; l'attività investigativa in questione è stata ritenuta ammissibile limitatamente ai reati lesivi di beni giuridici importanti, tali da poter giustificare una forte compressione delle libertà individuali[345].

III.3 Le garanzie costituzionali e le esigenze investigative nel diritto italiano.

Sulla base delle considerazioni sin qui esposte, l'utilizzo del captatore informatico in ambiti diversi da quelli previsti dalla legge nel campo delle intercettazioni sembrerebbe inammissibile; tuttavia, da più di un decennio, si sta affermando nell'ordinamento italiano una prassi differente, che riterrebbe ammissibili

---

[341] BVerfG, 27 febbraio 2008, cit., con riferimento alla vita, all'incolumità fisica, alla libertà dei singoli, nonché ai beni giuridici della collettività, la cui minaccia «tocchi le fondamenta dello Stato», oppure «dell'esistenza umana».

[342] F. ROGGAN, *Die strafprozessuale Quellen-TKÜ*, cit., p. 824.

[343] BVerfG, 27 maggio 2020, 1 BvR 1873/13, 1 BvR 2618/13.

[344] VerfGH, 11 dicembre 2019, G 72-74/2019-48, G 181-182/2019-18, in www.vfgh.gv.at.

[345] Cfr, L. PARLATO, *Le perquisizioni on-line*, cit., p. 361 s.

quei mezzi di ricerca della prova digitale (sequestro, ispezione e perquisizione *online*), che seppur non espressamente regolati da previsioni legislative, sono compiuti attraverso l'inoculazione del *malware*. Per questo motivo, è necessario individuare i valori e i diritti costituzionalmente garantiti che potrebbero essere intaccati dall'impiego inusuale del virus informatico, al fine di creare un bilanciamento che soddisfi anche le esigenze investigative volte alla ricerca della *digital evidence*, elementi essenziali nel contrasto delle fattispecie criminose. Nella ricerca di un modello tipico in cui ricondurre le perquisizioni *online*, deve adottarsi un canone ermeneutico di interpretazione tassativa: in queste ipotesi la norma processuale penale deve dar attuazione alla riserva di legge, stabilendo i "casi e modi" attraverso cui i pubblici poteri possono derogare i diritti inviolabili.

Seguendo lo schema costituzionale, l'art. 2 Cost. afferma solennemente che "*La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale*". Tale articolo mira sia a riconoscere i diritti inviolabili dell'uomo, ossia quei diritti imprescindibili che si riferiscono «al patrimonio irretrattabile della persona umana intesa come totalità ossia al principio supremo della libertà-dignità»[346], sia a garantirne una piena tutela attraverso una doppia riserva di legge e di giurisdizione. Inoltre, l'articolo in questione richiede l'adempimento di doveri inderogabili, ossia una serie di obblighi a cui il cittadino italiano non potrà sottrarsi dall'adempierli, e la cui violazione darà vita ad ipotesi derogatorie.

Tra i primi diritti inviolabili, risalta la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione, garantite dall'art. 15 della Cost., che consente limitazioni nel rispetto del principio della riserva di legge e mediante un provvedimento motivato dell'autorità giudiziaria. Inoltre, secondo la Corte costituzionale, le comunicazioni intercettate devono essere oggetto di "garanzie rinforzate", in quanto prevedono un controllo di natura tecnica (attività intercettive che saranno effettuate) e un controllo di natura giuridica[347] (relativo alla legittimità e ai

[346] F. MODUGNO, P. CARNEVALE, *Diritto Pubblico*, Giappichelli, Torino, 2015, p. 571 ss.

[347] Corte Cost., 4 aprile 1973, n. 34

limiti contenutistici del mezzo di ricerca della prova utilizzato), tralasciando le acquisizioni dei tabulati telefonici che rientrano nella disciplina documentale dell'art. 256 c.p.p. (questo prima dell'entrata in vigore dell'art. 132 d.lgs. 196/2003)[348].

Tuttavia, davanti alla vastità di attività di ricerca esperibili tramite *trojan*, non sempre può essere invocata la garanzia di cui all'art. 15 Cost., soprattutto quando gli elementi da acquisire, non rientrino nella categoria delle "comunicazioni", cui la disposizione si riferisce; inoltre, anche in riferimento alle "semplici" intercettazioni, la loro realizzazione mediante virus ne trasforma i connotati, implicando che, insieme all'art. 15 Cost., debbano essere considerate altre norme costituzionali, in una sorta di propensione comune, favorita anche dalle caratteristiche del dispositivo mobile, i cui contenuti sono oggetto della tutela fondamentale posta a salvaguardia della persona, trovando riscontro nella clausola di chiusura dell'art. 13 Cost., che si riferisce a «qualsiasi altra restrizione della libertà personale»[349].

Infatti, l'art. 13 garantisce e tutela la libertà personale, che include la libertà di autodeterminazione e la libertà psico-fisica e morale di ogni essere umano, trattandosi di un'accezione ampia che esprime il diritto di disporre liberamente della propria persona senza nessun tipo di coercizione, estendendosi ad ogni restrizione non condizionata da eccezioni tassativamente previste[350]. L'art. 14, oltre a sancire l'inviolabilità del domicilio, prevede deroghe in ragione dell'esecuzione di ispezioni o perquisizioni o sequestri, nel rispetto delle garanzie previste dalla legge. Entrambe le disposizioni sono strettamente collegate dalla relazione, intima e attuale, intercorrente tra la libertà di domicilio e la sfera della libertà personale, per cui il domicilio godrà delle garanzie previste per l'art. 13; viceversa, l'art. 14, limitandosi alle sole deroghe stabilite, non include ulteriori ipotesi di restrizioni della libertà domiciliare, suscitando dubbi interpretativi riguardanti le intrusioni del captatore e la lesione del domicilio

[348] Questa disciplina riguardante il dovere di esibizione di documenti, atti e dati riservati o segreti, in base alle sentenze Corte Cost. 17 luglio 1998, n. 281, § 3, e Corte Cost., 11 marzo 1993, n. 81, è stata successivamente modificata, poiché la norma di riferimento attuale è l'art. 132 del d.lgs. 196/2003.

[349] L. PARLATO, voce *Perquisizioni on-line*, in *Enc. dir., Annali*, vol. X, Giuffrè, 2017, p. 605.

[350] S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2019, p. 48 ss.

informatico, prontamente risolti dalla Corte Costituzionale[351]. In particolar modo, ai fini dell'applicabilità della tutela prevista dagli artt. 13 e 14 Cost., possono considerarsi "luoghi domiciliari", quelli inaccessibili agli estranei, dove si svolgono atti riservati relativi alla vita privata dell'individuo, per cui sussiste un rapporto di titolarità tra il luogo e il soggetto "tale da giustificare la tutela anche quando la persona è assente"[352]. Tuttavia, resta controversa la possibile estensione applicativa della tutela costituzionale dell'art. 14 al c.d. "domicilio informatico", inteso quale "spazio ideale" (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona[353], a cui viene estesa la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto"[354]; il diritto alla riservatezza sarà quindi subordinato da un accesso esclusivo agli "spazi virtuali", che prescinde dal contenuto dei dati archiviati[355]. Inoltre, le caratteristiche dello *smartphone* giustificano il ricorso all'art. 13 Cost., che tutela la libertà personale: la Corte costituzionale ha ricompreso, nella garanzia ivi prevista, oggetti o accessori "che abitualmente sono portati sulla persona o ad immediato contatto di essa"[356]. Tale canone si potrebbe interpretare in modo più ampio, tanto da considerare la sorveglianza effettuata sul cellulare «così incisiva nella sfera dell'intimità individuale da lambire l'inviolabilità della psiche, bene giuridico» riconducibile nel novero delle tutele previste dall'art. 13 Cost[357].

Ai fini processuali, è opportuno richiamare l'art. 24 Cost., che al comma 2 tutela il diritto inviolabile di difesa in ogni stato e grado del procedimento; tale diritto è connesso all'art. 111 Cost. riguardante i principi del "giusto processo", garantendo, nei

---

[351] Corte Cost., 24 aprile 2002, n. 135. Si è superato quell'orientamento secondo cui le videoriprese in ambito domiciliare sarebbero costituzionalmente INCOMPATIBILI a causa delle limitazioni previste dall'art. 14 Cost. Per approfondimenti sul tema, A. MACCHIA, *I diritti fondamentali "minacciati": lo sfondo delle garanzie in costituzione*, in *Diritto Penale Contemporaneo*, 17 luglio 2017.

[352] Cass., Sez. Un., 28 marzo 2006, n. 26795, *Prisco*, p. 21, in C.E.D. Cass., n. 234270

[353] Ritiene di estendere la tutela del domicilio fisico a quella del domicilio informatico S. SIGNORATO, *Le indagini digitali*, cit., p. 49 ss.

[354] Cass., pen., sez. V, sentenza 26/10/2012 n° 42021.

[355] R. ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. e proc. pen.*, 2014, p. 1151 s.

[356] Cfr. Corte cost., 31 marzo 1987, n. 88.

[357] L. PARLATO, *Le perquisizioni on-line*, cit., p. 350 e ss.

commi 3 e 4[358], il criterio della formazione della prova in contradditorio tra le parti. Una lettura restrittiva dei due articoli in correlazione potrebbe escludere dalla loro tutela la prova digitale, spesso precostituita al processo, in ragione del delicato processo di acquisizione del dato informatico a fronte di pericoli di contaminazione. Inoltre, considerando l'ingente quantità di dati che potranno essere appresi durante tutta la durate delle operazioni e registrati in un archivio digitale gestito dal procuratore della Repubblica[359], l'attività difensiva potrebbe risultare molto onerosa. Tuttavia, il legislatore, prescrivendo l'adozione delle cautele necessarie ad assicurare la conservazione e l'integrità del *file*, ne garantisce l'attendibilità processuale, attraverso procedure di verifica sulla correttezza delle procedure e sulla conformità della copia-clone, che le parti possono esercitare *ex post*[360], realizzandosi il contraddittorio costituzionalmente garantito.

Il diritto di difesa è considerato anche nei termini del "diritto al silenzio", soprattutto riguardo agli "avvisi" necessari sulla possibilità di poterlo esercitare: gli avvisi assumono importanza nel momento in cui l'autorità giudiziaria deve acquisire le *password* che proteggono il sistema (o parti della sua "memoria"); spesso, accade che non sia espresso alcun avvertimento chiaro, e ciò in ragione di evitare ostacoli investigativi che graverebbero sugli inquirenti, oppure mirate a realizzare le negative conseguenze di una reticenza[361]. Si aggiunge, ulteriormente, la connessione tra la riservatezza (o "confidenzialità") e l'interesse «all'affidabilità e alla fiducia della collettività nella sicurezza dello svolgimento dei rapporti giuridici *online* e *offline*», instaurati attraverso l'utilizzo di dispositivi tecnologici, oltre all'«integrità e

[358] I profili oggettivi e soggettivi del contraddittorio (comma 3 e 4) sono rilevanti per la prova scientifica, cfr. Così, P. TONINI, *Progresso tecnologico, prova scientifica e contradditorio*, in L. DE CATALDO NEUBURGER, (a cura di), *La prova scientifica nel processo penale*, Padova, 2007, p. 65 ss.

