Alma Mater Studiorum – Università di Bologna

DOTTORATO DI RICERCA IN

DIRITTO E NUOVE TECNOLOGIE

Ciclo XXVII

Settore Concorsuale di afferenza: 12/H3

Settore Scientifico disciplinare: IUS/20

ForensicStorage

Custodia, gestione ed analisi dei reperti informatici

Presentata da: Andrea Paselli

Coordinatore Dottorato
Prof. Giovanni Sartor

Relatore
Prof. Cesare Maioli

Esame finale anno 2016

Indice

Introduzione.

Nel mondo investigativo l'analisi forense digitale ha assunto un ruolo sempre più rilevante negli ultimi anni. La ricerca di prove digitali all'interno delle indagini è diventata imprescindibile da qualsiasi caso legale, dal più banale, in cui per recuperare il maggior numero d'informazioni sull'indagato viene sequestrato il suo *computer* per analizzarne il contenuto, al più complesso, come un caso di *cyber security*, in cui si cerca di combattere attacchi di *hacking* con le più recenti tecnologie *software* a disposizione.

Il mondo sta cambiando ed è in continua evoluzione, i morbosi interessi catodici del grande pubblico siano sempre più appagati da numerose trasmissioni che trasformano atroci e crudeli delitti di cronaca nera in emozionanti e attraenti *reality*, realizzando, di fatto, una sorta di tribunale virtuale dove vengono di volta in volta discusse e analizzate tesi accusatorie e difensive, trasformando spesso l'ignaro ascoltatore nel più improbabile criminologo.

E' tuttavia grazie anche a questa spettacolarizzazione del crimine che hanno preso piede i principi e le tecniche di investigazione scientifica, tra cui spicca proprio la *Digital Forensics*[1], la quale è stata la più giovane delle discipline d'indagine tecnica ad assurgere al ruolo di protagonista, diventando nota al grande pubblico almeno nelle sue applicazioni principali. Tutto ciò ha portato da un lato a considerare erroneamente il Consulente Tecnico quale unico responsabile della corretta soluzione del caso, talvolta in contrapposizione ai metodi investigativi tradizionali, e dall'altro alla banalizzazione della disciplina stessa, illudendo i più che basti avere qualche conoscenza informatica e del *software* idoneo, magari *open source*[2] per ambire al ruolo di Consulente Tecnico.

Un ulteriore aspetto degno di nota è l'ignoranza informatica, purtroppo ancora molto diffusa tra Giudici, Pubblici Ministeri ed Avvocati, che provenendo in molti casi da studi umanistici e giuridici non hanno la benché minima conoscenza in una materia spesso determinante nell'economia processuale.

Un altro aspetto degno di nota è l'ormai consolidata tendenza da parte di molti magistrati inquirenti a sopravvalutare l'importanza a fini investigativi degli accertamenti informatici anche a scapito di quelli "tradizionali".

---

[1] "*Digital Forensics*", è una branca della scienza forense che comprende il recupero e ricerca di materiale trovato in dispositivi digitali, spesso in relazione alla criminalità informatica.

[2] "*Open Source*", generalmente, *open source* si riferisce ad un programma per elaboratore in cui il codice sorgente è disponibile al pubblico per l'uso e/o modifica dal suo disegno originale.

Questa tendenza ha favorito un notevole incremento di richieste di perizie d'ufficio che ha fatto espandere il mercato dei Consulenti Tecnici che si è in tal guisa inevitabilmente popolato anche di operatori improvvisati spesso sprovvisti di sufficienti capacità e conoscenze tecniche necessarie per eseguire al meglio il delicato ruolo affidato loro. La giovane età di questa disciplina forense fa sì che la stessa sia ancora priva di un rigoroso inquadramento tecnico-giuridico e che soffra della mancanza di protocolli e linee guida riconosciuti a livello internazionale.

Infine, tra le maggiori criticità che questa disciplina si trova ad affrontare nella quotidianità, vi è il continuo e incessante progresso tecnologico e informatico che ha permesso in pochi anni all'utente medio di poter utilizzare *computer* sempre più potenti, sistemi operativi sempre più sofisticati, protocolli di comunicazione sempre più veloci e dispositivi di memoria sempre più capienti e capaci di fagocitare migliaia di *Gigabytes*[3] di dati. Basti pensare che appena cinque anni fa il massimo che potesse capitare a un Consulente Tecnico era di dover acquisire e analizzare un *hard disk* della capacità di 160 GB, mentre oggi la dotazione minima della maggior parte dei *computer* comprende *hard disk* della capacità di 2 *Terabyte*[4]; potrà inoltre capitare di trovarsi di fronte ad uno *storage* di rete di svariati TB, magari in RAID[5], per non parlare poi di *Cloud Storage*[6] e macchine virtuali sempre più diffuse e utilizzate. Il Consulente Tecnico non è pertanto un mero analista o un tecnico da laboratorio, deve essere invece un valido supporto all'organo inquirente o giudicante supportandoli nell'accertamento della verità processuale sin dalla formulazione dei quesiti, agendo sempre in modo neutro e asettico, redigendo al termine del proprio lavoro una relazione tecnica che fornisca al magistrato tutte le informazioni e le risposte necessarie affinché egli possa giungere alle sue conclusioni secondo il proprio libero convincimento.

La disciplina dell'informatica Forense, in inglese "*digital forensics*", è la scienza che studia in ambito giuridico, l'individuazione, la conservazione, la protezione, l'estrazione e la documentazione del dato informatico al fine di essere valutato in sede giudiziaria, è la disciplina che entra in gioco quando occorre

---

[3] "*Gigabyte*", il *gigabyte* è un'unità di misura dell'informazione o della quantità di dati ed è attualmente, fra i vari multipli del *byte*, quella più utilizzata nella pratica quotidiana. 1Gigabyte = 1 miliardo di *byte*.

[4] "*Terabyte*", il *terabyte* è un'unità di misura dell'informazione o della quantità di dati, il termine deriva dall'unione del prefisso *tera* con *byte* ed ha per simbolo TB. 1Terabyte = 1 bilione di *byte*.

[5] In informatica il RAID, acronimo di *Redundant Array of Independent Disks*, insieme ridondante di dischi indipendenti, è una tecnica di raggruppamento di diversi dischi rigidi collegati ad un *computer* che li rende utilizzabili, dalle applicazioni e dall'utente, come se fosse un unico volume di memorizzazione.

raccogliere prove all'interno di un *computer* o di un sistema informatico a seguito di un'azione criminosa[6]. La "*digital forensics*" è l'evoluzione naturale della "*computer forensics*", poiché ormai il numero di dispositivi digitali che utilizziamo quotidianamente è lievitato enormemente negli ultimi dieci anni: *smartphone*, *tablet*, macchine fotografiche digitali, lettori *eBook*, navigatori e lettori mp3, sono da un punto di vista tecnico tutti *computer* specializzati ciascuno nel proprio ambito, che complessivamente hanno ormai superato per diffusione i *personal computer* tradizionali, ecco perché è oggi più opportuna la definizione di "*digital forensics*". L'aspetto più noto e studiato della "*digital forensics*" è quello che si occupa, a fini probatori, delle tecniche e degli strumenti per l'esame metodologico dei sistemi informatici, *computer*, *hard disks*, *smartphone*, *tablet*, e altri dispositivi informatici. La "*computer forensics*" altro non è che l'estensione delle teorie, dei principi e delle tecniche, della scienza forense all'informatica, infatti, un'analisi forense effettuata su un *computer* o un sistema informatico può essere paragonata a un'autopsia effettuata dal medico legale corpo di una vittima[7].

In questo elaborato a partire dal primo capitolo si procederà ad una analisi dell'evoluzione normativa e giurisprudenziale dell'informatica giuridica con particolare attenzione alla ricerca ed analisi della prova digitale, partendo dai primi disegni di legge del 1984 fino ad arrivare alla Legge di ratifica della Convenzione di Budapest del 2008. Nel secondo capitolo si tratterà diffusamente dei principali reati informatici (*computer crimes*) compresi nella lista minima della Convenzione e che risultano all'atto pratico essere le tipologie di reati con i quali la Polizia Giudiziaria si trova a confrontarsi quotidianamente. Nel terzo capitolo si approfondirà uno dei reati più gravi e oggi di maggior impatto sociale al pari della lotta al terrorismo, ovvero il reato riguardante lo sfruttamento sessuale dei minori. Si analizzerà questo riprovevole fenomeno criminale partendo dalle prime normative in materia, fino alla ratifica della Convenzione di Lanzarote del 2012, confrontando la normativa italiana con altre normative straniere ed illustrando le varie attività di contrasto poste in essere dalla Polizia Giudiziaria, ed in particolare dalla Polizia Postale e delle Comunicazioni. Nel successivo quarto capitolo si approfondirà il tema della ricerca della prova informatica (*digital evidence*) a partire dalla ricerca della prova digitale così come prevista dall'attuale normativa novellata dalla ratifica della Convenzione di Budapest, con particolare riferimento

---

[6] "*Forensic Computing is the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable*", Rodney McKemmish (1999).

[7] James Borek, in un suo articolo (2001).

all'ispezione ed alla perquisizione informatica, la ricerca degli indirizzi IP e dei relativi *file* di *log*, confrontando anche in questo caso la normativa italiana con altre normative straniere ed in particolare quella statunitense. Nella seconda parte di questo capitolo verranno illustrate ed analizzate alcune delle principali attività investigative e di acquisizione della prova digitale con particolare riferimento al sequestro della corrispondenza ed alle intercettazioni telematiche.

Nel quinto capitolo si approfondiranno ulteriormente le tematiche inerenti l'informatica forense con particolare riferimento all'acquisizione, analisi e conservazione della prova digitale e della catena di custodia (*chain of custody*) nel rispetto della vigente normativa in materia novellata dalle citate Convenzioni e degli attuali standard operativi internazionali certificati nel recente Standard ISO/IEC 27037:2012 e nei recentissimi Standard ISO/IEC 27041:2015, ISO/IEC 27042:2015 e ISO/IEC 27043:2015. In un ambito investigativo mirato alla ricerca del dato digitale non si poteva non illustrare in un capitolo dedicato, il sesto capitolo, l'evoluzione storica e l'attuale formulazione della vigente normativa sulla *privacy* in Italia, con particolare attenzione all'attività investigativa. Illustrando infine le importanti novità previste dal Nuovo Regolamento *Privacy* che verranno introdotte a partire dal prossimo 25 maggio 2018 Dopo aver illustrato l'attuale panorama normativo riguardante le investigazioni informatiche e la ricerca ed analisi della prova digitale, nel settimo capitolo verrà illustrato il progetto *ForensicStorage* che vuole rappresentare una possibile soluzione alle criticità e difficoltà operative con le quali la Polizia Giudiziaria italiana deve confrontarsi quotidianamente. Un progetto che vuole suggerire un protocollo operativo cui possano uniformarsi gli inquirenti e le varie forze di polizia per standardizzare l'attività di sequestro, copia ed analisi dei supporti informatici individuati nel rispetto di quanto previsto dalla vigente normativa e dei più elevati standard qualitativi internazionali. Con notevole beneficio su numerosi aspetti: garanzie di sicurezza riguardo alla genuinità, inalterabilità e ripetibilità dell'acquisizione ed analisi delle prove digitali, maggiore rapidità e fruibilità nella loro messa a disposizione dell'Autorità Giudiziaria, notevole riduzione dei costi con inevitabile risparmio nelle spese di giustizia. Infine nell'ottavo capitolo verrà illustrato il progetto *ForensicWeb*, che rappresenta lo sviluppo di una importante applicazione *web* del progetto *ForensicStorage*, in questo capitolo se ne illustrerà un'implementazione pratica sperimentale a titolo dimostrativo.

CAPITOLO I

Informatica e Diritto Penale

1.1. I disegni di legge in materia di Informatica – 1.2. Il disegno di legge n. 1210 del 27 gennaio 1984 - Il disegno di legge n. 1602 del 2 ottobre 1987 – 1.4. Il disegno di legge n. 4367 del 21 novembre 1989 – 1.5. Il disegno di legge n. 5076 del 18 settembre 1990 – 1.6. Il disegno di legge n. 182 del 23 aprile 1992 – 1.7. Il disegno di legge n. 1526 del 1 settembre 1992 – 1.8. La Raccomandazione del Consiglio d'Europa del 9 settembre 1989 – 1.9. La Convenzione del Consiglio d'Europa sulla Criminalità Informatica - Budapest 23 novembre 2001 – 1.10. La Legge n. 48/2008.

1.1. *I disegni di legge in materia di informatica*.

Il Legislatore italiano inizialmente non ha trattato in modo organico la materia dei reati elettronici, ma se n'è occupato riguardo a temi informatici diversi, quali ad esempio, i sistemi informativi oppure la tutela dei programmi.

Solo dopo la Raccomandazione del Consiglio di Europa del 1989 ha messo mano ad un lavoro organico, diretto a regolare la materia informatica penale. Prima di commentare la legislazione emanata nel 1993 e inserita nel codice penale in modo interstiziale, si elencano di seguito i disegni di legge che si sono occupati nel tempo, in via incidentale o meno, di *computer crimes*.

1.2. *Il disegno di legge n. 1210 del 27 gennaio 1984*.

L'aspetto penale dell'informatica e della *privacy* è stato affrontato per la prima volta con il disegno di legge n. 1210, proposto da Seppia e altri legislatori in data 27 gennaio 1984, intitolato «Disciplina dell'uso dei sistemi informativi personali». La proposta prevedeva all'art. 10, una sanzione pecuniaria (da un minimo di 200.000 lire ad un massimo di due milioni di lire) e una pena detentiva (da sei mesi ad un anno) per chiunque avesse attuato, dolosamente o colposamente, una delle seguenti condotte criminose:

1. mantenere un sistema informativo senza darne notifica al Ministero dell'Interno;
2. fare circolare informazioni personali violando le norme elencate nella proposta di legge;
3. usare o comunque acquisire informazioni personali in violazione delle indicazioni contenute nella proposta di legge.

1.3. *Il disegno di legge n. 1602 del 2 ottobre 1987.*

Il disegno di legge numero 1602 fu proposto da Fumagalli Carulli e altri legislatori il 2 ottobre 1987. Il progetto proponeva l'inserimento di disposizioni in materia di "protezione dei programmi per elaboratore" nella Legge sul diritto d'autore. L'articolo 8 del disegno prevedeva delle sanzioni penali nei confronti dei c.d. "pirati del *software"*.

Le pene statuite erano graduate a seconda che la condotta fosse dolosa o colposa, oppure finalizzata ad un uso personale o commerciale delle copie illegali.

1.4. *Il disegno di legge n. 4367 del 21 novembre 1989.*

Il progetto di legge numero 4367, presentato dall'allora Ministro di Grazia e Giustizia Giuliano Vassalli il 21 novembre 1989, riguardava l'introduzione di disposizioni contro «l'abusiva duplicazione, riproduzione, importazione, distribuzione, vendita e locazione dei programmi per elaboratori elettronici e delle relative istruzioni».

Il disegno di legge, composto da un solo articolo suddiviso in due commi, proponeva l'ampliamento, sotto il profilo penale, del dettato normativo contenuto nell'art. 171 della Legge sul diritto d'autore. Si proponeva l'estensione del principio sanzionatorio, contenuto in tale Legge, ai programmi per elaboratori elettronici e alle relative istruzioni, nell'ipotesi in cui il fatto consistesse nella duplicazione abusiva e riproduzione a fini di lucro o nell'illecita importazione ai medesimi fini.