[359] Cfr. A. SCALFATI, *Intercettazioni: spirito autoritario, propaganda e norme inutili.,* in *Arch. Pen*., 2/2014, p. 3.

[360] «In primo luogo vi è la sacralità della conservazione dei dati originali, (…) nell'ottica di garantire che, anche a distanza di mesi od anni, ci possa essere sempre la possibilità, per le parti processuali, di riferirsi e di confrontarsi con i dati originali», G. ZICCARDI, *L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche,* in L. LUPÁRIA, *Sistema penale e criminalità informatica,* cit., p. 167.

[361] Come nel "caso Occhionero" in cui l'indagata, al fine di bloccare il sistema, ha digitato più volte una *password* falsa: G. TRINCHELLA, *Spionaggio, i fratelli Occhionero sapevano dell'indagine. Distrutti dati, file e account il giorno prima della perquisizione*, in www.ilfattoquotidiano.it, 11 gennaio 2017. Sul caso, v. Cass., 30 maggio 2017, cit.

disponibilità dei sistemi, dei dati e delle informazioni», in ragione di una lettura orientata verso le linee guida europee espresse nella direttiva del Parlamento europeo e del Consiglio 12 luglio 2002, 2002/58/CE, relativa alla vita privata e alle comunicazioni elettroniche, all'art. 15[362], in sintonia con il diritto alla *privacy*, tutelato dall'art. 2 Cost.[363], inteso come «diritto al mantenimento del controllo sui propri dati»[364]. Un rafforzamento della tutela della riservatezza della vita privata e familiare può discendere, sempre sul fronte sovranazionale, dall' art. 8 Cedu, che opera direttamente nel diritto interno per effetto dell'art. 117 Cost[365], e vieta ogni intrusione al di là delle ipotesi previste dall'articolo stesso ed espresse dalla Corte europea[366], riservando un'applicazione più severa per la disciplina in tema di intercettazioni[367].

La riforma delle intercettazioni del 2017 (mai entrata in vigore) e la successiva novella del 2020[368], in considerazione dei profili di riservatezza riguardanti la possibile divulgazione dei dati personali, hanno espressamente privilegiato un'impostazione ispirata ad un bilanciamento fra le garanzie di cui all'art. 15 Cost. e quelle *ex* art. 21 Cost: il legislatore ha voluto assicurare un "filtro esterno" rispetto alla diffusione degli elementi di prova raccolti durante le intercettazioni tradizionali e ambientali, regolando la possibilità per le parti di accedere al materiale acquisito[369], raccolto in un archivio digitale. Il materiale probatorio, costituito da diversi *file* come documenti, immagini e

---

[362] L. PARLATO, *Le perquisizioni on-line*, cit., p. 352.

[363] La protezione della riservatezza che si articola in tre livelli: quello nazionale (art. 2 Cost.), quello comunitario (artt. 7 e 8 Carta di Nizza) e quello internazionale (art. 8 Cedu).

[364] S. RODOTÀ, voce *Riservatezza*, in *Enc. it*., Appendice, VII, 2007, in www.treccani.it.

[365] Corte cost., 24 ottobre 2007, nn. 348 e 349; V. MANES, *Introduzione*, in V. MANES, V. ZAGREBELSKY, (a cura di), *La Convenzione europea dei diritti dell'uomo nell'ordinamento penale italiano*, Giuffrè, 2011, p. 12.

[366] S. MARCOLINI, *Le cosiddette perquisizioni on-line*, cit., p. 2865; S. LORUSSO, *L'arte di ascoltare e l'investigazione penale tra esigenze di giustizia e tutela della privatezza*, in *Dir. pen. proc*., 2011, p. 1399 s. Cfr. Corte eur., Grande Camera, 4 dicembre 2015, *Zakharov c. Russia*; Corte eur., 11 giugno 2013, *D'Auria e Balsamo c. Italia*; Corte eur., 30 aprile 2013, Cariello e altri c. Italia; Corte eur., 23 febbraio 2016, *Capriotti c. Italia*.

[367] A. BALSAMO, *Il contenuto dei diritti fondamentali*, in R. E. KOSTORIS, (a cura di), *Manuale di procedura penale europea*, Giuffrè, 2019, p. 176 ss.; A. CAMON, *Cavalli di Troia*, cit., p. 95.

[368] S. CIAMPI, *L'archivio delle intercettazioni tra presidio della riservatezza, tutela del diritto di difesa e svolta digitale*, in M. GIALUZ (a cura di), *Le nuove intercettazioni*, in *Diritto di internet*, 2020, fasc. 3 (suppl.), p. 21 s.

[369] G. ILLUMINATI, *La disciplina processuale delle intercettazioni*, Giuffrè, 1983, p. 4.

registrazioni potrebbe, infatti, coinvolgere diverse persone, anche soggetti esterni, in considerazione della interconnessione a cui siamo esposti (basti pensare alla nuova tecnologia di comunicazione c.d. 5G, ma anche all'abitudine di gestire attività quotidiane in modalità *smart*, rafforzatasi a causa dell'emergenza Covid-19, che ha costretto la popolazione a svolgere diverse attività rimanendo in casa)[370].

In ogni caso, le ampie funzionalità del captatore semplificherebbero il lavoro dell'autorità giudiziaria, ma in mancanza di una normativa specifica che possa giustificarne l'ammissibilità giuridica nel nostro ordinamento, e che possa bilanciare la tutela dei diritti costituzionalmente garantiti e le finalità investigative, le opinioni sono contrastanti. Un primo orientamento sosterrebbe l'uso del captatore per un efficace perseguimento dei reati, essendo i principi costituzionali oggetto di una tutela progressiva, intesa come «opportuno adeguamento all'evoluzione tecnologica e alle sfide del tempo»[371]; un altro orientamento, invece, ritiene inammissibile l'uso del captatore, in quanto, secondo la sentenza della Corte di Cassazione "Prisco" sul caso delle videoriprese domiciliari, tale strumento non sarebbe conforme alla disciplina processuale penale, in quanto sarebbe carente sotto il profilo delle garanzie costituzionali sopra esposte[372]: sicché affermarne la sua inammissibilità significherebbe relegare l'oggetto della captazione alle forme della mera intercettazione di comunicazioni (chiamate e SMS), riducendo considerevolmente l'ambito di applicabilità di tale strumento[373]. Ciò in considerazione dei vantaggi investigativi derivanti dall'uso dell'*agent*, che permettono di superare e aggirare diversi meccanismi dei dispositivi, tali da poter leggere "in chiaro" i contenuti memorizzati, escludendo l'archiviazione di dati presso il *server* prima che possano essere "salvati" sul *Cloud*, nonché tecniche di crittografia[374]: basti pensare ai sistemi VoIP (*Voice over Internet*

---

[370] L. PARLATO, *Le perquisizioni on-line*, cit., p. 354.

[371] R. ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela progressiva dei diritti fondamentali*, in *Riv. it. dir. e proc. pen*., 2014, pp. 1134 ss.

[372] Corte Cost., 30 novembre 2009, n. 317. Anche le Sez. Un., 28 marzo 2006, n. 26795, *Prisco*, ammettono la difficoltà di «accettare l'idea che una violazione del domicilio che la legge processuale non prevede […] possa legittimare la produzione di materiale di valore probatorio».

[373] In tal senso, L. GIORDANO, *Dopo le sezioni unite sul "captatore informatico*, cit. pp. 177-195.

[374] L. PARLATO, *Le perquisizioni on-line*, cit., p. 342.

Protocol) che hanno rivoluzionato il modo di comunicare[375] (come la crittografia *end-to-end*[376], adottata da *WhatsApp*[377] nel 2016, che permette di cifrare il traffico telematico, rendendo impossibile la captazione delle conversazioni da parte dei fornitori di servizi, che possono devolvere tale compito agli inquirenti che procederanno muniti di decreto motivato[378]).

Nella ricerca di un punto di equilibrio tra spinte investigative e garanzie individuali, la chiave di volta è rappresentata dal criterio di proporzionalità, che risalta come canone fondamentale nelle fonti dell'Unione europea[379], in particolare, nella Carta dei diritti fondamentali dell'Unione europea, agli artt. 7 e 8, ripresi dalla Convenzione di Budapest sulla criminalità informatica e recepita in Italia con la L. n. 48/2008: la *ratio* del principio si basa sulla verifica della "necessità" della sorveglianza, tale da giustificare una forte intrusione nella sfera individuale, che ne giustifichi un sacrificio dei suoi diritti bilanciato allo scopo investigativo[380].

Alcune criticità, inoltre, riguardano i profili di "atipicità" delle investigazioni digitali mediante *trojan,* in ragione delle conseguenze processuali che potrebbero rilevare a seconda della legittimità o meno di questo strumento investigativo, che non

---

[375] VOIP sta per "*Voice Over Internet Protocol*", la cui principale funzionalità consiste nella possibilità di compiere una vera e propria conversazione telefonica sfruttando una connessione di rete (può trattarsi o di una connessione internet o di un'altra rete dedicata che utilizza il protocollo IP); a differenza delle comunicazioni telefoniche tradizionali, nell'ambito del suo funzionamento vengono eliminate le centrali di commutazione. Il sistema Voip, infatti, attraverso appositi *software* (chiamati *gateways*), provvede ad instradare sulla rete pacchetti di dati contenenti le "informazioni vocali" (analogiche) codificate e compresse in forma digitale (*bits*), solo nel momento in cui è necessario cioè quando uno degli utenti collegati sta parlando. Cfr. C. PARODI, *VoIP, Skype e tecnologie d'intercettazione: quali riposte d'indagine per le nuove frontiere di comunicazione?*, in *Diritto penale e processo*, 2008, n. 10, pp. 1309, 1313; S. MARIOTTI – S. TACCONI, *Riflessioni sulle problematiche investigative e di sicurezza connesse alle comunicazioni VoIP*, in *Diritto dell'Internet*, 2008, n. 6, pp. 558- 562.

[376] La crittografia *end-to-end* (da "punto a punto") si basa su di un sistema di chiavi crittografiche asimmetriche. I messaggi in uscita sono protetti dalla chiave privata del mittente e possono essere decifrati solo attraverso la chiave pubblica del destinatario.

[377] Applicazione di messaggistica istantanea per dispositivi mobili che, attraverso la connessione ad Internet, consente lo scambio tra uno o più utenti di messaggi di testo e *files* multimediali. Ulteriori servizi sono *Telegram*, basato su *cloud*, e *Skype*, che aggiunge il sistema VoIP.

[378] F. CAJANI, *Odissea del captatore informatico*, in *Cass. pen*., 2016, p. 4143.

[379] M. CAIANELLO, *Il principio di proporzionalità nel procedimento penale*, in *Dir. pen. cont., Riv. trim.*, 2014, 3-4, p. 143 s.

[380] R. E. KOSTORIS, *La tutela dei diritti fondamentali*, in ID. (a cura di), *Manuale di procedura penale europea*, cit., p. 89.

può assumere come immediato riferimento le garanzie stabilite a livello costituzionale[381].

III.4 L'inquadramento giurisprudenziale delle perquisizioni *online*.

In considerazione dell'impossibilità di ricondurre le perquisizioni *online* ai mezzi di ricerca della prova già previsti dal codice di rito, la giurisprudenza ha prospettato due orientamenti interpretativi diversi, capaci di "salvare" dall'inammissibilità questo nuovo strumento investigativo di natura ibrida, a metà strada tra le intercettazioni e la perquisizione informatica, permettendone un utilizzo in sede processuale del dato istruttorio raccolto da remoto.

III.4.1 I profili di atipicità delle perquisizioni *online*.

Tra le numerose attività che possono essere compiute con il captatore, vi sono alcune che rientrano nella sfera delle indagini "atipiche"[382], in base a quanto fu stabilito nella Relazione al progetto preliminare del codice di procedura penale con l'introduzione dell'art. 189 c.p.p.[383] che disciplina le specifiche e determinate condizioni in cui possono essere acquisite le prove non disciplinate dalla legge[384] , nonché una pluralità di riscontri recenti, in giurisprudenza e in dottrina[385], anche in relazione ad attività riconducibili al *genus* delle perquisizioni *online*, come le videoriprese e il pedinamento tradizionale e quello "virtuale"[386], ritenendoli di competenza della polizia giudiziaria. Tuttavia, l'eventuale qualificazione "atipica" dell'attività investigativa deve

---

[381] L. PARLATO, voce *Perquisizioni* on-line, in *Enc. dir.*, *Annali*, vol. X, Giuffrè, 2017, p. 604 s.

[382] Cfr., S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018, p. 255 s.

[383] Art. 189 c.p.p.: "Quando è richiesta una non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova."

[384] Non sono mancate opinioni contrastanti, di cui una che affermava che i vincoli probatori in materia penale dovevano considerarsi mere eccezioni ed essere rigidamente contenuti in quanto potenzialmente pregiudizievoli per l'accertamento della verità, cfr. E. FLORIAN, *Delle prove penali*, 3, Milano, 1961, p. 8.

[385] S. MARCOLINI, *Le cosiddette perquisizioni on-line*, cit., p. 2855 s., Cfr. *Rel. prog. prel. c.p.p.*, pp. 191 - 198; Cass., 27 marzo 2008, *Gori*, in CED., n. 239774.

[386] Cass., Sez. Un., 28 marzo 2006, *Prisco*, cit.; Cass., 11 dicembre 2007, *Sitzia*, in CED., n. 239635.

essere comunque tener conto del principio della riserva di legge, stabilito da diversi degli articoli che tutelano i diritti fondamentali costituzionali, il cui rispetto deve costituire il principale punto di riferimento, superato il quale dovrebbero essere ritenute "incostituzionali"[387] le evidenze digitali acquisite e quindi inutilizzabili, ai sensi dell'art. 191 c.p.p.[388]

Ad esempio, nel caso delle videoriprese contenenti materiale "non comunicativo" la giurisprudenza[389] si era già espressa formulando delle riflessioni utili per il suo inquadramento in seno alle indagini atipiche e, soprattutto, in una possibile inclusione nell'alveo delle perquisizioni *online*: applicando i criteri declinati dalle Sezioni unite, la videoripresa sarebbe ammissibile, rientrando nelle ipotesi di attività atipica del pubblico ministero, a condizione che non sia svolta all'interno del domicilio, in quanto il loro utilizzo è ostacolato dalla riserva di legge e dalle garanzie previste costituzionalmente all'art. 14, mentre i luoghi riservati, ossia quei luoghi che non rientrano pienamente nella nozione di domicilio e in cui la "riservatezza" è limitata ad un determinato periodo di tempo, sono soggetti alla disciplina ex art. 189 c.p.p., se autorizzate dall'autorità giudiziaria. Nel caso, ad esempio, della c.d. localizzazione mediante GPS, anch'essa riconducibile nelle ipotesi di perquisizione *online*, la corte di Cassazione ha ritenuto che le operazioni da parte della polizia giudiziaria di rilevazione satellitare incidessero minormente sulle libertà fondamentali, e pertanto, ha affermato la

---

[387] La nozione di prova incostituzionale è controversa e solo in certi casi è stata accolta dalla giurisprudenza: Corte. cost., sent. 6 aprile 1973, n. 34, cit., p. 316 ss. Nello stesso senso, fra le altre, Corte. cost., sent. 9 luglio 1996, n. 238, in *Giur. cost*., 1996, p. 2142; ID., sent. 8 aprile 1993, n. 151, ivi, 1993, p. 1156; ID., sent. 11 marzo 1993, n. 81, ivi, 1993, p. 731.

[388] «Come si comprende, pur con tutte le delineate sfumature, il labile confine fra la prova incostituzionale e la prova atipica finisce per esaltare il ruolo nomotetico all'interprete, chiamato a operare bilanciamenti costanti fra le libertà fondamentali della persona e l'esigenza di prevenire, accertare, e reprimere i reati» P. MAGGIO, *Ascolto occulto delle conversazioni tra presenti*, in A. SCALFATI, (a cura di), *Le indagini atipiche*, cit. p. 87 s.; inoltre, sul principio di non sostituibilità v., C. CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Dir. Pen e processo*, 2018, pp. 1210-1221.

[389] Antonio Prisco era un gestore di night club indagato per associazione a delinquere finalizzata alla prostituzione, e altri reati con simili fini; viene tratto in arresto, e per giustificare i gravi indizi di colpevolezza, vengono posti una serie di elementi di prova come intercettazioni telefoniche, e video riprese nei camerini, i quali sono stati definiti "luoghi riservati", nei quali si svolgevano attività ambigue con i clienti. Cass., Sez. Un., 28 marzo 2006, n. 26795, *Prisco*.

loro ammissibilità al processo come prova atipica[390]; tuttavia la Corte europea, nel caso Uzun c. Germania[391] ha rilevato una serie di criticità in relazione all'ingerenza di tale strumento sul diritto fondamentale al rispetto della vita privata, previsto dall'art. 8 Cedu[392], riconoscendo la presenza di una sfera privata meritevole di protezione anche nella vita pubblica e di relazione, in quanto nell'art. 8 Cedu è compreso anche il diritto di stabilire e incrementare le relazioni umane[393], ma ritenendola comunque un'incisione minore rispetto alla compressione dei diritti ravvisabile per le intercettazioni di comunicazioni.

Oltre ai due casi particolari sopramenzionati, all'interno delle attività di perquisizioni *online* possono essere considerate "atipiche" le operazioni riguardanti la *online search,* volte principalmente all'acquisizione mediante copia della documentazione, totale o parziale, memorizzata e archiviata all'interno del dispositivo *target*, che consente l'ottenimento di una grande quantità di dati precostituiti al provvedimento autorizzativo dell'autorità giudiziaria, insuscettibili di alcuna preselezione rispetto all'utilità e ai fini dell'indagine[394].

---

[390] Cass., 7 gennaio 2010, *Congia* e altro, in *Cass. pen*., 2012, p. 1062; Corte eur., 2 settembre 2010, *Uzun c. Germania*; M. TROGU, *Le indagini svolte con l'uso di programmi spia*, cit., p. 73.

[391] Corte Europea dei Diritti dell'Uomo, *Uzun v. Germany*, 2 settembre 2010, ric. n. 35623/05.

[392] Corte eur., 2 settembre 2010, *Uzun v. Germany*: il caso trae origine dal ricorso presentato da Bernard Uzun, cittadino tedesco, sospettato di aver partecipato a tentati omicidi e attentati terroristici organizzati dalla cellula terroristica denominata *Antiimperialistische Zelle*, un movimento terrorista di estrema sinistra che aveva come obiettivo la lotta armata perseguita fino al 1992 dalla *Rote Armee Fraktion*. Uzun era stato sottoposto a partire dal 1993 a osservazione tramite videoriprese, intercettazioni e controllo della corrispondenza; nel 1995 era stato installato un trasmettitore sulla macchina di uno dei suoi complici. A seguito della scoperta e distruzione di tale trasmettitore da parte di Uzun e del complice, la polizia federale aveva installato un *tracker* GPS sull'autovettura del ricorrente. La Corte d'Appello di *Düsseldorf* aveva condannato Uzun e rigettato l'eccezione di inutilizzabilità delle prove ottenute attraverso il pedinamento satellitare sostenendo che non fosse necessaria una specifica autorizzazione per tale ultima attività di indagine in quanto si trattava di una forma di sorveglianza che andava ad aggiungersi alle altre già autorizzate. Dopo essere ricorso sia al *Bundesgerichtshof* che al *Bundesverfassungsgericht*, Uzun ha quindi adito la Corte EDU lamentando la violazione del diritto al rispetto della vita privata tutelato dall'art. 8 CEDU e del diritto ad un processo equo *ex* art. 61, § 1 CEDU.

[393] Precedentemente la Corte europea aveva affermato che la raccolta e conservazione di dati interferiva con la vita privata anche se l'attività di controllo veniva svolta pubblicamente. Cfr. Corte Europea dei Diritti dell'Uomo, Peck v. United Kingdom, 23 gennaio 2003, ric. n. 44647/98, §§ 57-59; Corte Europea dei Diritti dell'Uomo, *P.G. and J.H. v. United Kingdom*, 25 settembre 2001, ric. n. 44787/98, §§ 56-57; Corte Europea dei Diritti dell'Uomo, *Perry v. United Kingdom*, 17 luglio 2003, ric. n. 63737/00, §§ 36-38; *Rotaru v. Romania*, 4 maggio 2000, ric. n. 28341/95, §§ 43-44.

[394] L. PARLATO, *Le perquisizioni on-line*, cit., p. 367.

Le poche pronunce di legittimità in materia hanno ricondotto le attività di *online search* alla figura prevista dall'art. 189 c.p.p. relativo alla "prova atipica"[395]: per la giurisprudenza è legittimo il decreto del pubblico ministero di acquisizione in copia, attraverso l'installazione di un captatore informatico, della documentazione informatica presente nei dispositivi in uso all'imputato e installato presso un ufficio pubblico, qualora il provvedimento abbia riguardato l'estrapolazione di dati, non aventi ad oggetto un flusso di comunicazioni, già formati e contenuti nella memoria del dispositivo o che in futuro sarebbero stati memorizzati; pertanto nel caso di specie, in cui l'attività autorizzata dal pubblico ministero aveva ad oggetto "un flusso unidirezionale di dati" confinati all'interno dei circuiti del computer, la Corte di Cassazione ha ritenuto utilizzabili le risultanze di tali attività, disposte successivamente al decreto autorizzativo del pubblico ministero, legittimando sia il conseguimento, in copia mediante un *trojan*, del materiale memorizzato in un sistema informatico collocato in uffici pubblici, *ex* art. 234 c.p.p., sia la periodica registrazione dei dati salvati dopo che il provvedimento sia stato disposto, attraverso un monitoraggio ignoto e costante. Le motivazioni alla base di tale sentenza hanno suscitato dubbi, sia in relazione all'inapplicabilità degli artt. 15 Cost. e 266 e ss. c.p.p., in ragione dell'oggetto non coincidente a dei "flussi comunicazioni", in considerazione della mancanza di un vero e proprio trasferimento di dati con altri soggetti destinatari, poiché l'operazione era mirata all'acquisizione di dati precostituiti nell'*hard disk* dell'apparecchio[396]; sia riguardo all'esclusione dell'operatività del principio costituzionale previsto dall'art. 14, poiché nel caso di specie si trattava di un computer collocato esternamente alla dimora privata.