Erano puniti, con la reclusione da tre mesi a tre anni e con la multa da lire cinquecentomila a lire sei milioni, anche la distribuzione, la vendita e persino la locazione di supporti contenenti programmi per elaboratori elettronici, sprovvisti del contrassegno della Società Italiana degli Autori e degli Editori (SIAE); per i comportamenti di rilevante gravità il minimo della pena era elevato a sei mesi di reclusione, con l'aggiunta del pagamento di una sanzione pecuniaria di un milione di lire. Questo disegno di legge venne in seguito inserito nel D.Lgs. 29 dicembre 1992 n. 518 che ha modificato la Legge sul diritto d'autore introducendo un gran numero di nuove norme. Tra queste alcune, contenute nell'art. 171 *bis*, prevedono le stesse ipotesi di reato configurate nel disegno di legge in parola.

1.5. *Il disegno di legge n. 5076 del 18 settembre 1990.*

Alcune disposizioni contro i reati informatici e telematici erano previste nella proposta di legge numero 5076, presentata da Roberto Cicciomessere e altri.

Questo disegno di legge fu presentato al Parlamento subito dopo l'emanazione della Raccomandazione del Consiglio d'Europa del 1989. Seguendo l'esempio del Legislatore francese, che nel 1988 aveva inserito nel Terzo Libro del codice penale un nuovo Titolo «*De certains infractions en matière informatique*», si propose di inserire nel Capo III del Titolo XII del Codice Penale italiano una nuova Sezione dedicata ai «Delitti in materia informatica e telematica».

Per adeguare la legislazione italiana ai principi indicati nella Raccomandazione, la nuova sesta Sezione prevedeva l'introduzione nel codice penale dei seguenti reati informatici:

1. accesso abusivo e uso non autorizzato di un elaboratore di dati;
2. alterazione dell'integrità dei dati, dei programmi e della rete di trasmissione;
3. falsificazione dei documenti personali informatici.

L'ipotesi di reato e la relativa sanzione riguardo all'accesso abusivo e l'uso non autorizzato di un elaboratore fu prevista con l'inserimento di un nuovo articolo, il 623 *ter* c.p. Tale fattispecie poteva essere comparata al reato di violazione di domicilio. Attualmente le banche dati costituiscono sempre più un sistema complesso e interconnesso con altre banche dati, nel quale sono custoditi documenti che in passato erano registrati su supporti cartacei. Attraverso tale interconnessione si realizzano spesso delicate forme di comunicazione, come la messaggistica personale, la diffusione di notizie, la stipulazione di contratti, gli ordinativi bancari e commerciali. Il reato consisteva nell'accesso non autorizzato a una banca dati elettronica attraverso la forzatura delle difese informatiche. L'art. 623 *ter* primo comma del codice penale, il cui inserimento era previsto dalla proposta di legge in oggetto, conteneva anche una distinzione tra accesso totale e accesso parziale a una banca dati. Un archivio elettronico può presumere livelli differenti di accesso e, di conseguenza, anche diversi livelli di autorizzazioni.

Un soggetto potrebbe essere autorizzato ad accedere in alcune parti della banca dati ma non esserlo per altre.

Il reato di accesso non autorizzato era previsto anche nel caso di penetrazione incruenta attraverso lo sfruttamento di falle presenti nel sistema di protezione; tale condotta è stata assimilata a quella che integra il reato di violazione di domicilio.

Nella seconda figura di reato rientrano le ipotesi di danno, molto diverse tra loro, assimilabili a quelle previste dai reati di "falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche" o di "interferenze illecite nella vita privata" e anche a quelle previste dal furto e dal sabotaggio. L'alterazione dei dati o della rete di trasmissione può riguardare sia piccoli archivi personali, sia banche dati private o pubbliche di grande importanza. Non vi è solo la tutela della segretezza della corrispondenza, ma anche la necessità di impedire che si realizzino azioni di diffamazione che, per la grande velocità di propagazione propria del mezzo, possono provocare effetti devastanti. La terza previsione di reato si riferiva alla falsificazione dei documenti personali informatici, e cioè quei documenti digitali che consentono a un *computer* il riconoscimento della persona, come possono esserlo le carte di credito. Si vuole così tutelare la riservatezza e l'integrità dei dati gestiti da un *computer* e in particolare la *privacy* individuale contro ogni forma di intromissione e manipolazione da parte di terzi.

1.6. *Il disegno di legge n.182 del 23 aprile 1992*.

Nella proposta di legge Bassanini del 23 aprile 1992 n. 182 erano inserite "Norme per la tutela civile e penale del *software* e per l'esercizio dei diritti civili a esso collegati". L'art. 6 prevedeva l'istituzione di un sistema di sanzioni penali orientate a contrastare le condotte criminose dei c.d. "pirati del *software*" attuate con finalità di lucro, trattandosi nella maggior parte dei casi, di reati tipicamente economici. Erano ritenute più gravi le ipotesi della messa in commercio di un sistema *software* non destinato al suddetto uso o di quelle modifiche dalle quali derivava una potenziale lesione all'onore e alla reputazione del suo autore. Attraverso l'art. 8, invece, si voleva introdurre un sistema di pene accessorie mirate a colpire alla radice tale fenomeno criminale. A seguito della sentenza di condanna era, infatti, prevista la confisca e la distruzione del materiale contraffatto. L'ultimo articolo della proposta di legge, l'art. 9, proponeva di disciplinare una nuova fattispecie di reato, quella del «danneggiamento di *software*».

1.7. *Il disegno di legge n. 1526 dell'1 settembre 1992.*

Il disegno di legge n. 1526 del primo settembre 1992, presentato dall'allora Ministro di Grazia e Giustizia Claudio Martelli, riguardava la «Tutela delle persone rispetto all'elaborazione informatica di dati personali». Tale progetto prevedeva una rigorosa disciplina delle banche dati, al fine di adeguare la legislazione italiana alle direttive comunitarie che proponevano, l'inserimento di sanzioni penali per la tutela del bene giuridico della riservatezza dei dati personali.

Il suddetto orientamento, proposto dall'organismo sovranazionale, aveva il pregio di conciliarsi con il dettato normativo già presente nel nostro codice penale agli Artt. 615 *bis* - 620 che considerava i dati personali come «beni giuridici primari». Il progetto di legge, venne elaborato tenendo conto delle predette considerazioni e ipotizzando l'adeguamento della disciplina presente nel codice penale alle nuove esigenze di tutela legate alle condotte illecite di tipo informatico. Era previsto come reato la raccolta, l'elaborazione, la comunicazione e la diffusione illecita di dati nonché la mancata adozione di tutte le misure tecniche volte a garantirne la sicurezza.

1.8. *La Raccomandazione del Consiglio d'Europa* n. *R (89)-9 del 9 settembre 1989.*

L'Italia è stata una delle ultime nazioni, tra gli Stati membri dell'Unione Europea ad emanare una serie di disposizioni normative in materia di *computer crimes*. La Germania e la Francia avevano elaborato una legislazione penale riferita agli illeciti informatici, rispettivamente nel 1986 e nel 1988, mentre l'Inghilterra aveva provveduto in tal senso nel 1990, con l'approvazione del *Computer misuse act*, poco dopo l'emanazione della Raccomandazione del Consiglio d'Europa[8]. Con l'approvazione da parte del Parlamento della Legge n. 547/1993[9] il nostro paese si è finalmente adeguato ai principi generali proposti dall'organismo sovranazionale creando un «*corpus* normativo» dedicato al diritto

[8] R. BORRUSO, G. BUONOMO, G. CORASANITI, G. D'AIETTI, *Profili penali dell'informatica*, Giuffrè Editore, Milano, 1994, XII e ss.

[9] Il testo della Legge n. 547/1993 è stato elaborato durante un lasso di tempo molto lungo. Infatti, il disegno di legge ad esso corrispondente venne redatto, come citato in precedenza, da una Commissione nominata dal Ministro della Giustizia prof. Vassalli nel 1989. La Commissione ultimò i suoi lavori nel 1991, ma nel 1993 venne ripreso dal nuovo Ministro della Giustizia prof. Conso. Per ulteriori notizie sull'*iter* legislativo, si veda: C. SARZANA, *Informatica e diritto penale*, Giuffrè Editore, Milano, 1994, 196 e ss.; E. GIANNANTONIO, *Manuale di diritto dell'informatica*, Cedam, Padova, 1994.

penale dell'informatica. Il Legislatore italiano ha preferito scegliere la via dell'integrazione normativa del codice penale, cercando di ricondurre i nuovi reati alle figure già esistenti all'interno di tale codice[10]. Si è evitato così di creare una Sezione a parte dedicata ai crimini informatici, che avrebbe creato problemi di scelta per l'inserimento in un titolo piuttosto che in un altro, poiché i delitti in questione tendono a ledere beni giuridici di diversa natura, procedendo all'integrazione legislativa avendo però ben presente che i reati informatici oggetto di interesse potevano differenziarsi in due sottogruppi: quelli commessi *in danno* di un sistema informatico e quelli realizzati *per mezzo* di un sistema informatico.

La Raccomandazione prevede due liste di reati cui le singole nazioni possono uniformarsi: una lista *minima* e una *facoltativa*.

1.9. *La convenzione del Consiglio d'Europa sulla Criminalità Informatica - Budapest 23 novembre 2001*.

La Convenzione del Consiglio d'Europa sulla criminalità informatica[11], tenutasi a Budapest il 23 novembre del 2001, rappresenta il primo tentativo di giungere ad un accordo internazionale che consenta di realizzare una politica comune, tra gli Stati firmatari, nell'ambito della repressione dei crimini commessi mediante l'uso di tecnologie informatiche e telematiche.

Il testo della Convenzione, composto da 48 articoli, definisce quattro obiettivi principali[12]:

1. armonizzare le normative penali nazionali e le disposizioni comuni in tema di criminalità informatica, attraverso l'individuazione di nove fattispecie di reato[13];
2. aggiornare il diritto processuale penale affinché contenga gli elementi utili alla repressione delle condotte criminose attuate mediante l'uso di tecnologie informatiche e dei crimini al fine di acquisire le prove informatiche;

---

[10] Si veda R. BORRUSO, G. BUONOMO, G. CORASANITI, G. D'AIETTI, *Profili penali*, cit.

[11] La convenzione, finalizzata al contrasto del fenomeno della criminalità informatica, è stata elaborata da un comitato di esperti nominato nel 1996 dal Comitato Europeo per i Problemi Criminali. Il testo elaborato dal comitato viene firmato a Budapest il 23 novembre del 2001 da trenta Paesi, di cui 4 extraeuropei (Canada, Giappone, Stati Uniti e Sud Africa).

[12] Si veda D'AGOSTINI, *Diritto Penale dell'Informatica - dai computer crimes alla digital forensics*, Rimini, 2007, 239 e ss.; U. RAPETTO, D. MANCINI, *Novità legislative in materia di Crimine Informatico*, Roma, 2008, 10 e ss.

[13] Si rinvia agli articoli 2 *(Accesso illegale ad un sistema informatico)*, 3 *(Intercettazione abusiva)*, 4 *(Attentato all'integrità dei dati)*, 5 *(Attentato all'integrità di un sistema)*, 6 *(Abuso di apparecchiature)*, 7 *(Falsificazione informatica)*, 8 *(Frode informatica)*, 9 *(Reati relativi alla pornografia infantile)*, 10 *(Reati contro la proprietà intellettuale e diritti collegati)*.

3. favorire la cooperazione internazionale in materia di criminalità informatica;
4. stabilire una procedura comune per l'esecuzione di sequestri, perquisizioni, intercettazioni.

Per quel che riguarda l'armonizzazione delle normative interne, il testo, elaborato dal Consiglio d'Europa, identifica nove fattispecie di diritto penale sostanziale che vengono imposte agli Stati firmatari quale «lista minima» di reati informatici da inserire nel proprio ordinamento.

I temi principali affrontati dal testo della Convenzione sono:

1. la tutela del dato informatico;
2. l'abuso di apparecchiature informatiche finalizzato alla commissione di reati informatici;
3. la falsificazione di documenti informatici e la frode informatica;
4. la repressione della pornografia *online*;
5. la tutela della proprietà industriale e diritti collegati.

I restanti articoli della Convenzione, invece, rendono noti gli obiettivi fissati dal Consiglio d'Europa attraverso la previsione di avanzati strumenti che consentano un adeguato aggiornamento delle normative penali e processuali penali dei Paesi firmatari in modo da consentire alle stesse di «tenere il passo» all'evoluzione tecnologica in atto e ai reati informatici a essa connessi.

A tale fine il Consiglio d'Europa ha posto attenzione ad alcuni temi di particolare importanza, quale il delicato ambito concernente l'intercettazione, acquisizione e conservazione della prova informatica. Viene qua evidenziata la fragilità del dato informatico, dovuta alla sua intrinseca volatilità e modificabilità anche con riferimento all'ambiente all'interno del quale lo stesso viene registrato o trasmesso. La Convenzione prevede, pertanto, specifici strumenti a tutela del dato informatico, nella sua veste di prova digitale, strumenti che consentono la conservazione e cristallizzazione di informazioni al fine di evitare che le stesse vengano alterate o che vadano irrimediabilmente perdute.

Al fine di raggiungere lo scopo di preservare la prova digitale, il testo della Convenzione prevede specifichi obblighi in capo agli *Internet service provider*[14]

[14] L'*Internet Service Provider* è un fornitore di servizi quali l'accesso alla rete Internet e alla posta elettronica.

in materia di conservazione dei dati, relativi all'acceso e alla navigazione in Internet, utili alla rapida identificazione dell'autore di un illecito, prevedendo inoltre apposite procedure finalizzate al sequestro, acquisizione, anche in tempo reale, analisi e rimozione del dato da un sistema informatico[15].

L'art. 23 della Convenzione, espone, invece, i principi generali di cooperazione tra gli Stati firmatari e prevede che gli stessi devono attivarsi al fine di garantire il maggior livello di collaborazione possibile nelle "indagini o nei procedimenti riguardanti i reati collegati a sistemi e dati informatici, o per raccogliere le prove, in forma elettronica, di un reato", attraverso l'armonizzazione delle normative interne. Vengono, infine, previste apposite procedure con riferimento all'estradizione, alla mutua assistenza in indagini e procedimenti penali, alla trasmissione spontanea di informazioni tra Stati, alle procedure di richiesta di mutua assistenza in assenza di accordi internazionali, alle procedure di mutua assistenza provvisoria relativa a conservazione, accesso e intercettazione dei dati. Al tempo della firma della Convenzione, il Codice Penale Italiano conteneva solo le disposizioni in materia di criminalità informatica introdotte con la Legge n. 547/1993 ed ispirate ai principi generali proposti dalla Raccomandazione del Consiglio d'Europa del 1989. Il Legislatore, nonostante la firma della Convenzione e l'evidente e crescente necessità di aggiornare il codice penale tramite la previsione di nuovi reati informatici conseguenti all'inarrestabile processo di innovazione tecnologica, ha atteso ben sette anni prima di procedere alla sua ratifica che è avvenuta con la Legge n. 48 del 18 marzo 2008.