L'ampio spettro delle indagini intrusive non espressamente articolate dalla legge "svela un vulnus del nostro ordinamento"[397] che non terrebbe in considerazione il pieno rispetto del principio di legalità sancito a livello europeo nell'art. 8 Cedu: in realtà, l'ammissione delle prove atipiche, in base a quanto fu stabilito nella Relazione al

---

[395] Cass., 14 ottobre 2009, *Virruso*, in CED, n. 246954; v. al riguardo S. ATERNO, *Le investigazioni informatiche e l'acquisizione della prova digitale,* in *Giur. merito*, 2013, p. 962.

[396] Cass., 14 ottobre 2009, *Virruso*, cit.; v., in dottrina, S. ATERNO, *Le investigazioni*, cit., p. 962; L. GIORDANO, *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte*, in *Sist. pen*., 2020 (4), p. 126 s.

[397] Così, L. PARLATO, *Le perquisizioni on-line*, cit., p. 367.

progetto preliminare del codice di procedura penale con l'introduzione della seguente disposizione, funge da "valvola di salvezza" permettendo di adattare automaticamente il rito e gli istituti processuali tradizionali alle innovazioni tecnologiche; tuttavia, nonostante la "cautela" del legislatore del 1989, si nota come attraverso l'introduzione dell'art. 189 c.p.p. sia stato abbandonato il principio di tassatività dei mezzi di prova[398], a favore di una "apertura controllata" del catalogo legale indirizzata sulla linea dell'idoneità probatoria[399], della tutela della libertà morale della persona[400] e del rispetto del principio del contraddittorio nella formazione della prova[401]: infatti, non vi è una diretta acquisizione ai fini processuali, ma tale procedura è subordinata a determinate condizioni, tra cui la chiara necessità della realizzazione del contraddittorio tra le parti per l'espletamento della stessa, e il divieto di realizzazione di operazioni volte ad intaccare la libertà personale. Inoltre, la norma in esame non riesce a soddisfare

---

[398] Così, P. TONINI, *La prova penale*, Milano, 2002, p. 92. Contro, A. CIAVOLA, *Prova testimoniale e acquisizione per suo tramite del contenuto delle intercettazioni telefoniche*, in *Cass. pen*., 2000, p. 488, secondo cui proprio l'art. 189 c.p.p. dovrebbe considerarsi norma posta a chiusura della disciplina dei mezzi di prova.

[399] L'ammissibilità della prova atipica dipende, innanzitutto, dalla capacità dello strumento probatorio di offrire un contributo utile alla ricostruzione dei fatti, che non sarebbe raggiungibile attraverso i mezzi di prova tipici. Tale prognosi di idoneità probatoria con riferimento ai mezzi di prova atipici è onere del giudice e si traduce in un giudizio di "non manifesta inidoneità" del mezzo di prova atipico a verificare i fatti per cui si procede. Cfr. O. DOMINIONI, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, cit., p. 225 ss.; G. TABASCO, *Prove non disciplinate dalla legge nel processo penale, Le "prove atipiche" tra teoria e prassi*, Napoli, 2011, p. 52. C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Torino, 2007, p.116, precisando come «la preminenza accordata a tale primo requisito non è casuale perché questo rappresenta un *prius* logico anche rispetto alla verifica della compatibilità (della prova atipica) con la libertà morale».

[400] Tale requisito si identifica con il dovere di garantire ai soggetti coinvolti dall'utilizzo dello strumento atipico il diritto di autodeterminarsi rispetto agli stimoli esterni e si traduce nel divieto di utilizzare, «neppure con il consenso della persona interessata, metodi o tecniche idonei ad influire sulla libertà di autodeterminazione o ad alterare la capacità di ricordare e di valutare i fatti» (art. 188 c.p.p.). Sulla differenza tra libertà personale intesa come assenza di coercizioni fisiche e libertà morale, intesa come assenza di coercizione psichica idonea a pregiudicare la capacità di autodeterminazione del soggetto, v. G. VASSALLI, *La libertà personale nel sistema delle libertà costituzionali*, in Id., *Scritti giuridici*, vol. III, Milano, 1997, p.177 ss.

[401] Nel caso si debba acquisire una prova non disciplinata dalla legge il contraddittorio viene garantito non solo nel momento della formazione della prova, ma ancor prima, nel momento di individuazione del procedimento acquisitivo, non essedo quest'ultimo tipizzato nel codice di rito. Cfr., A. LARONGA, *Le prove atipiche nel processo penale*, Padova, 2002, p. 123; V. BOZIO, *Le prove atipiche*, in P. FERRUA - E. MARZADURI – G. SPANGHER (a cura di), *La prova penale*, Torino, 2013, pp. 74 ss. Il giudice non è comunque vincolato a tener conto dei suggerimenti espressi dalle parti sulle modalità di assunzione della prova atipica. Infatti, solamente la mancata audizione delle stesse in contraddittorio sarebbe causa di nullità *ex* art. 178 lett. b) o c) c.p.p. Sul punto, C. PANSINI, *È valida la prova atipica senza la preventiva audizione delle parti?*, in *Dir. pen. proc*., 1997, p. 1258.

totalmente la riserva di legge, neanche con riguardo alla fase dibattimentale, in quanto essa non può fungere da efficace presidio normativo per i mezzi di ricerca della prova e colmare, per questi ultimi, l'assenza di qualsivoglia dato positivo, neppure "in bianco" alla stregua dello stesso art. 189 c.p.p.[402]. La problematica viene sottolineata ancora di più per questo tipo di atti a "sorpresa", in cui il contraddittorio anticipato stabilito dall'articolo in questione è impedito.

La marcata "atipicità" delle perquisizioni *online* sottopone lo strumento al rischio che ne si abusi, compiendo azioni ulteriori rispetto a quelle stabilite dal provvedimento autorizzativo, che, in assenza di una specifica normativa, ne rendono problematico il controllo da parte dell'autorità giudiziaria (come nel caso in cui il *malware* inoculato per svolgere una specifica attività, come ad esempio l'intercettazione c.d. ambientale, venga poi utilizzato per svolgere un'operazione in sostituzione o in aggiunta[403], riguardante la visione dei *file* archiviati sull'*hard disk* del dispositivo, potendo addirittura modificarne il contenuto). A riguardo, il legislatore all'art. 271 comma 1-*bis* c.p.p., introdotto dall'art. 4 lett. *e*) d.lgs. n. 216 del 2017 ha previsto l'inutilizzabilità dei "dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore informatico sul dispositivo elettronico portatile". In ogni caso, affinché si possa evitare la sanzione processuale dell'inutilizzabilità per i casi rientranti nella particolare categoria delle perquisizioni *online*, è possibile procedere all'acquisizione dei dati originali terminate le operazioni e attraverso il sequestro del dispositivo digitale, confidando nella disponibilità di questi ultimi che potrebbero essere contaminati a causa delle procedure utilizzate[404].

---

[402] Così, L. PARLATO, *Le perquisizioni on-line,* cit., p. 368.

[403] A. CAMON, *Cavalli di Troia,* cit., p. 96. Il problema è emerso con chiarezza nella vicenda processuale cui si riferisce Cass., 20 ottobre 2017, Occhionero, cit., ed è posto in particolare evidenza da S. ATERNO, *La Cassazione, alle prese con il captatore informatico, non convince sull'acquisizione mediante screenshot,* in *Dir. pen. proc*., 2018, p. 1065 s.; L. GIORDANO, *Presupposti e limiti*, cit., p. 119; A. PAOLETTI, *La ricerca della prova penale*, cit., p. 436.

[404] L'accesso dell'*agent* al sistema potrebbe comportare una serie di "danni" sulla protezione del sistema del dispositivo sorvegliato, determinandone in futuro una maggiore vulnerabilità rispetto ad "attacchi" di varia provenienza, che, se accertati, potrebbero generare forme di responsabilità aquiliana. Un diverso aspetto riguarda il fatto che la disciplina dell'art. 267 comma 2-*bis* c.p.p., è circoscritta al campo delle attività eseguite su "dispositivo elettronico portatile" e non su apparecchi fissi: l'attività di "perquisizione *on-line*" tramite un computer "fisso" può anch'essa svelare buone potenzialità investigative, nonostante la collocazione dell'apparecchio sia rilevante per l'apprensione di risultanze probatorie (*password*, comunicazioni su *WhatsApp* se in uso il programma *WhatsApp Web*, dati digitali salvati sul *Cloud*, senza

III.4.2 Il "documento informatico" come soluzione interpretativa.

L'installazione del captatore informatico può generare numerose varietà di investigazioni, anche "atipiche", spesso scorporate tra di loro[405] dalla giurisprudenza, in cui risulta complicato sia comprendere quale uso dello strumento digitale sia stato eseguito all'interno di una determinata indagine, sia stabilire se le operazioni realizzate siano riconducibili all'istituto delle intercettazioni.

Sono recenti i richiami in diverse pronunce giurisprudenziali alla disciplina della prova documentale, e in particolar modo alla *species* del "documento informatico" per consentire l'utilizzo processuale delle prove reperite, in considerazione del fatto che determinate operazioni non potranno essere inquadrate nel novero delle intercettazioni, permettendone anche l'uso di queste risultanze negli altri procedimenti (art. 270 c.p.p.). Inoltre, un orientamento giurisprudenziale[406] ha confermato l'utilizzo processuale degli elementi raccolti, riconoscendo alla copia estratta del documento informatico la stessa valenza probatoria del *file* originario, salvo che non se ne dimostri l'alterazione.

Numerose sono le fattispecie controverse che vengono in rilievo: in primis la captazione di *e-mail*[407], che precedentemente era ricondotta dalla giurisprudenza alla stregua dell'art. 266-*bis* c.p.p. relativo alle intercettazioni di flussi telematici, pur trattandosi di conversazioni pregresse, già inviate o ricevute; infatti, a causa dei contrasti tra le seguenti operazioni e la disciplina ivi prevista, in considerazione della mancanza di contestualità tra la comunicazione e l'atto di acquisizione, per cui l'oggetto raccolto sarà un dato non criptato sul dispositivo *target* del mittente o del destinatario indagato[408], per questi motivi, la giurisprudenza ha riqualificato tale operazione,

---

considerare il periodo attuale di pandemia che ha modificato il modo di interagire degli utenti attraverso le piattaforme *online* di *Zoom* o *Teams*, e dunque mediante l'uso di microfono e telecamera, e spesso lasciando traccia sul computer dei partecipanti ai vari "eventi") utili ai fini dell'investigazione. Sul punto L. PARLATO, *Le perquisizioni on-line*, cit., p. 378.