1.10. *La Legge n. 48/2008*.

Importanti modifiche al Codice Penale, al Codice di Procedura Penale, al D.Lgs. n. 231/2001 e al Codice in materia di protezione dei dati personali, sono state introdotte con la Legge n. 48/2008, che ha finalmente ratificato la Convenzione del Consiglio d'Europa. In particolare, il provvedimento introduce le seguenti novità:

1. sanzioni più dure per i reati informatici;
2. fondi per il contrasto della pedopornografia e per la protezione delle infrastrutture informatiche di interesse nazionale;

[15] Si rinvia agli articoli 16 *(Conservazione rapida di dati informatici immagazzinati),* 17 *(Conservazione e divulgazione rapide dei dati relativi al traffico),* 18 *(Ingiunzione di produrre),* 19 *(Perquisizione e sequestro di dati informatici immagazzinati).* 20 *(Raccolta in tempo reale dei dati sul traffico),* 21 *(Intercettazione di dati relativi al contenuto).*

3. responsabilità delle persone giuridiche;
4. nuovi strumenti di indagine per le forze dell'ordine;
5. maggiore tutela per i dati personali.

Intenzione del Legislatore era quella di dare piena e completa esecuzione alla Convenzione. Solo gli articoli 1 e 10 comma 2, che contengono rispettivamente la definizione tecnica di sistema informatico[16] e quella relativa ai reati contro la proprietà intellettuale e ai delitti commessi a livello commerciale mediante sistemi informatici[17], non sono stati presi in considerazione.

La volontà di non voler fornire una definizione «rigida» di sistema informatico è giustificata dall'intenzione del Legislatore di lasciare tale interpretazione alla giurisprudenza, rendendo, quindi, tale concetto sempre al passo con l'evoluzione tecnologica, che ha più volte dimostrato quanto possa essere ampio e mutevole il significato di sistema informatico. Per quanto riguarda l'art. 10, comma 2, relativo ai reati contro la proprietà intellettuale, il Legislatore ha reputato di non inserirlo nella Legge di ratifica poiché tale fattispecie è già presente, con portata molto più ampia[18], nell'art. 171, co. 1, lett. a-*bis*, della Legge sul diritto d'autore, rispetto a quella prevista dal testo della Convenzione.

Com'è stato già affermato, la Legge n. 48/2008, ispirandosi ai principi contenuti nella Convenzione di Budapest, opera, come detto, una serie di emendamenti ad alcuni articoli del Codice penale, a suo tempo introdotti con la Legge n. 547/1993, provvedendo ad inserirne di nuovi. Il Legislatore, in particolare, è intervenuto sui reati di falso e di frode informatica, formulando due

---

[16] L'art. 1 lett. a della Convenzione di Budapest identifica quale sistema informatico: "Qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati".

[17] L'art. 10, co. 2, della Convenzione di Budapest prevede che "Ogni parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale la violazione di diritti connessi come definiti dalla legge dello Stato Parte, tenendo fede agli obblighi che ha assunto in base alla Convenzione Internazionale per la protezione degli artisti, interpreti ed esecutori, produttori di fonogrammi ed organismi di radiodiffusione, all'Accordo sugli aspetti commerciali dei diritti sulla proprietà intellettuale e al Trattato OMPI sull'interpretazione ed esecuzione dei fonogrammi, con l'eccezione di tutti diritti morali conferiti da queste convenzioni, se tali atti sono commessi deliberatamente, su scala commerciale e attraverso l'uso di un sistema informatico".

[18] L'art. 171, comma 1, lett. a-*bis* della legge sul diritto d'autore prevede che "Salvo quanto previsto dall'art. 171 *bis* e dall'articolo 171 *ter*, è punito con la multa [...] chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma [...] a-*bis*) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa". La previsione normativa ha una portata più ampia di quella contenuta nel testo della Convenzione di Budapest, poiché punisce tutte le condotte rientranti nella distribuzione di opere protette attraverso reti telematiche di tipo "*peer to peer*" e non solo quelle che avvengono su "scala commerciale".

nuovi reati legati alla figura del certificatore di firma elettronica[19], realizzando un riordino dei reati concernenti il danneggiamento informatico, ed operando al contempo una suddivisione tra danneggiamento di informazioni, dati e programmi informatici e danneggiamento di sistemi informatici e telematici. Importanti modifiche, infine, sono state previste al codice di procedura penale, introducendo numerosi concetti mutuati dalle pratiche consolidate in tema di investigazioni informatiche e in linea con il testo della Convenzione di Budapest.

Tali aggiornamenti prevedono nuove garanzie processuali a tutela dei momenti chiave della catena di custodia della prova digitale poiché mirati a preservare l'integrità dei dati acquisiti in sede di perquisizione e sequestro da possibili alterazioni o modifiche. La necessità del Legislatore di procedere a una veloce applicazione delle nuove norme, data l'importanza e l'attualità dei temi affrontati, è evidenziata dall'art. 14 della Legge che prevede una riduzione del normale intervallo per la sua entrata in vigore che viene ridotto al giorno successivo a quello della sua pubblicazione in Gazzetta Ufficiale.

[19] Vengono aggiunti al codice penale due nuovi articoli: l'art. 495 *bis* c.p. "Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o altrui"; l'art. 640 *quinquies* c.p. "Frode informatica del soggetto che presta servizi di certificazione di fama elettronica".

CAPITOLO II

Computer Crimes

2.1. Reati informatici – 2.2. L'accesso abusivo – 2.3. Il *port scanning – 2.4.* Detenzione e diffusione abusiva di codici di accesso – 2.5. I virus informatici – 2.6. L'intercettazione abusiva della posta elettronica – 2.7. L'intercettazione abusiva delle comunicazioni telematiche – 2.8. *Keylogger* e *sniffer – 2.9.* Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche – 2.10. Il *Phishing – 2.11.* Il danneggiamento informatico – 2.12. La frode informatica – 2.13. La frode informatica nella certificazione di firma elettronica - 2.14. Gli altri reati previsti nella lista facoltativa della raccomandazione del Consiglio d'Europa del 1989.

2.1. *Reati informatici*.

La dottrina italiana per oltre un ventennio è stata impegnata ed appassionata dalla definizione di reato informatico, è ancora oggi molto difficile individuare una definizione univoca. Dottrina e giurisprudenza si dividono in opposte scuole di pensiero, tuttavia la definizione maggiormente condivisa sembra essere quella secondo cui il crimine informatico è rappresentato da qualsiasi atto o fatto contrario alle norme penali, nel quale un *computer* è stato coinvolto come soggetto, oggetto o strumento[20]. Tale tesi, richiede pertanto la necessaria presenza di un elaboratore; possiamo, tuttavia, spingerci anche oltre, affinché si possa parlare di reato informatico, la presenza di un elaboratore deve essere ritenuta condizione necessaria, ma non sufficiente: la semplice presenza di un *computer* non può essere per se sufficiente a configurare un reato informatico dovendo l'interprete valutare anche le modalità con cui il reato è stato attuato, al fine di scartare tutte quelle ipotesi in cui l'elemento informatico, se pure presente, è assolutamente accidentale e, pertanto, irrilevante[21]. Quindi non ogni reato commesso con un *computer* può essere ritenuto per ciò solo *"reato informatico"*, ma soltanto quelli in cui il *computer* rappresenta un elemento essenziale della fattispecie criminosa[22].

---

[20] M. BOZZETTI, P. POZZI, *L'Osservatorio FTI - Sicurforum Italia sulla Criminalità ICT (OCI),* in *Cyberwar o sicurezza? II Osservatorio Criminalità ICT,* a cura di M. BOZZETTI, P. POZZI, Franco Angeli, Milano, 2000.

[21] E' il caso di chi cagiona lesioni personali scagliando contro un altro soggetto un *mouse* o altra componente informatica. In detta inverosimile ipotesi, l'elemento informatico è strettamente casuale e, pertanto, non si può assolutamente parlare di reato informatico.

[22] G. POMANTE, *Internet e* criminalità, Giappichelli Editore, Torino, 1999, osserva che "la condotta sanzionata dall'ordinamento è, nella quasi totalità dei casi, un comportamento caratterizzato da un'elevata specializzazione dell'agente nel settore informatico o telematico". In tal senso si veda anche D. MINOTTI, *I reati commessi su internet, in Internet nuovi problemi e questioni controverse,* a cura di G. CASSANO, Giuffrè Editore, Milano, 2001.

E’ inoltre opportuno distinguere tra reati informatici propri e reati informatici impropri a seconda che il *computer* rappresenti un elemento basilare del reato, ovvero soltanto un semplice strumento utilizzato. Pertanto si possono definire "*reati informatici propri*" tutte quelle fattispecie che vedono nel *computer* l'oggetto o il soggetto del reato e che, di fatto, non potrebbero esistere in sua assenza, mentre con il termine "*reati informatici impropri*", si identificano tutti quei reati che possono essere commessi anche mediante l'utilizzo di un *computer*.

Nuove fattispecie di crimini commessi attraverso *internet* e, più in generale, attraverso la rete informatica, sono in continua e progressiva crescita. Fenomeni quali la pirateria informatica, la frode e la falsificazione informatica, o le violazioni della proprietà intellettuale e dei diritti connessi, e ancora lo scambio e il commercio di materiale pedopornografico in Rete, sono solo alcune delle molteplici condotte che il Legislatore, integrando e aggiornando la normativa, non lascia più impunite. Si tratta di tipologie di reati legati alla nostra società dell'informazione e alla sua sempre più significativa e globale informatizzazione.

Analogamente al crimine tradizionale, quello informatico copre una gamma molto vasta di condotte antigiuridiche, condotte che assumono differenti forme secondo le tecniche usate ed i fini cui tende l'autore del reato. In generale, sono detti reati informatici sia quelle attività illecite nelle quali il *computer* è il mezzo per la commissione del reato, sia quelle attività nelle quali, invece, il sistema informatico è l'obiettivo della condotta illecita. E’, infatti, possibile distinguere le numerose tipologie di crimini informatici in due fondamentali categorie, quella che usa dispositivi e programmi come mezzi per altri fini (estorcere, molestare, ecc.) e quella che considera proprio i *computer* ed i programmi i principali obiettivi (diffusione di *virus* e danneggiamenti informatici). Appartengono alla ricca serie di reati informatici tutte quelle attività quali le molestie, gli abusi in danno a minori, l'estorsione, il ricatto, la manipolazione dei mercati finanziari, lo spionaggio, il terrorismo, attività caratterizzate da una serie di eventi che prevedono ripetute interazioni con l'obiettivo scelto. Qualche volta, ad esempio, la vittima viene contattata in una *chat* da qualcuno che nel corso del tempo instaura, o tenta di instaurare, una qualche relazione, finalizzata a commettere un reato.

Alla sempre più ricca serie di reati informatici appartengono ancora quei reati quali il furto e la manipolazione di dati o servizi, le frodi bancarie, il furto di identità, le truffe negli annunci *online*, si tratta di reati e condotte criminose facilitate dall'impiego di programmi quali *keylogger, trojan horse*, *virus*, ecc.,

spesso i difetti e le vulnerabilità dei *software* offrono punti di appoggio all'aggressore per introdurre *crimeware* in questi casi la vittima inconsapevolmente scarica il programma o si collega ad un sito che sembra noto, ma che, in realtà, è un sito ostile.

Condotte e reati devono essere distinti a seconda che (a) siano concepibili solo ai danni di un *computer* o di una rete telematica, oppure che (b) siano indirizzati al mondo reale, ancorché realizzati attraverso la rete.

Partendo da questa prima grande divisione, i principali reati informatici previsti dal Legislatore sono: l'accesso abusivo a un sistema informatico o telematico[23]; la detenzione e la diffusione abusiva di codici di accesso a sistemi informatici o telematici[24]; la diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico[25]; l'intercettazione, l'impedimento o l'interruzione illecita di comunicazioni informatiche o telematiche[26]; l'installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche[27]; la falsificazione, l'alterazione o la soppressione di comunicazioni informatiche o telematiche[28]; inoltre il danneggiamento di informazioni, dati e programmi informatici[29]; la frode informatica e il furto dell'identità digitale[30]; l'ingiuria e la diffamazione attraverso *internet*[31]; la pornografia minorile, produzione e divulgazione *online*[32]; la pornografia minorile, detenzione di materiale pedopornografico[33]. Dietro queste espressioni che indicano i principali reati informatici, si nascondono alcune volte nuove tecniche e antichi obiettivi, altre volte, invece, nuove tecniche e nuovi obiettivi. L'elenco è ampio e, come detto, in continua crescita. Qui di seguito, a titolo di esempio vengono riportate alcune tipologie di condotte illecite che mettono a repentaglio diritti e sicurezza di individui, gruppi e nazioni, e che soventemente costituiscono un reato informatico. *Cyberlaundering:* si tratta del fenomeno criminale del riciclaggio che

[23] Art. 615 *ter* c.p.;
[24] Art. 615 *quater* c.p.;
[25] Art. 615 *quinquies* c.p.;
[26] Art. 617 *quater* c.p.;
[27] Art. 617 *quinquies* c.p.;
[28] Art. 617 *sexies* c.p.;
[29] Art. 635 *bis* c.p.;
[30] Art. 640 *ter* c.p.;
[31] Art. 595 c.p.;
[32] Art. 600 *ter* c.p.;
[33] Art. 600 *quater* c.p.;

si manifesta in molteplici forme; la più classica è quella che prevede il trasferimento di denaro proveniente da attività illecita in conti resi disponibili e, da qui, la bonifica stessa delle somme. Una volta ottenuta la disponibilità delle somme, infatti, si possono predisporre, ad esempio, pagamenti a fronte di transazioni apparentemente lecite (ad esempio vendite fittizie di immobili). Dette tecniche di riciclaggio nell'era digitale sono quanto mai varie.

A queste, si aggiunga il più grande mercato nero digitale del mondo, *Silk Road 3.0,* una piattaforma di *e-commerce* non indicizzata dai comuni motori di ricerca, presente nel c.d. *deep web*, e accessibile esclusivamente attraverso Rete *Tor (software* gratuito che consente la navigazione del *web* in assoluto anonimato), ove è possibile non soltanto l'acquisto di droghe, di armi, *kit* per la costruzione di bombe, ecc., ma anche il riciclaggio dei proventi delle attività illecite. Su questa piattaforma, le transazioni non avvengono in valuta comune, bensì in *BitCoin*[34], una moneta elettronica, che consente di garantire l'anonimato nell'operazione di compravendita *online.* Non è un caso che Ross Ulbricht - fondatore di *Silk Road* - debba rispondere di ben sette capi d'imputazione tra cui figura la pirateria informatica e il riciclaggio di denaro. La cornice legislativa nazionale antiriciclaggio è oggi rappresentata dal D.Lgs. 21 novembre 2007, n. 231 e dalle relative disposizioni di attuazione emanate dal Ministro dell'economia e delle finanze. Più la tecnologia va avanti, più sono le persone e i gruppi che la utilizzano secondo le loro inclinazioni e decisioni. Si alternano senza interruzione i rimedi e i rischi, la sicurezza e l'insicurezza informatica si danno continuamente il cambio. Sempre più, comportamenti di segno diverso si sovrappongono e si contendono la scena. Qualche volta è lo spirito creativo, la curiosità sovversiva, il gusto per il gioco senza alcun altro fine - in altri termini l'attività tipica *dell'hacker* - che caratterizza la condotta. Qualche altra volta, la grande capacità tecnica non si accompagna e non è mossa dalla curiosità e dal divertimento fini a se stessi, ma, al contrario, abusa delle proprie capacità e il comportamento, tipico del *cracker,* è

---

[34] *BitCoin*, simbolo: ฿; codice: **BTC** o **XBT,** moneta elettronica creata nel 2009 dal sedicente Satoshi Nakamoto, implementando un'idea dello stesso autore presentata su Internet a fine 2008. A differenza della maggior parte delle valute tradizionali, *BitCoin* non fa uso di un ente centrale: esso utilizza un *database* distribuito tra i nodi della rete che tengono traccia delle transazioni, e sfrutta la crittografia per gestire gli aspetti funzionali come la generazione di nuova moneta e l'attribuzione di proprietà della stessa valuta. La rete *Bitcoin* consente il possesso e il trasferimento anonimo delle monete; i dati necessari a utilizzare i propri *Bitcoin* possono essere salvati su uno o più *personal computer* sotto forma di "portafoglio" digitale, o mantenuti presso terze parti che svolgono funzioni simili a una banca. In ogni caso, i *Bitcoin* possono essere trasferiti attraverso la Rete verso chiunque disponga di un "indirizzo *Bitcoin*". Si tratta di una delle prime implementazioni di un nuovo concetto definito *criptovaluta*, descritto per la prima volta nel 1998 da Wei Dai. (Fonte Wikipedia).

doloso e dannoso. Anche da questo si evince la confusione tra *hacker* e *cracker* che il linguaggio comune, di solito, propone tramite la stessa analogia *hacker*-malvivente. La prima normativa penalistica avente ad oggetto l'informatica risale a circa venti anni fa, e si tratta del *Counterfeit Access Device* and *Computer Fraud and Abuse*, emanato negli Stati Uniti d'America nel 1984, normativa in seguito integrata e sostituita dal *Computer Fraud and Abuse Act*, pubblicato il 6 ottobre 1986. La necessità di recuperare il tempo perduto rispetto agli Stati Uniti, ma anche rispetto ad altri Paesi europei che si erano già dotati di una legislazione penale sull'informatica, nonché quella di predisporre una necessaria difesa contro il dilagante fenomeno della criminalità informatica seguendo, da un lato, le indicazioni fornite dal Consiglio d'Europa e dall'altro, sfruttando l'esperienza legislativa maturata in altri Paesi, portarono a nominare nel gennaio 1989 una Commissione composta da magistrati, accademici ed esperti informatici, affidando ad essa l'incarico di elaborare uno schema di modifica delle disposizioni del codice penale. La Legge del 23 dicembre 1993, n. 547 «Modificazioni ed integrazioni delle norme del codice penale e del codice di procedura penale in tema di criminalità informatica» è stata la conseguenza dei lavori prodotti dalla Commissione. Il Legislatore, nell'intervenire, ha dovuto scegliere se creare delle nuove fattispecie incriminatrici, o se modificare, riadattandole, le figure di reato preesistenti che fossero in qualche modo riconducibili ai crimini informatici.

Questa norma ha seguito entrambe le direzioni: sia introducendo nuove fattispecie di reato, sia integrando disposizioni previgenti, ha quindi provveduto ad integrare il codice penale, inserendo nuovi articoli quali il 615 *ter* c.p. ed il 615 *quater* c.p. relativi all'accesso abusivo ad un sistema informatico o telematico, il 615 *quinquies* c.p. relativo ai cosiddetti *virus*, il 640 *ter* c.p. in materia di frode informatica. La norma in oggetto ha inoltre esteso la portata degli articoli già esistenti, quali, ad esempio, l'art. 392 del codice penale relativo alla violenza sulle cose o l'articolo 420 c.p. in materia di attentati ad impianti di pubblica utilità. Sebbene la Legge n. 547/1993 non sia l'unica a prevedere ipotesi di delitto connesse alle nuove tecnologie, infatti, altri interventi legislativi (quali, ad esempio, il D.Lgs. n. 518/92 in materia di tutela dei programmi per elaboratore o la stessa Legge n. 675/96, abrogata dal D.Lgs. n. 196/03 in materia di protezione dei dati personali), hanno permesso di identificare ulteriori ipotesi di illecito commesso mediante strumenti informatici e telematici, essa resta ancora il principio del nostro ordinamento.

2.2. *L'Accesso abusivo*.

L'accesso abusivo costituisce uno dei reati informatici più diffusi, dal momento che l'accesso abusivo a un sistema informatico rappresenta una delle sfide più avvincenti e interessanti per qualsiasi esperto di sicurezza; spesso poi, l'autore del fatto non ne avverte la portata antigiuridica, ma anzi lo vive come una verifica delle proprie capacità[35]. Il Legislatore, tuttavia, riconosciuto che il domicilio informatico descrive lo spazio in cui l'individuo trasferisce ed esercita alcune delle sue facoltà intellettuali, lo ha pertanto ritenuto meritevole di una tutela, quantomeno, pari a quella attribuita al domicilio fisico garantendogli una tutela piena ed esclusiva ed espandendo in tal modo l'area di rispetto garantita all'individuo dall'articolo 14 della Costituzione e dagli articoli 614 e 615 del codice penale[36]. Ai sensi dell'art. 615 *ter* c.p., "*chiunque si introduce in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo è punito con la reclusione sino a tre anni*", la norma pertanto prende in considerazione due condotte: la prima rappresentata dall'acceso abusivo, la seconda dall'illecito mantenimento. La norma prevede correttamente questa distinzione, poiché esiste la concreta possibilità che un soggetto acceda legittimamente all'interno di un sistema, avendo ricevuto esplicita autorizzazione da parte del titolare, ma decida in seguito di trattenersi in maniera abusiva oltre il limite temporale stabilito dal titolare oppure utilizzando l'accesso al sistema per finalità o scopi diversi da quelli autorizzati. Il reato in oggetto è considerato da una parte della dottrina come *plurioffensivo*, ovvero che la condotta illecita prevista aggredisca contemporaneamente diversi beni giuridici. In effetti, un accesso abusivo espone il titolare del sistema, o dei dati ivi contenuti, a numerosi pericoli, una volta entrato nel sistema il reo potrebbe compiere un'illimitata serie

[35] A tal proposito si veda Trib. Minori di Bologna, 7 maggio 2008, n. 659*:* "È noto come l'imputabilità del minore presupponga l'accertamento della capacità di intendere e di volere di costui, la quale si sostanzia nella c.d. 'maturità mentale', concetto, questo, a carattere relativo, poiché correlato alle caratteristiche del reato commesso, ed implicante in special modo la capacità del soggetto di percepire il disvalore etico sociale delle proprie azioni. Tale essendo la premessa è gioco forza concludere che l'indagine sull'imputabilità del minore debba essere condotta con particolare cautela rispetto a reati, come quelli informatici, in cui il comportamento incriminato può essere interpretato più come il sintomo di spiccate e non comuni capacità intellettive dell'agente piuttosto che quale manifestazione di un atteggiamento deviante di costui".

[36] Cfr. Ministero di Grazia e Giustizia, *Schema di disegno di legge contenente le modifiche ed integrazioni alle norme del codice penale e del codice di procedura penale, in tema di criminalità informatica*.

di condotte illecite, carpire informazioni riservate o dati sensibili, appropriarsi di codici di accesso, cancellare o trasferire i dati ivi presenti, danneggiare i *file* o i programmi presenti, impedire il corretto funzionamento del sistema, ecc.

L'inviolabilità del domicilio informatico, inteso come spazio di esclusiva pertinenza di una data persona fisica o giuridica, costituisce il bene giuridico tutelato dalla norma in esame. Questo poiché per la configurabilità del reato non è necessario che il reo prenda concretamente visione dei dati o delle informazioni riservate, se la norma in questione avesse avuto il fine di tutelare la riservatezza, allora il soggetto passivo avrebbe dovuto coincidere con il titolare dei dati contenuti all'interno del sistema. Invece l'art. 615 *ter* c.p. non opera alcun riferimento al titolare dei dati o delle informazioni contenute nel sistema informatico. Infatti, il reato di accesso abusivo a un sistema informatico si verrebbe a configurare anche nel caso in cui il sistema dovesse essere privo di dati sensibili, oppure del tutto sprovvisto di dati e informazioni, analogamente a quanto accade nel reato di violazione di domicilio, che si configura anche nel caso in cui l'agente acceda abusivamente in un'abitazione completamente vuota[37].

Pertanto, l'accesso abusivo a un sistema informatico o telematico non è stato punito dal Legislatore penale perché, attraverso di esso, vengono posti in pericolo numerosi e differenti beni giuridici, ma perché la condotta descritta aggredisce concretamente l'inviolabilità del domicilio, bene giuridico di maggiore importanza[38]. Nell'analisi di questa norma assume fondamentale importanza la nozione di "misure di sicurezza", infatti, la norma stessa subordina la rilevanza penale dell'accesso abusivo alla violazione di dette misure, viene quindi previsto e punito non il semplice accesso non autorizzato, ma l'accesso abusivo effettuato violando le misure difensive attuate dal titolare del sistema. In mancanza di tali misure difensive, anche minime, il titolare non potrà chiedere che l'intruso venga punito ai sensi dell'art. 615 *ter* c.p..

Solo in alcuni e specifici casi la legge obbliga il titolare di un sistema informatico o telematico di predisporre opportune misure di sicurezza[39].

---

[37] G. D'AIUTO, L. LEVITA, *I reati informatici. Disciplina sostanziale e questioni processuali,* Giuffrè Editore, Milano, 2012, Quando si afferma che "l'introduzione penalmente rilevante si concretizza mediante la lettura dei dati contenuti nel sistema, eventualmente mediante le copiature dei medesimi", bisogna avere cura di specificare che la lettura o la copiatura dei dati sono condotte che *normalmente* conseguono ad un accesso abusivo, ma non rappresentano in alcun modo elementi costituivi del reato.

[38] Nella Raccomandazione numero 9 del 1989 con cui il Consiglio di Europa invitava il nostro Paese ad incriminare la mera condotta di accesso abusivo ad un sistema informatico.

[39] Si veda, al riguardo, il *Codice in materia di protezione dei dati personali,* Artt. 33-36.

Il Legislatore da un lato ha ritenuto giusto non definire tecnicamente il concetto di "misure di sicurezza", lasciando libero l'utente di approntare i mezzi che ritenga adatti a tutelare il proprio domicilio informatico, consentendo in questo modo anche di adeguare dette tutele all'evoluzione tecnologica; dall'altro lato giurisprudenza e dottrina ritengono che la dicitura "misure di sicurezza" non debba essere intesa in maniera letterale, poiché il reato si perfeziona, anche in caso di violazione di un'unica misura di sicurezza, non rilevando né il numero, né tantomeno l'adeguatezza o la complessità delle misure di sicurezza adottate.

Ciò che rileva è che il titolare abbia dotato il sistema almeno di una misura di sicurezza e che la stessa rappresenti una barriera percepibile dall'esterno, rilevando in questa sede più il valore simbolico dello *ius excludendi*, che non l'effettiva efficacia delle misure di protezione adottate, poiché attraverso essa il titolare palesa la volontà di proteggere il proprio domicilio informatico.

Le misure di sicurezza possono essere divise in due categorie: misure di sicurezza digitali e non digitali. Le prime possono essere ulteriormente distinte come *misure di sicurezza software*, quali ad esempio un *firewall*[40] o una *password* di accesso, e *misure di sicurezza hardware*, ad esempio un *badge* per la firma digitale o un *token* generatore di codici utilizzabili come *one time password*. Le seconde possono essere utilizzate per proteggere il sistema informatico o telematico nella sua estrinseca materialità, ad esempio, una porta blindata, una cassaforte. Per quanto attiene alla seconda modalità commissiva, rappresentata dall'illecito *mantenimento*, è fondamentale considerare che il reato non sussiste nel caso in cui il titolare presti il proprio consenso. Non tanto perché al titolare di un diritto viene genericamente riconosciuta la potestà di rinunciarvi, quanto perché l'assenza di un consenso - espresso o tacito - è esplicitamente prevista dalla norma e rappresenta, quindi, un *elemento costitutivo della fattispecie.* Il consenso del titolare non opera dunque come una mera causa di esclusione della punibilità, ma impedisce *tout court* che si perfezioni il reato.

Di particolare interesse è la decisione del maggio 2008[41]; il procedimento vedeva accusato un cancelliere cui era stato contestato il reato di cui all'art. 615

[40] In informatica, nell'ambito delle reti di *computer*, un *firewall* (termine inglese dal significato originario di *parete refrattaria*, *muro tagliafuoco*, *muro ignifugo*; in italiano anche *parafuoco* o *parafiamma*) è un componente passivo di difesa perimetrale di una rete informatica, che può anche svolgere funzioni di collegamento tra due o più tronconi di rete, garantendo dunque una protezione in termini di sicurezza informatica della rete stessa. (Fonte Wikipedia).

[41] Cass. Pen., Sez. V, Sent. 26797 del 29 maggio 2008. Per un commento si veda R. FLOR, *Permanenza non autorizzata in un sistema informatico o telematico, violazione del segreto d'ufficio e concorso nel reato da parte* dell'*extraneus*, in Cass. Pen, 2009, 5, 1509.

ter c.p., in concorso con quello di rivelazione di segreti d'ufficio, perché, tramite il sistema informatico dell'ufficio, egli aveva potuto conoscere notizie riservate relative a un fascicolo processuale penale, rivelandole poi indebitamente a un avvocato. La Corte rigettava il ricorso avverso la condanna per il reato di rivelazione di segreti d'ufficio, ma lo annullava limitatamente al reato di accesso abusivo, sulla base della valutazione che l'operatore giudiziario era, in effetti, autorizzato ad accedere senza limiti al registro informatico dell'ufficio, per tale ragione non poteva ritenersi fosse stato compiuto un accesso abusivo. A ciò doveva aggiungersi che, non soltanto non vi era alcuna norma o disposizione interna organizzativa che impediva al cancelliere addetto alla singola sezione di consultare i dati del registro generale e le assegnazioni ai diversi uffici, ma anche qualora vi fosse stata tale proibizione sarebbe stata da considerarsi contraria a ogni buona regola organizzativa, attese le necessità di consultazione di un ufficio giudiziario[42].

Per ciò che concerne l'utilizzo illecito dei dati così acquisiti i Giudici hanno ritenuto che siffatta violazione non attiene alle norme che regolano l'accesso al sistema e la consultazione dei dati in esso registrati, poiché l'uso successivo, che di tali dati s'è fatto e l'infedeltà dell'agente ammesso in via privilegiata al sistema, veniva ad essere assorbito nella condotta di rivelazione di notizie d'ufficio che erano, invece, destinate a rimanere segrete.

Nella sua forma semplice, il reato è perseguibile a querela di parte, mentre, nella forma aggravata è perseguibile anche d'ufficio; inoltre, nel caso in cui occorra una circostanza aggravante, la pena massima aumenta da tre a cinque anni di reclusione.