[405] Cass., 28 giugno 2016, *Grassi* e altri, in CED n. 268227; cfr. L. GIORDANO, *Presupposti e limiti all'utilizzo del captatore informatico*, cit., p. 125.

[406] Cass., 20 dicembre 2018, *Viviano*, in CED., n. 275541.

[407] In tema, E. M. MANCUSO, *L'acquisizione di contenuti* e-mail, in A. SCALFATI (a cura di), *Le indagini atipiche*, cit., p. 497 s.

[408] Cfr. Cass., 28 giugno 2016, *Grassi e altri*, cit.; v. pure in precedenza, Cass., 14 febbraio 2005, *Palamara*, in CED., n. 231591.

affermando che le missive elettroniche memorizzate nell'*account* o nel dispositivo dell'utente indagato sono documenti informatici "statici" e sono soggetti alla disciplina dell'art. 234 c.p.p., non potendo trattarsi di una realizzazione di flussi di comunicazioni[409]. Inoltre, sempre nel campo della posta elettronica, hanno trovato difficile inquadramento sistematico i messaggi archiviati nella casella delle "bozze", ossia quei messaggi che non sono stati mai inoltrati al destinatario, ma che vengono comunque conservati dalle applicazioni delle e-mail o in archivi virtuali (es. *Dropbox* o *Google Drive*): partendo sempre dall'ipotesi di operatività o meno dell'art. 266-*bis* c.p.p., anche in questa ipotesi la giurisprudenza ha stabilito la natura di questi elementi come "documenti informatici" ai sensi dell'art. 234 c.p.p., affermando la possibilità di procedere al sequestro di tali documenti ove il soggetto acceda tramite inserimento delle credenziali, in mancanza di un provvedimento autorizzativo giurisdizionale[410]; tuttavia, la possibilità che diversi utenti possano controllare e comunicare attraverso le "bozze" accedendo – conoscendo la *password* – ad un unico *account*, produce ancora numerosi dubbi interpretativi, in considerazione del fatto che in questa vicenda si stesse compiendo una vero e proprio dialogo nascosto tra diversi utenti[411]. Inoltre, sempre nella pronuncia "Grassi ed altri", la Corte di Cassazione ha incluso nell'alveo delle intercettazioni l'operazione di *keylogger*, relativa alla captazione di ciò che viene digitato sulla tastiera del dispositivo portatile, includendo *password* e la lista degli *account* presenti nella posta elettronica, oltre alla comparazione tra questa sorveglianza e il tradizionale uso di microspie[412].

---

[409] Cass., 28 maggio 2019, *Pizzarotti*, in CED, n. 276227; Cass., 6 febbraio 2020, *Ceriani*, in CED n. 278808; L. GIORDANO, *Presupposti e limiti all'utilizzo del captatore informatico*, cit., p. 126 s.

[410] Cass., 28 giugno 2016, Grassi e altri, cit.; Cass., Sez. Un., 7 settembre 2017, *Andreucci*. In seguito, v. Cass., 16 aprile 2019, *Maliterno*, in CED., n. 276358; Cass., 6 febbraio 2020, *Ceriani*, cit.

[411] «Il sequestro, inoltre, secondo la decisione in esame, giustifica nel procedimento in esame l'acquisizione delle e-mail "bozza". Sul punto, la sentenza critica la tesi che, per salvaguardare il profilo della contestualità della captazione rispetto alla trasmissione, ravvisa un flusso informatico intercettabile quando, per accedere alla "bozza", si entra nella casella di posta elettronica. La decisione, invece, accoglie il "criterio dell'inoltro": l'invio del messaggio – e non la contestualità della captazione rispetto alla conversazione da parte del mittente al destinatario segnerebbe il discrimine tra l'applicazione della disciplina delle intercettazioni e di quella del sequestro»: così, L. GIORDANO, *Dopo le Sezioni unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in *Dir. pen. cont*., 20 marzo 2017, p. 14 s.

[412] L. PARLATO, *Le perquisizioni on-line*, cit., p. 372.

Da ultimo, la giurisprudenza ha chiarito la qualificazione dei messaggi *WhatsApp* e SMS salvati nella memoria del cellulare come "documenti informatici", consentendone la loro assunzione attraverso una sola "riproduzione fotografica", senza che si dia luogo ad operazioni intercettive o di sequestro, ex art. 254 c.p.p., non versandosi nel caso della captazione di un flusso di comunicazioni in corso, bensì nella mera documentazione *ex post* di detti flussi[413].

L'argomento più delicato riguarda l'utilizzo investigativo dei c.d. *screenshot*[414], metodo ancora totalmente inesplorato da parte della giurisprudenza[415], capaci di fotografare l'intera schermata dello *smartphone* per carpire ulteriori informazioni di tipo comunicativo o meno; solo recentemente è stata affermata l'acquisizione legittima degli SMS attraverso una riproduzione fotografica dello schermo del cellulare, come documento probatorio da poter consegnare alla polizia giudiziaria[416]; diversamente, la Corte di Cassazione[417] ha ricondotto tale operazione nella fattispecie dell'art. 266-*bis* c.p.p., nonostante, nella vicenda in questione, oggetto della captazione fosse un flusso intercorso in tempo reale sul dispositivo digitale, maggiormente paragonabile ad una perquisizione *online* in quanto al momento dell'acquisizione non vi è in corso alcuna comunicazione tra i soggetti[418].

---

[413] Cass., 12 novembre 2019, *Tacchi*, in CED. n. 278124.; sul tema, P. DI STEFANO, *Il* Trojan *horse nel processo penale*, in www.giustiziainsieme.it, 28 ottobre 2020; Cass., Sez. V, 10 marzo 2021, n. 17552.

[414] «Tale problematica si è posta in Germania, dove la giurisprudenza (…) si è limitata a escludere la sua assimilabilità alle "semplici" intercettazioni ai sensi del citato § 100a StPO, quando al momento dell'acquisizione non fosse in corso alcuna telecomunicazione»: così, L. PARLATO, *Le perquisizioni on-line*, cit., p. 373.

[415] S. ATERNO, *La Cassazione*, cit., p. 1068 ss.

[416] Cass., 6 novembre 2019, R., in CED. n. 278635.

[417] Cass., 30 maggio 2017, *Occhionero*, cit.; rilievi critici, S. ATERNO, *La Cassazione*, cit., p. 1065 s.

[418] «Non si tratta di intercettazione ambientale con l'uso del microfono, non si tratta di captare da remoto tutti i *files* e contenuti del supporto, ma soltanto fare una" foto" di ciò che appare a video»: così S. ATERNO, *Captatore informatico e regolamento tecnico: quid juris per la modalità "screen shot"?,* dicembre 2017, *online* http://www.dirittopenaleinformatica.it/wp-content/uploads/2018/03/S.-ATERNO_Captatore-informatico_quid-iuris-per-modalit%C3%A0-screen-shot-1.pdf.

III.5 Perquisizioni *online* e finalità preventive.

Le discussioni sulla legittimità delle perquisizioni *online* si concentrano maggiormente sugli aspetti relativi alle investigazioni nel corso del processo penale, non considerando un aspetto altro fondamentale, caratterizzato dall'utilizzo di questa nuova fattispecie per l'efficace repressione dei reati (anche futuri o non ancora conosciuti[419]) e nelle politiche estere di lotta al terrorismo[420] che sollecitano l'uso dello strumento, quale il *trojan*, che potrebbe comportare numerosi rischi in tema di protezione delle garanzie fondamentali[421].

Attualmente un uso parallelo dei captatori informatici consentirebbe attività di *intelligence* mediante le perquisizioni *online* preventive "in senso stretto", e ipotesi di sorveglianza "di massa", e sono volte all'acquisizione del materiale investigativo attraverso una ricerca con parole chiave, le cui risultanze sono utilizzate a monte, rispetto alla successiva iscrizione della notizia di reato[422].

Per i controlli preventivi *stricto sensu*, il fondamento normativo si può riscontrare nell'art. 226 disp. att. c.p.p. sulla cui base il procuratore della Repubblica potrà autorizzare le "intercettazioni e controlli preventivi sulle comunicazioni"[423], in cui sono disciplinati anche i profili procedurali relativi alla conservazione o distruzione dei dati acquisiti, modificato nel 2015 sulla base delle disposizioni europee relative al terrorismo[424]; inoltre, la disciplina sarà estesa anche nei luoghi indicati dall'art. 614 c.p. qualora sia necessario per la prevenzione di gravi reati o delitti commessi dalla criminalità organizzata. I dati raccolti da tali operazioni preventive potranno essere utilizzati solo per "finalità interne", ex art. 226 disp. att. c.p.p., comma 5, ossia solo per

---

[419] R. FLOR, *Brevi riflessioni*, cit., p. 696 s., 703 s.; S. MARCOLINI, *Le cosiddette perquisizioni on-line*, cit., p. 2855 s.

[420] In particolare, direttiva 2016/680/UE e direttiva 2016/681/UE, del 27 aprile 2016; direttiva 2017/541/UE, del 15 marzo 2017; cfr. d.l. 18 febbraio 2015, n. 7 convertito dalla L. 17 aprile 2015, n. 43.

[421] Sulla tutela delle garanzie fondamentali e finalità preventive delle perquisizioni *online*, *infra* § III.3 Il bilanciamento tra le garanzie costituzionali e le esigenze investigative nel diritto italiano.

[422] W. NOCERINO, *Il captatore informatico: un Giano bifronte. Prassi operative vs risvolti giuridici*, in *Cass. pen*., 2020, p. 824 s.

[423] Sulla norma, G. DI PAOLO, voce *Prova informatica (diritto processuale penale)*, in *Enc. dir., Annali*, vol. VI, Giuffrè, 2013, p. 748.

[424] D.l. 18 febbraio 2015, n. 7, cit.

scopi investigativi e al fine di poter richiedere in seguito al giudice un provvedimento che autorizzi le intercettazioni[425]. Le attività preprocedimentali dovranno essere tenute distinte dalle attività successive processuali, potendo, peraltro, alcuni elementi raccolti in sede preventiva, finire per essere qualificati come prove "precostituite", ai sensi dell'art. 234 c.p.p.[426]. La citata normativa potrebbe essere applicata alle intercettazioni tramite captatore, se intese come un'innovazione del tradizionale mezzo di ricerca della prova che, analogamente a quanto avviene nella fase processuale, potrebbe finire per essere utilizzato per le altre attività esperibili attraverso il trojan, rendendo più ampia la categoria dei controlli preventivi.