Le aggravanti previste dal Legislatore riguardano le modalità della condotta, il reato è aggravato se il soggetto è palesemente armato, ovvero agisce con violenza su persone o cose; relativamente alla natura del sistema informatico o telematico, il reato è aggravato nel caso in cui la condotta riguardi sistemi informatici "di interesse militare, o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico"; le conseguenze della condotta, nel caso in cui dal fatto derivi la distruzione o il

[42] Si veda in tal senso, Cass. Pen., Sez. V, 25 giugno 2009, n. 40078 che, nel rigettare il ricorso proposto dal P.M., osservava "[...] secondo un condivisibile orientamento giurisprudenziale, la qualificazione di abusività va intesa in senso oggettivo, con riferimento al momento dell'accesso e alle modalità utilizzate dall'autore per neutralizzare e superare le misure di sicurezza, apprestate dal titolare dello *Ius excludendi*, al fine di impedire accessi indiscriminati. Non hanno quindi rilevanza la finalità che si propone l'autore e l'uso successivo dei dati che, se illeciti, integrano eventualmente un diverso titolo di reato... ".

danneggiamento del sistema; l'interruzione anche parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi ad esso pertinenti o in esso contenuti, e lo *status personale* del reo, ovvero, nel caso in cui il reato sia stato commesso da pubblico ufficiale o incaricato di pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla propria funzione; da chi esercita, anche abusivamente, la professione di investigatore privato o con abuso della qualità di operatore di sistema.

2.3. *Il port scanning*.

Riguardo al c.d. *port scanning*[43], è acceso il dibattito se si possa configurare un tentativo riguardo al reato di cui all'art. 615 *ter*; si tratta di una tecnica piuttosto diffusa che consiste nell'utilizzare idonei programmi in grado di verificare se un determinato sistema informatico abbia alcuni servizi attivi, eseguendo per l'appunto uno *scanning* o scansione delle porte TCP e UDP attive.

Lo *scanning* di per sé non può essere ritenuto un accesso abusivo al sistema informatico, poiché la configurabilità di detto reato si perfeziona solo quando l'accesso al sistema sia effettivamente avvenuto. E' tuttavia pacifico che lo *scanning* possa essere ritenuto un'attività preparatoria all'accesso vero e proprio, essendo la tecnica principale utilizzata per raccogliere informazioni ed eventuali vulnerabilità sul sistema informatico interessato. E' quindi necessario stabilire se lo *scanning* di un sistema sia un atto diretto in modo non equivoco alla violazione dello stesso sistema, e quindi punibile, oppure, costituisca un'attività a se stante e pertanto non punibile[44]. E' tuttavia evidente che non sia sufficiente eseguire un *port scanning* per accedere a un sistema informatico; anche qualora s'individuasse una vulnerabilità, occorrerà pertanto contestualizzare l'azione svolta, valutando la

[43] E' possibile definire il *port scanning* come quel processo di connessione a porte TCP e UDP appartenenti ad un sistema al fine di determinare quali servizi siano in esecuzione. In tal senso Trib. Roma, Ordinanza 1 agosto 2001, Iacorelli *vs* Infostrada SpA in cui il Tribunale ha definito tale pratica come "una serie programmata di tentativi di accesso diretti ad evidenziare, in base alle risposte fornite dallo stesso sistema attaccato, le caratteristiche tecniche del medesimo al fine di acquisire gli elementi per una successiva intrusione o conoscere le caratteristiche dell'altrui sistema o *server*, adibito a determinati servizi in rete". In alternativa al *port scanning* è possibile effettuare un *net scanning*. Quest'ultimo prende di mira un'intera rete, o una sua porzione, per verificare quali e quanti *computer* abbiano una determinata porta (o alcune determinate porte) in ascolto.

[44] Cass. Pen., Sez. II, n. 2791 del 16 marzo 1992 "anche un atto preparatorio può integrare gli estremi del tentativo, quando sia idoneo e diretto in modo non equivoco alla consumazione di un reato, cioè quando abbia la capacità, valutabile *ex ante*, di raggiungere il risultato prefisso, in relazione alle circostanze del caso, e sia inoltre univocamente diretto alla consumazione del reato"; Cass. Pen., Sez. II, n. 3692 del 20 aprile 1985 "un atto meramente preparatorio può costituire materia di tentativo punibile, sempre che l'atto stesso risulti idoneo e diretto in modo non equivoco alla commissione di un delitto".

condotta dell'agente. Ad esempio sarà evidente l'intenzione qualora lo *scanning* avvenga su una *subnet* alla ricerca di *computer* infetti, volta a individuare sistemi compromessi allo scopo di utilizzare l'indirizzo IP ad essi associati al fine di nascondere la propria identità. Ancora un *port scanning* mirato alla ricerca di una o più porte generalmente utilizzate da programmi malevoli tipo *Trojan Horse* potrà essere, analogamente all'ipotesi precedente, ritenuto un atto idoneo diretto in maniera non equivoca alla violazione del sistema informatico, potrà quindi ravvisarsi l'ipotesi di tentativo. Il reato in oggetto inizia a perfezionarsi nel momento in cui l'agente inizia a saggiare le difese del sistema oppure si pone alla ricerca di specifiche e mirate vulnerabilità, l'art. 56 c.p. mira quindi a tracciare il confine tra atti leciti e illeciti, identificando il momento nel quale l'attività illecita ha inizio.

2.4. *Detenzione e diffusione abusiva di codici di accesso*.

La norma in esame, prevista e punita dall'art. 615 *quater*, sanziona la condotta di "*chiunque al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a un anno e con la multa sino a cinquemilacentosessantaquattro euro*".

Questa norma si pone in maniera complementare rispetto all'art. 615 *ter*, anticipando la condotta sanzionabile. Infatti, non sanziona unicamente le condotte relative al traffico di codici e *password*, ma anche la condotta dell'agente che fornisca istruzioni o indicazioni utili a realizzare un accesso abusivo ad un sistema informatico. L'abusività del comportamento unita al dolo specifico dell'agente è la caratteristica imprescindibile di questa tipologia di delitto, individuabile nella coscienza e volontà di portare a termine il reato per trarne un profitto, non necessariamente illecito, o causare un danno, non necessariamente ingiusto.

La stessa Convenzione di Budapest, all'articolo 6, prevede una importante eccezione, laddove stabilisce espressamente che la condotta di detenzione abusiva di codici e mezzi idonei all'accesso ad un sistema informatico non dovrebbe essere punita nel caso in cui non sia finalizzata alla commissione di un reato, come potrebbe realizzarsi nell'ipotesi di test autorizzati e finalizzati al miglioramento della sicurezza del sistema informatico. Altresì non si può ritenere

illegittima la condotta del soggetto avente diritto, o autorizzato dal titolare, che consegni ad un terzo (magari un tecnico informatico addetto alla manutenzione) la *password* di accesso al sistema, mentre dovrà ritenersi in ogni caso illecita la comunicazione della stessa *password* effettuata da un soggetto ad un terzo con l'intento di arrecare un danno o di procurarsi un vantaggio. Non è necessario in questo caso che il profitto sia illecito e/o quantificabile di una valutazione economica, potendosi configurare come "profitto" anche il soddisfacimento di un bisogno materiale o psicologico. In tal modo sarà quindi configurabile il reato *de quo* nel caso in cui un dipendente, senza alcun vantaggio, anche solo per vendetta o rivalsa, comunichi ad altri i codici per accedere all'infrastruttura informatica dell'azienda ove presta servizio, oppure nel caso in cui un fidanzato geloso per vendetta pubblichi *online* o consegni ad un terzo i codici di accesso al *computer* o all'*email* della fidanzata.

Inoltre la normativa in questione non appare per niente chiara nella seconda parte. Un'interpretazione letterale della stessa potrebbe far pensare il termine "abusivamente" sia riferito alle sole condotte di procurarsi, riprodurre, diffondere, comunicare o consegnare i codici o gli altri mezzi idonei all'accesso ad un sistema informatico e non anche a colui che fornisca indicazioni o istruzioni idonee al medesimo scopo. In pratica, sembrerebbe trattarsi di due differenti ipotesi criminose di cui solo la prima richiederebbe l'abusività della condotta, ma è di tutta evidenza che una tale interpretazione causerebbe non poche difficoltà nello studio delle problematiche legate alla sicurezza informatica, fino ad arrivare all'impossibilità di analizzare e discutere ogni problematica legata alla sicurezza di un sistema ed ogni tecnica di *password recovering.* Ad esempio, come si dovrebbe procedere se un soggetto pubblicasse in un gruppo di discussione dedicato alla sicurezza, oppure in un sito *web*, una *"full disclosure"*[45] per una nuova vulnerabilità? È certo che questa persona procurerebbe a sé un profitto (individuabile nella fama e nel rispetto acquisito agli occhi degli altri componenti

[45] In ambito di sicurezza informatica con il termine *"full disclosure"* si indica un rapporto di sicurezza in cui vengono rivelati *(to disclose)* tutti i dettagli di una qualsiasi falla nella sicurezza di un sistema. Spesso insieme alla *full disclosure* vengono indicate anche le modalità con cui sarebbe possibile, per un terzo ostile, sfruttare tale vulnerabilità a proprio vantaggio. Perché possa parlarsi di *"full disclosure"* è necessario che tutti i dettagli della vulnerabilità siano discussi in pubblico incluse le istruzioni su come individuarla e come sfruttarla. Ciò avviene in quanto vi è la convinzione che ciò possa contribuire ad un più rapido intervento di eliminazione della vulnerabilità stessa, ma non vi sono dubbi che, nel tempo che passa tra la comunicazione della falla e la scoperta della soluzione, vi sia una pericolosa finestra in cui il sistema è esposto ad attacchi. In estrema sintesi la *full disclosure* si pone agli antipodi del concetto di sicurezza attraverso la segretezza *(security through obscurity)* ritenendo che soltanto la piena conoscenza di rischi e vulnerabilità di un sistema possa portare alla sua messa in sicurezza.

del gruppo) e, pur essendo in buona fede e non istigando nessuno ad abusare delle informazioni della *"full disclosure"*, esporrebbe, comunque, altri soggetti ad uno *"zero-day attack"*[46]. Analizzando con attenzione la fattispecie in esame, non si può non osservare come comportamento di un soggetto che ponga in essere una simile condotta, sia indubbiamente estremamente pericoloso dato che esporrebbe centinaia di migliaia di sistemi al rischio di uno *zero-day attack*, contro il quale non esiterebbero difese. D'altra parte, lo sviluppo della sicurezza informatica è fortemente collegato alla libertà dell'informazione ed alla condivisione delle conoscenze, quindi non sarebbe neppure immaginabile la possibilità di tenere a lungo segreta una vulnerabilità scoperta in un sistema. In questi casi la soluzione, logica prima ancora che giuridica, è da individuarsi nella cosiddetta *"Responsible disclosure"*[47], che consentirebbe ai produttori di *hardware* e *software* di predisporre gli opportuni strumenti necessari ad evitare uno *zero-day attack*.

2.5. *I virus informatici*.

Con l'espressione "*virus* informatico" si fa comunemente riferimento ad un *software* in grado di danneggiare un sistema informatico, o comunque di alterarne il corretto e regolare funzionamento. Per tale motivo, i *virus* informatici, rientrano a pieno titolo nella categoria dei c.d. *malware*[48], tuttavia a differenza di altri *software* dannosi, i *virus* sono in grado di riprodursi e diffondersi autonomamente. In pratica tutti i *malware* impediscono ad un sistema informatico di funzionare correttamente, ma solo i *virus* possiedono la peculiare capacità di introdursi in altri *computer*, infettando o quantomeno tentando di infettare tutti i *computer* con i quali vengono a contatto come se fossero *virus* biologici.

L'art. 615 *quinques* c.p. prevede un reato informatico proprio, tale articolo vieta e sanziona la diffusione di programmi o apparecchiature dirette a danneggiare un sistema informatico o i dati in esso contenuti. Si tratta, nelle

---

[46] Con il termine *"zero-day" attack* si vuole indicare una minaccia *(threat)* informatica diretta a sfruttare una vulnerabilità ancora sconosciuta o appena scoperta. L'obiettivo è quello di portare l'attacco prima che il produttore del *software* affetto da tale falla possa rimediare pubblicando *patch* o aggiornamenti. Si parla di *"zero-day protection"* quando un produttore di *software* è in grado di rimediare alla vulnerabilità non appena questa viene scoperta.

[47] Con questo termine si indica un rapporto di sicurezza in cui vengono rivelati tutti i dettagli di una qualsiasi falla nella sicurezza di un sistema. A differenza della *full disclosure*, però, viene stabilito un periodo di tempo tra la scoperta e la divulgazione della notizia per dare il tempo al produttore di sviluppare le opportune contromisure; a seconda della vulnerabilità questo periodo di tempo può andare da poche settimane a qualche mese.

[48] Questo neologismo deriva dalla crasi delle parole *malicious* e *software*, che potrebbe essere tradotto in italiano con "programma malvagio".

intenzioni del Legislatore, di un articolo destinato a punire la diffusione dei *virus informatici*, che come detto sono destinati principalmente a danneggiare il funzionamento di un *computer*, e operano installandosi abusivamente, all'insaputa dell'utente. L'articolo in lettera, recentemente modificato dalla Legge 8 marzo 2008 n. 48[49], ai fini della sua configurabilità richiede ora un dolo specifico individuato nello "scopo di danneggiare illecitamente" un sistema informatico, mentre in precedenza si era concordi nel ritenere che l'elemento psicologico del reato fosse rappresentato dal dolo generico, ovvero dalla coscienza e volontà di diffondere, comunicare o consegnare un programma diretto a danneggiare o interrompere un sistema informa*tico*[50].

La nuova formulazione della norma, risulta essere decisamente più chiara ed è destinata a punire tutti coloro che "allo scopo di danneggiare illecitamente" si procurano, producono, diffondono o comunicano un programma o un apparato in grado di danneggiare un sistema informatico ovvero le informazioni, i dati o i programmi in esso contenuti. In realtà, ampi margini di incertezza continuano a sussistere, in quanto la norma in questione, punisce anche coloro che agiscono allo scopo di favorire l'interruzione, o l'alterazione del funzionamento di un sistema senza richiedere che tale interruzione, o alterazione, sia illecita o abusiva.

Ancora una volta, una grossa responsabilità è lasciata all'interprete che, sulla base dell'analisi del caso concreto, dovrà stabilire se la condotta del soggetto sia conforme alla legge ovvero sia suscettibile di sanzione.

Bisogna tener conto del fatto che ogni programma ha, necessariamente, per scopo o per effetto l'alterazione del funzionamento del sistema su cui viene installato, altrimenti sarebbe privo di qualsiasi utilità. Si pensi ad esempio agli aggiornamenti rilasciati dal produttore di un dato sistema operativo, che necessariamente comporta delle modificazioni ed alterazioni al funzionamento di un *computer*.

Relativamente a questo argomento, di grande importanza risulta essere l'analisi della Corte di Appello di Bologna, sul celebre caso Vierika. In

---

[49] Legge 8 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 in *Gazz. Uff. n. 80 del 4 aprile 2008*.

[50] In tal senso si veda Trib. Bologna, Sez. I, Sent. 1823 del 22 dicembre 2005 secondo cui "Ai fini della sussistenza dell'elemento soggettivo del reato *ex* art. 615 *quinquies* c.p., consistente nella diffusione di programmi (nella specie il programma Vierika) atti ad alterare alcune delle funzionalità telematiche dei sistemi informatici, si ritiene sufficiente che vi sia l'accertata volontà dell'agente di diffondere il programma con la consapevolezza dei suoi effetti non esigendo la norma che il fine dell'azione sia la distruzione o il danneggiamento del sistema informatico".

particolare, la difesa aveva eccepito che il programma Vierika non avesse provocato né l'alterazione, né il danneggiamento di un programma informatico dato che il *software* in questione si limitava ad installarsi e a diffondersi, senza apportare ulteriori modifiche. La Corte, pur riconoscendo che, non era ravvisabile, nelle modalità di installazione e di funzionamento di Vierika, alcun "danneggiamento" dei programmi o del sistema dell'utente, osservava che, comunque, il programma utilizzava ad insaputa dell'utente alcuni programmi installati nel sistema nonché alcuni dati presenti nella rubrica di posta elettronica.

In questa circostanza veniva stabilito che "alterare" un programma significasse manipolarlo in modo da fargli compiere azioni non volute dall'utente, ovvero cambiarne i parametri di funzionamento, in maniera che lo stesso agisca contro la volontà dell'utilizzatore o ad insaputa dello stesso[51]. Per questo motivo, veniva definita "alterazione" l'azione occulta ed indesiderata di modifica del registro di Windows, attraverso i comandi impartiti dal programma Vierika, e finalizzata a modificare l'*home page* predefinita del *browser*, provvedendo nello stesso tempo a diminuirne le protezioni. Allo stesso modo potevano essere considerati, alterazione di funzionamento, l'invio occulto di messaggi di posta elettronica.

Tale decisione, tracciava una rotta alquanto precisa nel *mare magnum* delle possibili interpretazioni: sono da considerarsi alterazioni abusive quelle che avvengono nell'incolpevole ignoranza del legittimo utilizzatore del sistema, o del programma, mentre sono da considerare perfettamente legittime tutte le altre modifiche introdotte a causa di aggiornamenti e simili, nella consapevolezza dell'utilizzatore. Va considerato inoltre, che molti *virus* non sono pericolosi tanto per i sistemi informatici ed i dati in essi contenuti, quanto per la riservatezza degli stessi: spesso tali programmi si propagano dal *computer* infetto utilizzando gli indirizzi che trovano nella rubrica di Windows, il loro scopo non è tanto danneggiare il sistema quanto sottrarre dallo stesso dati ed informazioni.

2.6. *L'intercettazione abusiva della posta elettronica*.

La protezione della libertà individuale originariamente assicurata dal codice penale, è stata nel tempo ampliata dalla Legge n. 98 del 1974 e successivamente dalla Legge n. 547 del 1993, mediante aggiornamenti ed inserimenti di nuove ed ulteriori figure di reato. In particolare la Legge n. 547/1993 con l'art. 5 ha

[51] Vedasi Corte di Appello di Bologna, Sez. II, 27 marzo 2008.

modificato il quarto comma dell'art. 616 c.p. estendendone la previsione normativa, che adesso recita: "*Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da 30 euro a 516 euro. Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni. Il delitto è punibile a querela della persona offesa. Agli effetti delle disposizioni di questa sezione, per corrispondenza s'intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza*". L'incidenza della nozione allargata di "corrispondenza".

Con riferimento alla corrispondenza informatica aziendale ed alle connesse problematiche anche di natura sindacale, risulta di particolare interesse la sentenza con la quale la Corte di Cassazione ha puntualizzato che non incorre nel reato di cui sopra il datore di lavoro che legge le *email* aziendali dei propri dipendenti, se l'impresa ha adottato un regolamento che impone la comunicazione della *password* del PC e della posta elettronica al proprio responsabile. Ciò risulta essere lecito, poiché l'art. 616 c.p. punisce la condotta di chiunque prenda conoscenza del contenuto di una corrispondenza chiusa, a lui non diretta, pertanto quando non vi è sottrazione o distrazione, la condotta di chi si limita a prendere cognizione è sanzionabile solo se riguarda corrispondenza "chiusa"[52]. Detta corrispondenza informatica o telematica può essere considerata "chiusa" solo nei confronti dei soggetti non autorizzati all'accesso ai sistemi informatici.

Sempre in tema di rapporti di lavoro, anche la giurisprudenza, ha precisato che il dipendente che utilizza la casella di posta aziendale, si espone al rischio che anche altri soggetti appartenenti alla stessa azienda, unica titolare dell'indirizzo *email* aziendale, possano lecitamente accedere alla casella in suo utilizzo non esclusivo e leggerne i contenuti previa acquisizione della relativa *password*[53].

Ne consegue che in caso di accesso alla posta elettronica aziendale del dipendente, non potrà ravvisarsi un elemento essenziale della fattispecie delittuosa

[52] Cass. Pen. Sez. V, 11 dicembre 2007, n. 47096.

[53] Tribunale di Torino, 15 settembre 2006, n. 143, in Guida Dir., n. 16, 2007.

prevista dall'art. 616 c.p., rappresentato, dal fatto che la casella di posta elettronica aziendale ed il suo utilizzo rientri nel quotidiano scambio di corrispondenza svolto dall'impresa nello svolgimento della propria attività organizzativa e produttiva; pertanto tutti gli apparati informatici e gli *account* di posta elettronica aziendali debbono ritenersi direttamente correlati all'impresa stessa, e solo assegnati in via mediata al soggetto utilizzatore, che in conseguenza di un rapporto di lavoro in quel dato momento rappresenta l'impresa. La *password* non sarà pertanto funzionale alla protezione dei dati e delle comunicazioni personali del dipendente, bensì ad impedire che a detti strumenti informatici possano accedere persone estranee alla società.

Il datore di lavoro può pertanto accedere liberamente alla casella di posta elettronica del personale dipendente e leggerne i messaggi in entrata ed in uscita, purché la stessa sia configurata con il dominio aziendale, e l'accesso avvenga per motivi connessi allo svolgimento delle attività lavorative; tranne nel caso in cui la qualifica del lavoratore comporti l'impossibilità o il divieto di compiere qualsiasi controllo da parte dell'azienda. Tornando alla norma rubricata all'art. 616 c.p. va puntualizzato che il bene giuridico tutelato dalla stessa, è la segretezza della corrispondenza di per sé considerata e non del suo contenuto, pertanto "nel reato di violazione di corrispondenza, di cui alla prima ipotesi dell'art. 616 c.p., oggetto della tutela penale non è il segreto, che eventualmente sia affidato alla corrispondenza, ma la corrispondenza in sé, la quale è dalla legge per se stessa ritenuta segreta, indipendentemente cioè dalla segretezza o non segretezza del suo contenuto"[54].

2.7. *L'intercettazione abusiva delle comunicazioni telematiche*.

Il bene giuridico tutelato dall'art. 616 c.p. differisce da quello protetto dal successivo art. 617 c.p. rinvenibile nella genuinità delle comunicazioni e che riguarda la "Cognizione, interruzione o impedimento illecito di comunicazioni o conversazioni telegrafiche o telefoniche", la norma recita: "*Chiunque, fraudolentemente, prende cognizione di una comunicazione o di una conversazione, telefoniche o telegrafiche, tra altre persone o comunque a lui non dirette, ovvero le interrompe o le impedisce è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico,*

[54] Vedasi Cass. Pen., Sez. V, 10 luglio 1997, n. 8838, in Cass. Pen., 1998.

in tutto o in parte, il contenuto delle comunicazioni o delle conversazioni indicate nella prima parte di questo articolo. I delitti sono punibili a querela della persona offesa; tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale o di un incaricato di un pubblico servizio nell'esercizio o a causa delle funzioni o del servizio, ovvero da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione di investigatore privato".

La fattispecie di reato in esame, comporta necessariamente che tali condotte vengano poste in essere in maniera fraudolenta, ossia con modalità in grado di eludere l'eventuale sorveglianza del soggetto passivo, trattandosi di un reato avente ad oggetto le comunicazioni in qualunque forma tra due o più soggetti, ne discende che la registrazione di conversazioni tra soggetti presenti, esclude la configurabilità del delitto.

La genuinità delle comunicazioni rappresenta l'elemento che ha spinto il Legislatore nel 1974 con la Legge n. 98 ad introdurre il reato previsto e punito dall'art. 617 *bis* c.p., installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche: "*Chiunque, fuori dai casi consentiti dalla legge, installa apparati, strumenti, parti di apparati o di strumenti al fine di intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche tra altre persone è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni ovvero da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio o da chi esercita anche abusivamente la professione di investigatore privato*".

Essendo la norma in parola diretta a scongiurare la violazione della riservatezza delle comunicazioni, non ha rilievo ai fini della configurabilità del reato, l'effettiva intercettazione o registrazione di altrui comunicazioni, essendo sufficiente la sola attività di installazione di apparati idonei allo scopo, anche qualora gli stessi non siano stati attivati o non abbiano funzionato[55]. La responsabilità potrà essere esclusa soltanto se l'apparecchiatura installata sia assolutamente inidonea all'intercettazione, e non nel caso di difetti tecnici o di errata installazione. Sulla base dell'articolo esposto, operando un'opportuna

[55] Vedasi Cass. Pen. Sez. V, 14 dicembre 2010, n. 3061, e Cass. Pen. Sez. II, 24 settembre 2008, n. 37710, in Dirittoitalia.it, 2012.

estensione delle condotte illecite previste è stato introdotto l'art. 617 *quater* c.p., che recita: "*Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:*
1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
2) da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
3) da chi esercita anche abusivamente la professione di investigatore privato".

Il rapido sviluppo delle tecnologie di comunicazione, unitamente alla lentezza del Legislatore, non risulta sempre facile definire cosa la norma intenda per "sistema informatico" e "sistema telematico", in linea di principio un sistema informatico è uno strumento tecnologico complesso costituito da un elemento materiale *hardware* e da un elemento immateriale *software*, capace di compiere autonomamente funzioni ed elaborare dati sulla base delle istruzioni impartite.

Il sistema telematico, consiste invece in un particolare sistema integrato, nel quale si fondono tecnologia informatica e mezzi di telecomunicazione, che lo rendono in grado di elaborare dati utilizzando il *software* installato e di trasmetterli a distanza attraverso linee telefoniche, impianti radio e satellitari[56].

Per intercettazione deve intendersi una presa di cognizione che si realizzi attraverso l'intromissione nella comunicazione in corso tra terzi e deve avere ad oggetto il contenuto di una comunicazione informatica o telematica.

---

[56] Nel 1999 la Corte di Cassazione ha individuato il sistema informatico nel "complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di codificazione e decodificazione – dalla registrazione o memorizzazione, per mezzo di impulsi elettronici, su supporti adeguati, di dati, di rappresentazioni elementari di un fatto, effettuata attraverso simboli (*bit)*, in combinazioni diverse, e dall'elaborazione automatica di tali dati, in modo da generare informazioni, costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente. La valutazione circa il funzionamento di apparecchiature per mezzo di tali tecnologie, costituisce giudizio di fatto, insindacabile in cassazione ove sorretto da motivazione adeguata e immune da errori logici". Cass. Pen., Sez. VI, 14 dicembre 1999.

Fattispecie tipica di intercettazione abusiva è l'analisi del traffico di rete con modalità tali da acquisire messaggi di posta elettronica, *password* ed ogni altra comunicazione o informazione in transito, ancora una volta appare chiaro che detta condotta deve essere caratterizzata da una modalità di realizzazione fraudolenta, ovvero essere posta in essere in maniera che risulti nascosta ai soggetti intercettati. Infatti, non può ritenersi fraudolenta l'intercettazione che venga posta in essere in maniera palese.

L'interruzione e l'impedimento consistono, nel compimento di atti tecnicamente idonei, rispettivamente a far cessare una comunicazione in atto e ad impedire che una nuova comunicazione abbia inizio. Una parte della dottrina ritiene che le condotte di interruzione o di impedimento in esame non richiedano una modalità di realizzazione fraudolenta, teoria che appare poco convincente.

Infatti, una simile interpretazione renderebbe illecita l'attività di installazione e di utilizzo di dispositivi di sicurezza come i c.d. *firewall*, che hanno il compito di impedire e interrompere eventuali comunicazioni di dati ritenute pericolose o non autorizzate in base alle impostazioni predisposte. Risulterebbe altresì illegale l'attività posta in essere da un amministratore di rete, che espletando le proprie funzioni, configura l'impostazione della rete da lui amministrata in modo da non permettere il transito di determinati flussi di dati, ad esempio traffico di dati da reti P2P, comunicazioni VoIP, ecc.

2.8. *Keylogger e sniffer*.

Evidentemente modellato sulla base dell'articolo 617 *bis* c.p., l'articolo 617 *quinquies* c.p. sanziona quelli che sono gli atti preparatori all'intercettazione e cioè la predisposizione e l'installazione di apparecchiature[57] "atte ad intercettare,

[57] In relazione alle apparecchiature, si veda Uff. Indagini preliminari di Milano, 19 febbraio 2007 "Integra il reato di cui all'art. 617 *quinquies* c.p. e non il reato di cui all'art. 615 *quater* c.p. la condotta di chi installa su uno sportello bancomat, in sostituzione del pannello originario, un'apparecchiatura composta da una superficie plastificata, con una microtelecamera con funzioni di registratore video per la rilevazione dei codici bancomat, quando non vi sia prova certa dell'avvenuta captazione di almeno un codice identificativo. L'attività illecita di intercettazione, infatti, nel silenzio dell'art. 617 *quinquies* c.p., deve ritenersi possa essere consumata con qualunque mezzo ritenuto idoneo a svelare la conoscenza di un sistema informatico quale è da considerarsi la digitazione da parte dell'operatore umano del codice di accesso ad un sistema attraverso una tastiera alfanumerica, digitazione che era destinata ad essere l'oggetto dell'illecita captazione". Si veda poi Cass. Pen., Sez. II, 9 novembre 2007, n. 45207 "Integra il reato di cui all'articolo 617 *quinquies* c.p. la condotta consistente nell'utilizzare apparecchiature idonee a copiare i codici alfanumerici di accesso degli utenti applicandole ai vari terminali automatici delle banche. Infatti, giacché la digitazione del codice di accesso costituisce la prima comunicazione di qualsiasi utente con il sistema informatico, conseguendone che la copiatura abusiva di detti codici rientra nel concetto di intercettazione di comunicazioni telematiche tutelata dalla norma".

impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi". La norma sanziona anche l'installazione abusiva di programmi o strumenti in grado di individuare e memorizzare i tasti premuti dall'utente sulla tastiera del personal *computer*[58] nonché la predisposizione di programmi in grado di intercettare i *pacchetti* in transito attraverso una rete, acquisendone i contenuti e permettendo all'utente di visualizzarli[59].

Esattamente come avvenuto per altre fattispecie di reato, il Legislatore ha ritenuto di poter applicare all'informatica una norma preesistente, senza interrogarsi sulle conseguenze del suo gesto, lasciando a giurisprudenza e dottrina l'arduo compito di sbrogliare la matassa.

A questo proposito la Corte di Cassazione ha, ripetutamente ribadito che il diritto alla riservatezza delle comunicazioni non può essere limitato se non in presenza di una specifica norma. Tuttavia, in relazione all'articolo in trattazione si dovrebbe adottare una maggiore tolleranza, da parte della giurisprudenza, nei confronti di atteggiamenti che pur se potenzialmente invasivi, sono assolutamente necessari alla tutela della sicurezza di un sistema informatico ovvero alla tutela della sicurezza di un minore.