Le tecniche di sorveglianza di massa sono, invece, attività di investigazione "passiva", volte alla raccolta generale dei dati, che saranno conservati e selezionati ai fini dei controlli preventivi in senso stretto, nel caso in cui si palesi un pericolo o una grave minaccia da scongiurare: i dati raccolti saranno esaminati da determinati programmi di analisi, basati su "criteri c.d. *target*" fondati sul concreto rischio in questione; si tratterebbe di una sorta di preinchiesta dalle numerose perplessità[427], considerando che le relative risultanze probatorie condurrebbero all'iscrizione della notizia di reato e nell'inizio formale delle indagini preliminari[428], nonostante il divieto previsto dall'art. 226, comma 5, disp. att. c.p.p., sulle operazioni intercettive svolte mediante captatore informatico.

III.5.1 Il caso "*Ryanair*" e il divieto di perquisizioni *ad explorandum*.

Il principale approdo normativo relativo alle tecniche di sorveglianza di massa è la sentenza della Corte di Cassazione del 17 aprile 2012, "Soc. *Ryanair*"[429] in cui è stato

---

[425] Cfr. A. VIRGILIO, *Il nuovo regime delle intercettazioni preventive*, in *Giust. pen.*, 2002, p. 545. Sul divieto che gli elementi raccolti siano oggetto di deposizione nel corso del procedimento penale, Corte cost., 29 luglio 2008, n. 305; cfr. N. GALANTINI, *Inutilizzabilità della prova e diritto vivente*, in *Riv. it. dir. e proc. pen.*, 2012, p. 64 s.

[426] Così L. PARLATO, *Le perquisizioni on-line*, cit., p. 375.

[427] *Ibidem*, p. 376 ss.

[428] W. NOCERINO, *Il captatore informatico*, cit., p. 824 s., in particolare §§ 5.2 e 6.

[429] Cass., Sez. IV, 17 aprile 2012, *Soc. Ryanair*, in *Cass. pen.*, 2013, p. 1523 s. Cfr. A. PAOLETTI, *La ricerca della prova penale*, cit., p. 434.

fissato un limite invalicabile relativo alla disciplina delle perquisizioni *online*: la Suprema Corte ha ritenuto legittima la decisione di annullamento disposta dal Tribunale del riesame, del decreto del pubblico ministero di perquisizione e sequestro, ai sensi dell'art. 247 c.p.p., delle *password* per il sistema di *booking online* dei voli della compagnia aerea. Tale investigazione era volta al preventivo riconoscimento dei c.d. "ovulatori", ossia i corrieri internazionali di sostanze stupefacenti e psicotrope, sulla base di un sospetto nato dall'analisi di diversi parametri sintomatici relativi alle prenotazioni dei voli, quali, soggiorni di breve durata, prenotazioni *last-minute*, o la preferenza di itinerari notturni. Nel caso *de quo*, l'obiettivo illecito consisteva in una inversione dell'ordine consequenziale delle fasi del procedimento penale, in quanto il monitoraggio preventivo ed illimitatamente esplorativo del sistema delle prenotazioni *online*, oltre alla problematica relativa all'inclusione di dati personali di soggetti estranei alle indagini, era effettuato in mancanza di una originaria notizia di reato iscritta nel registro, ex art. 335 c.p.p., dal quale decorrono i termini per la durata delle indagini preliminari.

Nell'avallare la decisione in sede di riesame, la Corte di Cassazione ha confermato l'annullamento sostenendo che tale provvedimento fosse mirato, non all'acquisizione di elementi utili per l'iscrizione della *notitiae criminis*, ma fosse volto al monitoraggio «illimitato, preventivo e permanente del contenuto di un sistema informatico», in modo da pervenire «all'accertamento di reati non ancora commessi, ma dei quali si ipotizzava la futura commissione da parte di soggetti ancora da individuarsi»; vietando questa prassi, si è ritenuto «da escludere un preventivo ed indefinito monitoraggio in attesa dell'eventuale e futura comparsa del dato da acquisire a base delle indagini». Inoltre, la Suprema Corte ha osservato le differenze tra la perquisizione tradizionale e le particolari perquisizioni *online,* affermando che quest'ultima potrebbe essere utilizzata non solo come un nuovo mezzo di ricerca della prova di un reato oggetto di indagini, ma anche come «un nuovo ed anomalo strumento di ricerca della prova, con finalità nettamente esplorative, di mera investigazione»; infatti, tale sentenza fa emergere i rischi che potrebbero verificarsi se si utilizzasse un mezzo di ricerca della prova non disciplinato dal legislatore, relativi soprattutto alla compromissione dei diritti fondamentali dell'individuo e al rispetto del principio di legalità e della riserva di legge.

III.6.1 L'inammissibilità delle perquisizioni occulte come un punto di partenza per il futuro.

Le ragioni garantistiche opposte agli approdi giurisprudenziali sin qui menzionati, affermerebbero l'inammissibilità delle perquisizioni online compiute attraverso il captatore informatico. L'inoculazione del *software* esplorativo comporterebbe un'attività di ricerca altamente intrusiva simile ad una sorta di perquisizione personale, incompatibile con il principio del rispetto della dignità umana[430]. Pertanto, le uniche perquisizioni ritenute legittime sono quelle riconducibili nell'alveo delle perquisizioni informatiche di cui all'art. 247, comma 1-*bis* c.p.p., che sono conoscibili da parte dell'indagato nonostante si tratti di atti "a sorpresa".

Tuttavia, affermare che le perquisizioni *online* siano un mezzo di prova inammissibile funge da punto di partenza per un ragionamento basato sullo stabilire le condizioni per cui tale strumento possa essere ritenuto legittimo, considerando l'importanza che lo stesso ha acquisito nell'ordinamento italiano per lo svolgimento delle indagini, e a livello sovranazionale[431]. È innegabile la necessità di un intervento da parte del legislatore, nella previsione di una regolamentazione normativa nel sistema italiano ad *hoc* relativa alle perquisizioni *online*, non solo in chiave preventiva, in considerazione degli impulsi europei in tema di lotta al terrorismo, ma soprattutto in chiave investigativa, raggiungendo un equo bilanciamento, alla luce del principio di proporzionalità, tra il diritto costituzionalmente protetto alla riservatezza, anche informatica, e l'esigenza dell'efficace repressione dei reati: spetterà al legislatore prevedere i casi e i modi in cui queste operazioni di intromissione nei sistemi informatici potranno essere realizzate, stabilendo, ad esempio un'elencazione dei reati presupposto, le forme del provvedimento dell'autorità giudiziaria, i relativi casi di urgenza, le modalità di esecuzione dell'attività occulta di indagine, svolte da professionisti del settore ; inoltre, dovranno essere stabilite particolari garanzie a tutela dei dati personali irrilevanti per le indagini, con relative sanzioni di inutilizzabilità.

---

[430] Sulle criticità espresse dalla dottrina si rinvia a P. BALDUCCI, *Perquisizioni*, in *Enc. dir*., IV, Milano, 2000, p. 982.

[431] F. IOVENE, *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale.*, in *Riv. trim. dir. pen. cont*. 2014, 3-4.

Uno spunto potrebbe essere l'esempio tedesco che ha recepito l'importanza di questo strumento, già per l'attività preventiva, ma anche e soprattutto in relazione allo svolgimento delle indagini preliminari[432].

[432] *Infra*, § III.2.2.

BIBLIOGRAFIA

AGOSTINI B., *La disciplina delle intercettazioni preventive nel sistema antiterrorismo.*, in *Riv. trim. Diritto penale contemporaneo*, Milano, 2016.

ALGERI L., BACCARI G., CAJANI F., CONTI C., CURLOTTI D., MARRAFINO M., NOCERINO W., TOGNAZZI S., TORRE M., *Nuove tecnologie e processo penale. Articoli estratti dalla rivista "Diritto penale e processo"*, Wolters Kluwer, novembre 2021.

ALONZI F., *Revisioni Normative in Tema Di Intercettazioni: Riservatezza, Garanzie Difensive e Nuove Tecnologie Informatiche*, GIOSTRA, G., ORLANDI, R., Giappichelli, Torino, 2021.

AMATO G., *I reati informatici: nuova disciplina e tecniche processuali di accertamento*, Padova, CEDAM, 2010.

AMOROSO A., "*Digital Forensics: La Prospettiva Di Un Informatico*", in *Sicurezza e scienze sociali.* Milano, 2017, 3, 2018, 110–126.

ANGELI F., "*Cibercrimine e Anonimato in Rete. Riflessioni Su Sicurezza, Efficacia Investigativa e Tutela Delle Libertà Personali*." in *Sicurezza e scienze sociali*, Milano, 2017, 3, 2018, 29–43.

ANGELI F., "*Computer Forensic*." in *Sicurezza e scienze sociali*, Milano, 2017, 3 2018, 99–109.

APRILE E., *voce Captazioni atipiche (suoni, immagini, segnali)*, in SCALFATI, A., (diretto da), *Dig. proc. pen. online*, Giappichelli, Torino, 2013.

ATERNO S., *Acquisizione e analisi della prova informatica*, in *Dir. Pen. Proc.*, 2008.

ATERNO, S., *Captatore informatico e regolamento tecnico: quid juris per la modalità "screen shot"?,* dicembre 2017, *online* http://www.dirittopenaleinformatica.it/wp-content/uploads/2018/03/S.-ATERNO_Captatore-informatico_quid-iuris-per-modalit%C3%A0-screen-shot-1.pdf.

ATERNO S., *Digital forensics (investigazioni informatiche)*, in *Dig. disc. pen.* (agg.), 2014, pp. 217-247.

ATERNO S., *La Cassazione, alle prese con il captatore informatico, non convince sull'acquisizione mediante screenshot*, in *Dir. pen. proc.*, 2018.

ATERNO S., *Le investigazioni informatiche e l'acquisizione della prova digitale,* in *Giur. merito*, 2013.

ATERNO S., CAJANI F., COSTABILE G., MATTIUCCI M., MAZZARCO G., *Computer Forensics e Indagini digitali*, vol.1, Experta, 2011.

ATERNO S., MATTIUCCI M., *Cloud Forensics e nuove frontiere delle indagini informatiche nel processo penale*, in *Arch. pen.*, 3/2013.

BAIGUERA ALTIERI A., *La cultura Hacker negli Stati Uniti d'America*, in *La criminalità informatica in Svizzera e in Italia*, in *diritto.it*, dicembre 2011.

BALDUCCI P., *Perquisizioni*, in *Enc. dir*., IV, Milano, 2000.

BALLONI A., BISI R., SETTE R., *Principi di criminologia applicata: criminalità, controllo, sicurezza*, Assago, Wolters Kluwer, 2015.

BALSAMO A., *Intercettazioni ambientali mobili e cooperazione giudiziaria internazionale: le indicazioni desumibili dalla giurisprudenza della Corte di Strasburgo*, in *Cass. pen.*, 2016.

BALSAMO A., *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*, in *Cass. pen*., 2015.

BENE T., *Intercettazioni. Intrecci e discordanza di idee nella stagione delle riforme processuali*, in *Diritto penale e processo*, 2020, fasc. 12, pp. 1641-1647.

BENE T., (a cura di), *L'intercettazione di comunicazioni*, Bari, Cacucci Editore, 2018.

BERGHELLA F., BLAIOTTA R., *Diritto penale dell'informatica e beni giuridici*, in *Cass. Pen*., 9/1995, 2329.

BLECHSCHNITT L., *Zur Einführung von Quellen-TKÜ und Online Durchsuchung*, in *StraFo*, 2017.

BRODOWSKI D., FREILING F., *Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, in Forschungsforum Öffentliche Sicherheit*, 4/2011, 164 ss., in www.sicherheit-forschung.de.

CACCAVELLA D. E., *La L. 48/2008 ed il reperimento delle fonti di prova da sistemi digitali*, http://www.marcomattiucci.it/l482008.php.

CADOPPI A., CANESTRARI S., MANNA A., PAPA M., *Cybercrime*, Torino, UTET giuridica, 2019.

CARDONA G.R., *Antropologia della scrittura*, Torino, 2009.

CAIANELLO M., *Il principio di proporzionalità nel procedimento penale*, in *Dir. pen. cont., Riv. trim.*, 2014, (3-4).

CAJANI F., et al., *Phishing e furto d'identità digitale: indagini informatiche e sicurezza bancaria*, Milano, Giuffrè, 2008.

CAJANI F., *La L. 48/2008 ed il reperimento delle fonti di prova da sistemi digitali*., gennaio 2010, e consultabile gratuitamente *online* su: http://www.marcomattiucci.it/informatica_digitalforensics_l482008.php

CAJANI F., *Odissea del captatore informatico*, in *Cass. pen*., 2016, p. 4143.

CAMON A., *Cavalli di Troia in Cassazione*, in *Arch. nuova proc. pen.*, 2017.

CAMON A., *Il nuovo procedimento di spoglio dei risultati delle intercettazioni*, in *La Legislazione penale*, 2020, fasc. 11.

CAMON A. *Fondamenti di procedura penale*, Assago, Wolters Kluwer, 2021.

CALABRÒ V., COSTABILE G., FRATEPIETRO S., IANULARDO M., NICOSIA G., *L'alibi informatico. Aspetti tecnici e giuridici*, in IISFA Memberbook 2010, Forlì, Experta.

CANZIO G., LUPÁRIA L., *Prova scientifica e processo penale*, Padova, CEDAM, 2018.

CAPRIOLI F., *La procedura di filtro delle comunicazioni rilevanti nella legge di riforma della disciplina delle intercettazioni (The Filtering Procedure of the Relevant Communications in the New Wiretap Law)*, in *Cassazione penale*, 2020, fasc. 3, pp. 1384-1416.

CARRATTA A., et al., *Dimensione Tecnologica e Prova Penale*, Torino, Giappichelli, 2020.

CASADEI T., PIETROPAOLI S., *Diritto e tecnologie informatiche*, CEDAM, 2021.

CASSANO G., SCORZA G., VACIAGO G., *Diritto Dell'Internet: Manuale Operativo: Casi, Legislazione, Giurisprudenza*, CEDAM, Padova, 2013.

CASSANO G., PREVITI S., *Il diritto di internet nell'era digitale*, Milano, Giuffrè Francis Lefebvre, 2020.

CATANIA E., *Profili essenziali delle intercettazioni telematiche. Dalla tutela costituzionale della segretezza ed inviolabilità di qualsiasi forma di comunicazione alla disciplina ex art. 266 c.p.p.*, in *Diritto.it Rivista giuridica elettronica, online* su https://www.diritto.it, 27 dicembre 2013.

CHELO A., *Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria*, Padova, CEDAM, 2014.

CIAVOLA A., *Prova testimoniale e acquisizione per suo tramite del contenuto delle intercettazioni telefoniche*, in *Cass. pen*., 2000.

CICCIA ROMITO C., ZICCARDI G., *Il GDPR nella micro, piccola e media impresa: un percorso di semplificazione della compliance tra protezione dei dati e adempimenti di legge*, Milano, Giuffrè Francis Lefebvre, 2021.

COLAIOCCO S., *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *Arch. Pen*. LXVI, 1, 2014, p. 187-197.

COLAROCCO V., GROTTO T., VACIAGO G., *La prova digitale*, Milano, Giuffrè Francis Lefebvre, 2020.

COLOMBO C. F., *Economia criminale: geodiritto, globalizzazione e nuovi canali per i reati d'impresa*, Milano, Wolters Kluwer, 2021.

CONIGLIARO V., *La nuova tutela penale europea dei sistemi di informazione, Una prima lettura della direttiva 2013/40/UE del Parlamento europeo e del Consiglio*, in *Dir. pen. cont*., 30 ottobre 2013.

CONSO G., GREVI V., BARGIS M. (a cura di), *Compendio di procedura penale*, X ed., Torino, 2020.

CONTI C., *Accertamento del fatto e inutilizzabilità nel processo penale*, CEDAM, Padova, 2007.

CONTI C., *Le nuove norme sulla riservatezza delle intercettazioni: anatomia di una riforma discussa*, in *Giur. it., Speciale*, 2018, 1754.

CONTI C., *La prova scientifica alle soglie dei vent'anni dalla sentenza Franzese: vette e vertigini in epoca di pandemia*, in *ww.sistemapenale.it*., 9 febbraio 2021.

CONTI C., *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Dir. Pen e processo*, 2018, pp. 1210-1221.

CORASANITI G., CORRIAS LUCENTE G., ATERNO S., *Cybercrime, responsabilità degli enti e prova digitale: commento alla legge 18 marzo 2008, n. 48, ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*, Padova, CEDAM, 2009.

COSTABILE G., *Scena criminis, documento informatico e formazione della prova penale*, in *Dir. inf*., 2005.

CUOMO L., RAZZANTE R., *La nuova disciplina dei reati informatici*, Torino, Giappichelli, 2009.

D'AGOSTINI D. et al., *Diritto penale dell'informatica: dai computer crimes alla digital forensic*, Forlì: Experta, 2007.

DANIELE M., *Il diritto al preavviso della difesa nelle indagini informatiche*, in *Cass. pen.*, p. 441 s., 2012.

DANIELE M., *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, 2.

DE CATALDO NEUBURGER L. (a cura di), *La prova scientifica nel processo penale*, Padova, CEDAM, 2007.

DE GREGORIO E., *Riflessioni in tema di attualità e prospettive della raccolta e dello scambio della prova digitale*, in *Informatica e diritto*, (2), 171-184, 2016.

DI BITONTO M. L., *L'accentramento investigativo delle indagini sui reati informatici*, in *Dir. dell'internet*, 2008.

DI PAOLO G., *Acquisizione dinamica dei dati relativi all'ubicazione del cellulare ed altre forme di localizzazione tecnologicamente assistita. Riflessioni a margine dell'esperienza statunitense*, in *Cass. pen.*, n. 3, 2008.

DI PAOLO G., voce *Prova informatica (diritto processuale penale)*, in *Enc. dir., Annali*, vol. VI, Giuffrè, 2013, pp. 736-762.

DI RESTA F., BRUN A., PIZZETTI F., *La tutela dei dati personali nella società dell'informazione.*, Torino, Giappichelli, 2009.

DI STEFANO P., *Il* Trojan horse *nel processo penale*, in www.giustiziainsieme.it, 28 ottobre 2020.

DOLCINI E., MARINUCCI G., GATTA L., *Codice penale commentato*, 5 edizione, Assago, Wolters Kluwer, 2021.

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

EPIFANI M., LA MUSCATELLA D., MEDA C., *Guida alla prova digitale: il primo approccio del Consiglio d'Europa all'armonizzazione delle diverse metodologie investigative*, in *Ciberspazio e diritto*, vol. 15, n. 51 (2/3-2014), pp. 375-411.

FARINA M., GOMETZ G., *Elementi di diritto dell'informatica*, Milano, Wolters Kluwer, 2019.

FELICIONI P., *L'acquisizione da remoto dei dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Processo penale e giustizia*, n. 5, 2016.

FELICIONI P., *Le ispezioni e le perquisizioni*, Milano, Giuffrè, 2004.

FERRUA P., MARZADURI E., SPANGHER G. (a cura di), *La prova penale*, Giappichelli, Torino, 2013.

FIANDACA G., MUSCO E., *Diritto penale. Parte generale*, Settima edizione, Bologna, Zanichelli, 2014.

FILIPPI L., *Intercettazioni: "habemus legem"!*, in *Diritto penale e processo*, 2020, fasc. 4, pp. 453-466, 2020.

FLOR R., *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online durchsuchung*, in *Riv. trim. dir. pen. ec*., 3, 2009.

FLOR R., *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, in *Dir. pen. proc*., 2015, 10.

FLOR R., *La corte di giustizia considera la Direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in Riv. trim. *Diritto penale contemporaneo*, 2014.

GABRINI D., *La L. 48/2008 ed il reperimento delle fonti di prova da sistemi digitali, online* su http://www.marcomattiucci.it/l482008.php.

GALANTINI N., *Inutilizzabilità della prova e diritto vivente*, in *Riv. it. dir. e proc. pen.*, 2012.

GHIRARDINI G., FAGGIOLI G., *Digital forensics.*, Apogeo, 2013.

GIALUZ M., (a cura di), *Le nuove intercettazioni. Legge 28 febbraio 2020, n. 7*, in *Diritto di internet*, 2020, fasc. 3 (suppl.).

GIALUZ M., *Riservatezza e nuova disciplina delle intercettazioni*, in *Rivista penale*, 2020, fasc. 7-8, pp. 667-677.

GIORDANO L., "*Dopo le sezioni unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo.* Osservazioni a seguito di Cass., SSUU, sent. 28 aprile 2016 (dep. 1° luglio 2016), n. 26889, Pres. Canzio, Rel. Romis, ric. Scurato", in *Diritto penale contemporaneo*, 2017, 3, pp. 177-195.

GIORDANO L., *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte*, in *Sist. pen*., 2020 (4).

GLESS S., *Wenn das Haus mithör: Beweisverbote im digitalen Zeitalter*, in *StV*, 2018.

GUPTA BRIJ B., DAHIYA A., *Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges, and Countermeasures*, Boca Raton, FL; CRC Press, Taylor & Francis Group, 2021.

HEINRICH M., *Surfen im Internet und Cloud Computing zwischen Telekommunikationsüberwachung und Online Durchsuchung*, in *ZIS*, 2020.

HIÉRAMENTE M., *Surfen im Internet doch Telekommunikation im Sinne des § 100a StPO,* in *HRRS,* 2016.

IASELLI M., *Investigazioni digitali*, Milano, Giuffrè Francis Lefebvre, 2020.

ILARDA G., MARULLO G., *Cybercrime: conferenza internazionale: la Convenzione del Consiglio d'Europa sulla criminalità informatica*, Milano, Giuffrè, 2004.

ILLUMINATI G., *La disciplina processuale delle intercettazioni*, Milano, Giuffrè Francis Lefebvre, 1983.

ILLUMINATI G., *Osservazioni a margine di Cass., Sez. un., 28 novembre 2019 (dep. 2 gennaio 2020), n. 50, Pres. Carcano, est. Caputo*, in *Sistema Penale*, 30 gennaio 2020.

IOVENE F., *"Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale."*, in *Riv. trim. dir. Pen. Cont*. (2014): 3-4.