Non vi sono dubbi, infatti, sulla liceità dei programmi destinati ai genitori per sorvegliare e limitare l'attività informatica dei propri figli per quanto gli stessi, astrattamente, possano essere ricondotti nel novero delle apparecchiature "atte ad intercettare, impedire o interrompere comunicazioni intercorrenti tra più sistemi".

---

[58] Si tratta dei c.d. "*keylogger*". La parola *keylogger* era già definita ai tempi del sistema operativo MS DOS. Evidentemente, la maggior parte dei *keylogger* dell'epoca si limitavano a registrare soltanto i tasti che venivano premuti obbligando la spia, una persona che doveva avere accesso diretto alla macchina, a prelevare tale registro in un momento successivo per vedere cosa venisse digitato. I moderni *keylogger* sono notevolmente migliorati dato che non si limitano a registrare le battute da tastiera, ma eseguono anche delle istantanee dello schermo, a determinati intervalli temporali ovvero alla digitazione di determinate parole chiave, per mostrare con quali finestre l'ignaro utente ha lavorato, catturando informazioni riguardo l'uso di internet e molto altro. A ciò si aggiunga che non vi è più la necessità di accedere fisicamente alla macchina in quanto molti dei *keylogger* moderni inviano per posta elettronica i loro rapporti.

[59] Si tratta dei c.d. "*sniffer*", compito di questo *software* è quello di analizzare il traffico in transito sulla rete a cui appartiene il *computer* che esegue il programma. Lo *sniffer* basa il suo funzionamento sull'architettura di un gran numero di protocolli di rete; in gran parte delle reti (Internet in testa) i dati vengono suddivisi in pacchetti, ciascuno recante le informazioni relative al destinatario (nel caso di Internet, l'indirizzo IP). Questi pacchetti transitano attraverso le reti e giungono ad ogni *computer* collegato fisicamente alla rete; in genere vengono acquisiti solo i pacchetti indirizzati a quel determinato indirizzo, ma lo *sniffer* consente di ricevere, ed elaborare, ogni pacchetto che passa sulla rete, ignorando il suo indirizzo di destinazione. È bene sottolineare che il pacchetto raggiunge comunque anche la sua destinazione originaria e, grazie a questa procedura, è possibile raccogliere dati su tutto il traffico di rete, ammesso che il *computer* sia sufficientemente potente da riuscire ad elaborarlo.

Spesso un amministratore ha la necessità di controllare il traffico dei dati all'interno della propria rete, in modo da individuare eventuali falle nella sicurezza e di verificare che non risultino attività "sospette" o potenzialmente pericolose. Allo stesso modo potrebbe ritenersi necessario bloccare determinati servizi, in quanto potenzialmente dannosi per la produttività dei dipendenti ovvero eccessivamente onerose in termini di risorse utilizzate.

In presenza di un'applicazione rigida della norma in questione, tali attività risulterebbero illecite (anche se effettuate in relazione ad un eventuale intruso[60]), ma non vi può essere alcun dubbio in relazione al fatto che le stesse possano essere lecitamente effettuate.

La soluzione preferibile è quella di predisporre un TOS (*Terms Of Service*)[61], in pratica una policy di gestione della rete informatica chiara per mezzo della quale gli utenti della rete autorizzano il loro amministratore a svolgere tutte quelle attività che, pur comportando una potenziale riduzione del loro diritto alla riservatezza, sono necessarie per garantire la loro sicurezza e l'affidabilità dell'intero sistema. Tanto per tornare all'esempio dello *sniffing*, si pensi che utilizzare un *pocket sniffer* non serve solo a capire quanto un potenziale attaccante potrebbe scoprire della rete e, quindi, a migliorarne la sicurezza, ma anche a individuare e valutare al meglio eventuali malfunzionamenti, per non parlare del fatto che molti IDS (*Intrusion Detection System*)[62] sfruttano tale sistema per rilevare pacchetti malformati o indizi di un attacco in corso.

L'attività di intercettazione di un amministratore di rete dovrebbe, pertanto, essere ritenuta giustificata *ex* art. 51 c.p. purché non eccedano le misure necessarie alla protezione del sistema stesso, senza scavalcare il confine tra difesa ed attacco[63] in particolare modo in considerazione della giurisprudenza formatasi in relazione all'articolo 617 *bis* c.p.

---

[60] A tale proposito si consideri quanto affermato da Cass. Pen., Sez. V, 4 aprile 1989, in Cass. Pen., 1990, I, 1303 ed in *Foro it.*, 1990, II, 180, secondo cui "ai fini della sussistenza del delitto di cui all'art. 617 *bis* c.p. l'espressione altre persone sta a significare qualsiasi persona diversa da colui che ha operato l'installazione dell'apparecchiatura atta ad intercettare od impedire la comunicazione oppure la conversazione telegrafica o telefonica".

[61] *Terms Of Service*, si tratta del regolamento di utilizzo di una determinata risorsa, in cui vengono previsti obblighi e diritti degli utenti ed in cui gli utenti possono rinunciare ad alcuni diritti per avere un servizio migliore e più accurato.

[62] *Intrusion Detection System.* Si tratta di programmi in grado di monitorare ed individuare eventuali accessi abusivi al sistema ovvero alla rete.

[63] Vedasi Cass. Pen., 11 febbraio 1988 in *Riv. pen.*, 1989, 865, secondo cui "non può ipotizzarsi l'esistenza degli estremi della necessità e proporzione di difesa, richiesti dall'art. *52* c.p., quando si reagisca con mezzi di aggressione del diritto alla riservatezza e all'inviolabilità dei segreti (nella specie, è stata esclusa la legittima difesa, quale scriminante del reato di installazione di apparecchiature per intercettazioni telefoniche, di cui all'art. 617 *bis*, c.p., osservandosi che

Infine è da osservarsi come, analogamente a quanto accade per l'art. 615 *bis* c.p., per il perfezionamento del reato non è necessario che il soggetto abbia le capacità tecniche di effettuare l'intercettazione, o l'impedimento delle comunicazioni, ma è sufficiente che abbia predisposto le apparecchiature.

2.9. *Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche*.

In questa fattispecie di reato, il bene tutelato è, come per l'art. 617 *ter* c.p., la libertà delle comunicazioni informatiche o telematiche, sotto il particolare profilo della sicurezza, genuinità e veridicità delle stesse.

In particolare questa norma tutela il contenuto della comunicazione, il reato in questione si consuma nel momento in cui viene utilizzato (falsificato, alterato o soppresso) il testo intercettato. Perplessità sorgono in merito ai possibili rapporti tra l'articolo 617 *sexies* c.p. e la fattispecie nota come *phishing*[64], soprattutto se si considera che non esiste ancora una norma incriminatrice che prenda in considerazione specificatamente questa fattispecie, che attualmente è perseguita con un combinato disposto di numerose norme penali.

Di particolare interesse ai fini della comprensione della norma in questione si rivela l'analisi della giurisprudenza sul tema. In una delle prime decisioni[65] in merito al fenomeno criminale c.d. "*phishing*" il GUP ricostruiva la condotta dell'imputato per poi arrivare alla condanna dello stesso per i reati di truffa, sostituzione di persona e falsità nell'utilizzo di carte di credito. In particolare il GUP forniva una prima definizione della fattispecie di reato osservando che "la tecnica utilizzata dall'imputato è quella del *phishing* (che suona come *fishing*, dall'inglese pescare), cioè dell'acquisizione dei dati di utenti di un servizio di carta di credito o di *home banking*, i quali volontariamente rispondono ad una richiesta di dati, inviata a un grande numero di persone, contattate grazie all'acquisizione

---

l'imputato, anziché compiere le intercettazioni abusive, ben avrebbe potuto ricorrere al giudice denunziando le dedotte molestie e ottenendo la tutela richiesta)".

[64] F. CAJANI, *Profili penali del phishing*, in Cass. Pen. 2007.

[65] GIP Milano, 15 ottobre 2007: " [...] acquistando un pacchetto di messaggi da inviare a terzi, aveva avuto modo di accedere ad un programma che consente di estrapolare numeri telefonici da siti internet che raccolgono annunci privati di compravendita di beni (autoveicoli ed immobili), indicati dagli stessi privati che avevano inserito l'annuncio. Inviato un SMS dal testo 'Chiami il numero 02/123456789 di Servizi Interbancari per verificare la transazione con la sua carta di credito, al fine di verificare usi fraudolenti ai telefoni cellulari così acquisiti, alla chiamata dei titolari di carte di credito allarmati dall'SMS ricevuto rispondeva non F.G. personalmente, ma, sotto le apparenze di un numero telefonico al quale corrispondeva in realtà l'indirizzo elettronico del suo PC, una voce sintetica che forniva una risposta automatica che richiedeva i dati della carta di credito di colui che stava chiamando".

dei loro recapiti, nel caso di specie questa captazione avveniva per mezzo di programmi informatici che estrapolano i numeri dei telefoni cellulari da siti che raccolgono inserzioni private. Il meccanismo comporta l'utilizzo di plurimi mezzi fraudolenti: in primo luogo l'alterazione dell'identità di chi chiede di essere chiamato (costituente di per sé un autonomo reato) fingendo di essere emissario di una società emittente carte di credito [...], la falsa segnalazione di un allarme, che fungendo da esca induca l'utente a rispondere al messaggio, e la predisposizione di un servizio automatico di risposta che sia simile a quello effettivamente corrispondente alla società di gestione delle carte di credito, ed induca l'interlocutore ad indicare i dati relativi alla propria carta di credito e al codice segreto, che verranno quindi utilizzati da chi ha predisposto la truffa. In una decisione successiva[66] il GIP individuava altre e differenti ipotesi criminose osservando che il c.d. "*phishing*" consiste nell'illecita intrusione per mezzo della Rete internet da parte di soggetti su sistemi informatici concernenti servizi "*home banking*" in danno ad utenti titolari di conti correnti bancari, clienti degli istituti di credito. Il reato integra, di per sé, i reati di accesso abusivo informatico e falsificazione del contenuto di comunicazioni informatiche di cui agli Artt. 615 *ter* e 617 se*xies* c.p.. Qualora detta attività venga svolta da parte di soggetti operanti in Paesi stranieri, in accordo con soggetti residenti nel territorio dello Stato al fine di realizzare truffe analoghe, carpendo mediante l'invio di false *email* apparentemente spedite da detti istituti di credito, le loro generalità ed i codici segreti (*userid* e *password*) relativi a detti servizi di *home banking*, realizza il reato di associazione a delinquere, con l'aggravante di reato transnazionale, di accesso abusivo informatico e di falsificazione di comunicazioni informatiche". Esistono pertanto, svariate norme nel cui alveo sembrano potersi ricondurre, le condotte sopra esposte, così come del resto è stato opportunamente messo in evidenza in numerosi commenti[67]. La creazione e l'invio della falsa *email* iniziale, finalizzata a truffare il malcapitato destinatario, può integrare numerose e diverse fattispecie penali di cui agli articoli 617 *sexies e* 494 c.p. in quanto, proprio nella sostituzione di persona, si sostanzia la falsificazione *ex* art. 617 *sexies* c.p. possono poi trovare applicazione le condotte di cui agli articoli 615 *quinquies* c.p., se l'acquisizione delle credenziali viene posta in essere attraverso un *software malware*, e 615 *quater* c.p.

[66] GIP Milano, 10 dicembre 2007, in *Foro ambrosiano*, 2008, 3, 280.

[67] L. FEROLA, *Il riciclaggio da phishing*: *tra vecchie e nuove questioni interpretative*, in *Giur. mer.*, 2009, 11, 2831.

Nella fattispecie criminosa, infine, si individua anche l'art. 615 *ter* c.p., che si concretizza nell'accesso abusivo al conto corrente della vittima.

2.10. *Il Phishing*.

Qualche tempo fa si è affacciato alle cronache un nuovo fenomeno criminale, strettamente legato allo strumento informatico, si tratta del fenomeno criminale del *phishing*[68], l'attività illecita aveva inizio con l'invio di false offerte di lavoro che, in realtà, conducevano "ignari" utenti a svolgere attività di riciclaggio o di ricettazione di denaro. Si trattava in genere di offerte di lavoro nelle quali il truffatore si presentava come il responsabile di una grossa multinazionale interessata ad espandere la propria attività sul mercato italiano ed alla ricerca di figure presentate come *"financial manager"* o responsabili di area.

Praticamente all'interlocutore italiano veniva richiesto di mettere a disposizione della sedicente azienda il proprio conto corrente bancario in modo da ricevere sullo stesso bonifici da parte di "clienti" dell'azienda stessa. Una volta

[68] Vedasi GUP Milano, 29 ottobre 2008, in *Foro ambrosiano*, 2008, 4, 406. Si veda, poi, lo stesso L. FEROLA, *Il riciclaggio da phishing: tra vecchie e nuove questioni interpretative*, in *Giur. mer.*, 2009: "La condotta del terzo che, fuori del caso di concorso nel reato, contribuisce al successo del phishing sostituendo o trasferendo denaro proveniente dai delitti attribuibili al *phisher* (quali, ad esempio, la truffa, la frode informatica, l'accesso abusivo ad un sistema informatico o telematico) oppure compiendo altre operazioni idonee a dissimularne od occultarne l'origine illecita, integra indubbiamente gli estremi del riciclaggio ai sensi dell'art. 648 *bis* c.p. L'estensione legislativa operata già dalla novella del 1990 consente, in effetti, di ricomprendere nell'ambito di applicazione della norma anche ipotesi relative ad operazioni bancarie, economiche o finanziarie realizzate tramite strumenti informatici o telematici, come i bonifici bancari, i trasferimenti di fondi, i pagamenti *online* e la creazione di depositi bancari". Si veda poi GUP di Palermo, 21 aprile 2009. Interessante si rivela la ricostruzione della vicenda allorché uno degli imputati aveva dichiarato che "che il proprio figlio, O. F., in cerca di un lavoro, aveva risposto ad una *email* inviata da una società spagnola, la I. che, affermando di operare nel settore assicurativo e nella vendita di automobili ed impegnandosi ad inviare la spedizione di documenti che avrebbero provato la legalità delle operazioni finanziarie, aveva concluso con O. F. un contratto di lavoro. Le condizioni di lavoro prevedevano che l'O. garantisse alla società la disponibilità di un conto corrente e che, tramite la Western Union, spedisse le somme transitate sul conto, al netto del compenso pari all'8% della somma, a soggetti che la società avrebbe, di volta in volta, indicato. Il 12 novembre 2007. O. F. aveva ricevuto sul proprio conto la somma di euro 2.965,00. Nell'attesa che la società inviasse la chiesta documentazione, l'O. si era recato, per avere dei chiarimenti in ordine all'operazione, presso un Commissariato di P.S., dove tuttavia non riceveva alcun aiuto (secondo quanto dichiarato dall'O. al Commissariato gli era stato detto di rivolgersi agli uffici della Polizia Postale competente). Trattenendo sul conto la provvigione pari all'8% della somma ricevuta, l'O. spediva comunque la restante parte ad una cittadina russa. Ricevuto un secondo bonifico, pari ad euro 3.500,00 e trasferita la somma ad un altro cittadino russo, non avendo ricevuto dalla I. la documentazione richiesta, appena ricevuto l'avviso di un terzo bonifico, decideva di bloccare le operazioni di accredito di somme". Nel corso dell'udienza il PM ed il difensore della parte civile avevano affermato la penale responsabilità degli imputati osservando che gli imputati, ove fossero stati in buona fede, avrebbero bloccato immediatamente l'accredito di somme sul loro conto ed avrebbero verificato immediatamente la liceità dell'operazione ed evidenziando come già il contenuto della corrispondenza tra gli O. e la società spagnola lasciasse trasparire l'illiceità dell'operazione. La difesa eccepiva che gli imputati erano stati vittime inconsapevoli di quel fenomeno denominato *phishing* e che l'elemento soggettivo del riciclaggio non poteva essere costituito dal dolo eventuale.

ricevuto il bonifico il *"financial manager"* non doveva fare altro che prelevarlo in contanti dal proprio conto, recarsi presso uno dei tanti servizi di trasferimento di denaro quali ad esempio: Western Union o Moneygram, ed inviare tramite queste piattaforme finanziarie la somma prelevata a terze persone residenti all'estero, detratte le commissioni previste dal suo contatto. Dette commissioni potevano variare da un minimo del 10% fino ad arrivare al 25% della somma ricevuta.