KOSTORIS R. E., (a cura di), *Manuale di procedura penale europea*, Giuffrè, 2019.

LARONGA A., *Le prove atipiche nel processo penale*, CEDAM, Padova, 2002.

LEIPOLD K., BEUKELMANN S., *Online-Durchsuchung und Quellen-TKÜ,* in *NJW-Spezial*, 2017.

LORENZETTO E., *Utilizzabilità dei dati informatici incorporati su computer in sequestro: dal contenuto al contenitore, passando per la copia*, in *Cass. pen*., 2010, pp. 1522-1533.

LORUSSO S., *L'arte di ascoltare e l'investigazione penale tra esigenze di giustizia e tutela della privatezza,* in *Dir. pen. proc*., 2011.

LUPARIA DONATI L., ZICCARDI G., *Investigazione penale e tecnologia informatica: l'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, Giuffrè, 2007.

LUPARIA L., *Internet Provider e Giustizia Penale: Modelli Di Responsabilità e Forme Di Collaborazione Processuale,* Milano, 2012.

LUPARIA L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa* (l. 18 marzo 2008, n. 48). *Profili di diritto processuale*, in *Dir. pen. proc*., 6/2008.

LUPÁRIA L., *Sistema penale e criminalità informatica: profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul Cybercrime (l. 18 marzo 2008, n. 48)*, Milano, Giuffrè, 2009.

MACCHIA A., *I diritti fondamentali "minacciati": lo sfondo delle garanzie in costituzione,* in *Diritto Penale Contemporaneo,* 17 luglio 2017.

MADEO A., CIANCHELLA V., *Guida pratica operativa alle investigazioni. II edizione riveduta e aggiornata alla Legge n. 7/2020*, Padova, CEDAM, 2020.

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

MANES V., ZAGREBELSKY V., (a cura di), *La Convenzione europea dei diritti dell'uomo nell'ordinamento penale italiano*, Giuffrè, 2011.

MARCOLINI S., *Le cosiddette perquisizioni on-line (o perquisizioni elettroniche)*, in *Cass. pen*., 07/08, 2010.

MARINELLI C., *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Torino, 2007.

MARIOTTI S., TACCONI S., *Riflessioni sulle problematiche investigative e di sicurezza connesse alle comunicazioni VoIP*, in *Diritto dell'Interne*t, 2008, n. 6, pp. 558- 562.

MARTINO L., *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica&Società*, 2018, 1.

MENSI M., FALLETTA P., *Il diritto del web*, Padova, CEDAM, 2018.

MILITELLO V., *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*, in *Riv. trim. dir. pen. econ*., 1992, pp. 365-377.

MIRIELLO A, GOVERNATORI L., *Captatore informatico: aspetti tecnici e criticità. I nostri dati sono in buone mani?*, in www.scienzeforensi.org, 30 maggio 2020.

MODUGNO F., CARNEVALE P., *Diritto Pubblico*, Giappichelli, Torino, 2015

MOLINARI F. M., *Questioni in tema di perquisizioni e sequestro di materiale informatico*, in *Cass. pen*., 2012, n. 2, pp. 696-716.

MONTI A., *Attendibilità dei sistemi di computer forensic*, in ICT-Security, Vol. 9, 2003 (disponibile on line: http://www.ictlex.net/?p=287).

MONTI A., *No ai sequestri indiscriminati di computer*, in *Diritto dell'Internet*, 3, 2007, 264-270.

MORGANTE G., *Commento a L. 18 marzo 2008, n. 48. Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*. Pubblicata nella Gazz. Uff. 4 aprile 2008, n. 80, in *Legislazione Penale*, 2008, vol. 3, pp. 251-280.

MOSCARINI P., *Lineamenti Del Sistema Istruttorio Penale*, Giappichelli, Torino, 2017.

NERI G., *Criminologia e reati informatici: profili di diritto penale dell'economia*, Roma, Laterza, 2014.

NEVOLI F., *Intercettazioni informatiche e telematiche: ricorso ad impianti esterni ed obbligo motivazionale del pubblico ministero*, in *Arch. nuova proc. pen*., 2010.

NOCERINO W., *Il captatore informatico: un Giano bifronte. Prassi operative vs risvolti giuridici*, in *Cass. pen*., 2020.

NOVARIO F., *Criminalità informatica e sequestro probatorio: le modifiche introdotte dalla l. 18 marzo 2008, n. 48 al codice di procedura penale*, *Rivista di diritto processuale*, 63 n. 4 (Luglio-Agosto2008), p.1069-1071.

ONG W. J., *Oralità e scrittura. Le tecnologie della parola*, Bologna, 1986.

ORLANDI R., *La riforma del processo penale fra correzioni strutturali e tutela progressiva dei diritti fondamentali*, in *Riv. it. dir. e proc. pen*., 2014.

PANATTONI B., *Compliance, cybersecurity e sicurezza dei dati personali*, Assago, Wolters Kluwer, 2020.

PAOLETTI A., *La ricerca della prova penale nell'era delle nuove tecnologie informative*, Key, 2020.

PARLATO L., *Il legislatore tedesco approfitta di una più ampia riforma per disciplinare le perquisizioni online,* in *Cass. pen*., 2019.

PARLATO L., voce *Perquisizioni on-line*, in *Enc. dir*., Annali, vol. X, Giuffrè, 2017.

PARODI C., *La disciplina delle intercettazioni telematiche*, in *Dir. pen. e proc*., 2003.

PARODI C., *VoIP, Skype e tecnologie d'intercettazione: quali riposte d'indagine per le nuove frontiere di comunicazione?*, in *Diritto penale e processo*, 2008, n. 10.

PECORELLA C., *Diritto penale dell'informatica*, Ristampa con aggiornamento, Padova, CEDAM, 2006.

PETRINI D., *La responsabilità penale per i reati via internet.,* Napoli, Jovene, 2004.

PEYRON C., *L'ispezione giudiziale*, in *En. Dir*, vol. XXII, Giuffrè, Milano, 1972.

PICOTTI L., *Commento all'art. 3 della l. n. 547 del 1993*, in *L. Pen*., 1996.

PICOTTI L., *Il diritto penale dell'informatica nell'epoca di Internet.,* Padova, CEDAM, 2004.

PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa* (l. 18 marzo 2008, n. 48). *Profili di diritto penale sostanziale*, in *Dir. pen. proc*., 6/2008, 700.

PRETTI D., *La metamorfosi delle intercettazioni: la contro-riforma Bonafede e l'inarrestabile mito della segretezza delle comunicazioni*, in *Sist. pen.* (o SP), 2/2020, pp. 71-107.

RESTA F., *Cybercrime e cooperazione internazionale nell'ultima legge della legislatura, in Giur. Merito*, 2008, fasc. 9, pp. 2147-2161.

ROGGAN F., *Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung: Elektronische Überwachungsmaßnahmen mit Risiken für Beschuldigte und die Allge meinheit*, in StV, 2017, p. 821, richiamando BVerfG, 20 aprile 2016.

ROSONI I., *Verità Storica e Verità Processuale. Lo Storico Diventa Perito*. *Acta Histriae*, vol. 19, no. 1-2, 2011, pp. 127-140.

SARZANA DI S. IPPOLITO C., CONSO G., *Informatica, internet e diritto penale*, 3. ed. riveduta, corretta ed ampliata, Milano, Giuffrè, 2010.

SARZANA DI S. IPPOLITO C., *La Convenzione europea sulla cibercriminalità*, in *Dir. pen. proc*., 4/2002.

SCALFATI A., *Intercettazioni: spirito autoritario, propaganda e norme inutili,* in *Arch. Pen*., 2014, 2.

SCALFATI A., (a cura di), *Le indagini atipiche.*, Seconda edizione, Torino, Giappichelli, 2019.

SHINDER LITTLEJOHN D., *Scene of the Cybercrime. Computer Forensics Handbook /*. Rockland, MA: Syngress Publishing, 2002.

SIGNORATO S., *Le indagini digitali. Profili strutturali di una metamorfosi investigativa,* Giappichelli, 2018.

SINGELNSTEIN T., DERIN B., *Das Gesetz zur effektiven und praxistauglicheren Ausgestaltung des Strafverfahrens,* in *NJW,* 2017.

SIRACUSANO F., *Manuale di procedura penale,* Milano, Giuffrè, 1990.

TABASCO G., *Prove non disciplinate dalla legge nel processo penale, Le "prove atipiche" tra teoria e prassi*, Napoli, 2011.

TONELLOTTO M., *Evidenza informatica, computer forensics e best practices*. *Rivista di Criminologia, Vittimologia e Sicurezza* 8.2, 2014, 68-103.

TONINI P., CONTI C., *Manuale di procedura penale,* Ventiduesima edizione, Milano, Giuffrè Francis Lefebvre, 2021.

TONINI P., *Dalla perizia "prova neutra" al contraddittorio sulla scienza*, in *Dir. pen. proc*., 2011, pp. 360-369.

TONINI P., *Documento informatico e giusto processo,* in *Dir. pen. proc*., 2009, pp.401-406.

TONINI P., *Il documento informatico: problematiche civilistiche e penalistiche a confronto,* in *Corriere giuridico* (Il), 2012, n. 3, p. 432/239.

TORRE M., *Aspetti giuridici e tecnici relativi al trattamento della prova digitale nel processo penale. La prova informatica nella legge 18 marzo 2008, n. 48*, in *Informatica e diritto*, XLI annata, Vol. XXIV, 2015, n. 1-2, pp. 65-104.

TORRE M., *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali,* Milano, 2017.

TORRE M., *La raccolta della prova digitale in Italia: dagli accertamenti statici al captatore itinerante*, *Informatica e diritto,* (2), 157-170, 2016.

TRINCHELLA G., *Spionaggio, i fratelli Occhionero sapevano dell'indagine. Distrutti dati, file e account il giorno prima della perquisizione,* in www.ilfattoquotidiano.it, 11 gennaio 2017.

UBERTIS G., VOENA G.P., (diretto da), *Trattato di procedura penale*, XIX, Milano, 2012.

VASSALLI G., *La libertà personale nel sistema delle libertà costituzionali*, in Id., *Scritti giuridici*, vol. III, Milano, 1997.

VIRGILIO A., *Il nuovo regime delle intercettazioni preventive*, in *Giust. pen.*, 2002.

VITALE A., *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico*, in *Dir. dell'Internet*, 2008.

ZICCARDI G., *Informatica giuridica. Privacy, sicurezza informatica, computer forensics e investigazioni digitali*, Tomo II, Seconda ed., Milano, 2012.

ZICCARDI G., *Manuale breve di informatica giuridica*, Milano, Giuffrè, 2008.

ZICCARDI G., *Parlamento europeo, captatore informatico e attività di hacking delle Forze dell'Ordine: alcune riflessioni informatico giuridiche*, in *Arch. pen.*, 2017, 1.

ZONARO M., *Il Trojan - Aspetti tecnici e operativi per l'utilizzo di un innovativo strumento di intercettazione*, in *Parole alla difesa*, 2016, n. 1.