Le somme pervenute sul conto corrente del soggetto erano, in realtà, importi sottratti indebitamente a soggetti cui erano stati sottratte le credenziali di accesso ai rispettivi conti correnti *online.* Il GUP del Tribunale di Milano ha osservato che, ove il "ricettatore o riciclatore sia consapevole dell'attività truffaldina del *phisher*, ed assicuri a questi la propria collaborazione nel ricevere bonifici fraudolenti e quindi nel trasferire a terze persone ignote le somme percepite con altri mezzi non bancari quali il *'money transfer*' internazionale, è indubbio che debba rispondere di concorso nell'attività delittuosa del *phisher*. Al contrario, nel caso in cui il c.d. "*financial manager*" riceva solo la mera richiesta di farsi accreditare somme su un proprio conto corrente e di trasferire all'estero successivamente in altro modo le somme di denaro così ricevute, essendo quindi inconsapevole del disegno criminoso complessivo, non si potrà configurare il concorso reato presupposto, ma potrà incorrere, sulla base della valutazione degli elementi concreti a lui noti, nel reato di riciclaggio e/o ricettazione a titolo di dolo eventuale"[69]. Il delitto di riciclaggio prevede, infatti, solo il dolo generico, che consiste "nella coscienza e volontà di ostacolare l'accertamento della provenienza dei beni, del denaro e di altre utilità, senza alcun riferimento a scopi di lucro"[70] ed è proprio l'elemento soggettivo, costituito dal dolo specifico dello scopo di lucro previsto nella ricettazione e dal dolo generico previsto nel delitto di riciclaggio, a distinguere i due delitti. A questo riguardo, nel riciclaggio l'elemento soggettivo del delitto può essere sicuramente integrato dall'accettazione del rischio che la propria condotta possa ostacolare l'identificazione della provenienza delittuosa del denaro, dei beni o di altre utilità e che, al fine di valutare la responsabilità penale degli imputati, occorrerà verificare se l'adesione al programma delittuoso sia stata dolosamente condivisa dagli stessi, nel qual caso sarà possibile riconoscere la loro

[69] Vedasi in tal senso si veda anche GUP di Palermo, 21 aprile 2009. Il Giudice evidenziava che la condotta delittuosa degli O. poteva ben inserirsi nel fenomeno indicato comunemente con il termine *phishing* e che "detto fenomeno, che non corrisponde ad alcuna figura giuridica contemplata specificamente dal codice penale, può assumere rilievo giuridico in quanto si snoda attraversi fasi, potenzialmente idonee a concretizzare gli elementi strutturali, oggettivi e soggettivi, di condotte delittuose sanzionate penalmente".

[70] Cass. Pen., Sez. VI, 24 aprile 2008, n. 16980; Cass. Pen., Sez. VI, 12 aprile 2005, n. 13448.

responsabilità penale in ordine al delitto di riciclaggio[71].

2.11. *Il danneggiamento informatico*.

Il recepimento nel nostro ordinamento della Convenzione del Consiglio d'Europa del 23 novembre 2001, intervenuta con la già citata Legge n. 48/2008, ha comportato la creazione di numerose ipotesi di danneggiamento speciali.

Precedentemente alla suddetta ratifica nel codice penale italiano, l'articolo 635 *bis* c.p. poteva considerarsi, di fatto, una semplice trasposizione del reato di danneggiamento già prevista all'articolo 635 c.p., nei cui confronti si poneva in rapporto di specialità e questa circostanza. Per questo motivo, l'effetto pratico della novella legislativa del 1993 era stato esclusivamente quello di rendere procedibile d'ufficio il reato e di aumentarne significativamente la pena.

Il "patrimonio informatico", inteso quale complesso di dati raccolti, trattati e gestiti per mezzo del *computer*, rappresenta oggi un bene di rilevante importanza e grande valore economico. La norma recita: "*Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni*".

L'articolo 635 *bis* c.p., è stato sostituito da ben quattro nuovi articoli, rendendo se possibile, ancora più difficoltosa l'applicazione della normativa in esame.

La Legge 18 marzo 2008, n. 48, all'articolo 6, ha abrogato il secondo ed il terzo comma dell'articolo 420 c.p., mentre all'articolo 5 ha sostituito l'articolo 635 *bis* c.p. ed introdotto nel codice gli articoli 635 *ter, quater* e *quinquies* del codice penale.

Il Legislatore ha voluto in questo modo separare fattispecie di reato differenti, la difficoltà maggiore in cui si è imbattuto è rappresentata dal medesimo problema già avvertito dalla dottrina precedentemente alla Legge n.

[71] Nel caso specifico il GUP rilevava che l'*email* conteneva vistosi errori di grammatica, ripetizioni e fantasiose nozioni giuridiche, tanto che "il contenuto e la forma della *email*, le condizioni del contratto ed in particolare la richiesta del numero del conto corrente, non potevano indurre gli O. a ritenere che la proposta contrattuale avesse una dignità giuridica e non celasse un'operazione dai connotati illeciti".

547/1993, cioè attribuire ai dati ed ai programmi lo *status* di cosa mobile e di conseguenza poter applicare agli stessi la previgente disciplina.

La riforma del 2008 non ha apportato grandi modifiche alla previgente disciplina; la formulazione della fattispecie viene sostanzialmente riproposta dal disegno di legge, che si limita ad omettere la condotta di colui che rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, condotta oggi punita dal "nuovo" art. 635 *quater* c.p.. L'unica rilevante modifica riguarda la condizione di procedibilità del reato che diviene perseguibile a querela della persona offesa, mantenendo la perseguibilità d'ufficio solo nell'ipotesi aggravata del comma 2.

In conseguenza della stessa riforma, il vecchio inciso "o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui" si è trasformato nel nuovo articolo 635 *quater* c.p. destinato a punire con la reclusione da uno a cinque anni, colui che, mediante le condotte di cui all'articolo 635 *bis* c.p., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento. Il reato risulta essere aggravato laddove ricorra la circostanza di cui al numero 1) del secondo comma dell'articolo 635 c.p. ovvero se il fatto viene commesso con abuso della qualità di operatore del sistema. Si rappresenta che nonostante la rilevante portata delle novità introdotte dalla citata Legge, continua a mancare nel codice una definizione in grado di stabilire in modo certo e definitivo che cosa si intenda per "sistema informatico".

A questo proposito, la Corte, rilevato che la legge ancora oggi non fornisce alcuna definizione di "sistema informatico" dandone per presupposta la nozione, ha osservato che: "pare comunque che si debba ritenere che l'espressione “sistema informatico” contenga in sé il concetto di una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche"[72].

Tale indirizzo non differisce molto da una precedente pronuncia[73] in cui il giudice di legittimità individuava nei *decoder* delle trasmissioni satellitari un

[72] Cass. Pen., Sez. VI, 4 ottobre 1999, n. 3067. In tal senso si veda anche la definizione offerta dall'articolo 1 lettera *a)* della Convenzione di Budapest secondo cui "*computer system means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*".

[73] Cass. Pen., Sez. V, 2 luglio 1998, n. 4389: "Il *decoder*, che utilizza lo stesso principio di funzionamento degli elaboratori e dei *computer*, è un apparecchio che rielabora il segnale ricevuto, utilizzando i dati digitali contenuti sulla card e ricompone il segnale in maniera che sia intellegibile dal televisore. Pertanto, i sistemi di trasmissione televisivi satellitare, differiscono dalle normali trasmissioni televisive terrestri, in quanto costituiti da un insieme di apparati, in particolare trasmettitori, convertitori, satelliti, elaboratori di dati in trasmissione (*encoder*) e analoghi

sistema informatico protetto da misure di sicurezza. Analogamente, in una recente decisione, il Tribunale di Milano[74] ha stabilito che per sistema informatico "deve intendersi una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione, anche in parte, di tecnologie informatiche, poiché non è un sistema informatico tutto ciò che, in un sito *web* o nel mondo dell'informatica, non è capace di gestire, od elaborare dati in vista dello svolgimento di una funzione".

Alla luce delle citate pronunce la dottrina ha tentato di individuare gli elementi distintivi del sistema informatico identificandolo in tutte quelle "apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo attraverso l'utilizzazione (anche in parte) di tecnologie informatiche"[75].

Quindi, ciò che caratterizza il sistema informatico è la diversa programmabilità e la variabilità dei risultati alla luce dei differenti dati di *input* eventualmente inseriti, caratteristica che permette di non confonderlo con un mero apparecchio elettronico. Dunque la capacità del sistema informatico di elaborare dati è l'elemento essenziale per la sua definizione, ed è proprio a tale elemento che dovrà farsi riferimento per individuare in concreto la fattispecie di danneggiamento.

Anche alla luce di quanto appena detto, la definizione del nuovo articolo 635 *quater* c.p. genera numerose perplessità, resta da comprendere perché il Legislatore abbia duplicato la fattispecie di cui al precedente articolo 635 *bis* c.p. generando una sorta di norma ibrida.

Dalla lettura delle due norme novellate, sembrerebbe, che, mentre l'articolo 635 *bis* c.p. è finalizzato a tutelare l'integrità dei dati, il 635 *quater* c.p. sia destinato a tutelare la funzionalità del sistema informatico nel suo insieme.

La cancellazione di dati, informazioni o programmi comporta necessariamente un malfunzionamento del sistema, quantomeno allo scopo per cui quel programma è stato installato e, anche se i dati e le informazioni fossero

---

elaboratori in ricezione (*decoder*), ricevitori protetti da misure di sicurezza (criptazione), finalizzati alla trasmissione di dati che non sono costituiti solamente da immagini e suoni, ma anche da testi, che diffusi da centri di smistamento costituiti dalle reti televisive, permettono di raggiungere gli utenti abilitati e, cioè, in possesso di *cards* legalmente acquisite, che contengono i codici necessari alla lettura dei segnali codificati. Ne consegue che anche sotto tale aspetto, considerati i vari sistemi di trasmissione televisiva, le *cards* siano idonee a permettere l'accesso a sistemi informatici e/o telematici".

[74] Tribunale di Milano, Sez. III, 19 marzo 2007.

[75] Vedasi a questo proposito S. ATERNO, *Sull'accesso abusivo a un sistema informatico o telematico,* in Cass. Pen., 2000, 2990 e anche L. CUOMO, *La tutela penale del domicilio informatico,* in Cass. Pen., 2000, 2990.

comunque ancora disponibili in un supporto di *backup*, la loro rimozione avrebbe comunque causato un ostacolo al buon funzionamento del sistema, ma quand'è che un simile ostacolo può essere definito grave? In linea di massima sembrerebbe che tale non possa essere definita la semplice necessità di dover accedere all'archivio, prendere un supporto di *backup* ed inserire nuovamente i dati cancellati, ma, tuttavia, seguendo questa logica è assai difficile individuare in quale tipo di manomissione possa ravvisarsi il "grave ostacolo".

A ciò occorre aggiungere che il Legislatore non ha fornito indicazioni in merito alle modalità con cui devono essere alterati i dati per il perfezionamento del reato: non è, infatti, richiesta la volontà di arrecare un danno, l'abusività della condotta e nemmeno l'ingiustizia del danno stesso, ma soltanto la semplice condotta di colui che distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.

Alla luce di quanto esposto risulta pertanto difficoltoso individuare con assoluta certezza i limiti della condotta sanzionabile, soprattutto in presenza di attività che normalmente un amministratore di rete compie ordinariamente nello svolgimento delle proprie mansioni, ad esempio disinstallare dai *computer* utilizzati in una determinata società, eventuali programmi non autorizzati, procedendo quindi alla loro cancellazione. È evidente che, in tale circostanza, l'imputato potrebbe invocare l'esercizio di un diritto o l'adempimento di un dovere, ma resta il fatto che il Legislatore avrebbe dovuto prevedere la possibilità che un terzo possa legittimamente intervenire in un PC o su programmi altrui.

Occorrerà pertanto, come per altre norme analizzate in precedenza individuare caso per caso limiti e portata della norma considerata.

Procedendo nell'analisi della fattispecie di reato si riporta l'art. 635 *ter* c.p. che recita:"*Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni*".

Per quanto attiene agli altri due articoli aggiunti dalla novella del 2008, l'articolo 635 *ter* c.p., sopra riportato che, con il 635 *quinquies* c.p., ha sostituito il 2° ed il 3° comma dell'articolo 420 c.p., occorre anzitutto osservare che, anche in questo caso, la scelta relativa alla collocazione *delle* norme risulta essere decisamente criticabile: non si comprende la ragione per cui gli articoli 635 *ter* e 635 *quinquies* c.p., attinenti a reati contro lo Stato, altro ente pubblico o comunque impianti o sistemi di pubblica utilità, siano stati collocati all'interno del Titolo XIII, delitti contro il patrimonio, e non all'interno del Titolo V, delitti contro l'ordine pubblico, dove pure si trovavano in precedenza quali 2° e 3° comma dell'articolo 420 c.p.

La seconda critica è relativa alla formulazione dell'articolo 635 *quinquies* c.p., che risulta essere eccessivamente poco chiara. Detto che lo schema della norma è riconducibile ad un delitto di mera condotta, con un secondo comma che prevede un'aggravante speciale nel caso in cui si verifichi l'evento dannoso, i due articoli in questione rappresentano in pratica la "versione pubblica" dei due articoli trattati in precedenza, ma senza alcuna distinzione, ai fini della pena, tra *hardware* e *software*.

Scelta del Legislatore, che ricalca quanto già previsto dal "vecchio" articolo 420 c.p., rende ancora più difficile da capire la scelta operata con la modifica del 635 *bis* c.p. e l'introduzione del 635 *quater* c.p. in cui il danneggiamento dell'*hardware* viene punito assai più gravemente del danneggiamento del *software* o dei dati. In pratica, si è venuto a creare il paradosso per cui l'*hardware* di proprietà dei privati o comunque non destinato ad impieghi di pubblica utilità gode, da un punto di vista giuridico, di una maggior tutela rispetto ai sistemi informatici di interesse pubblico. Per un rapido confronto si riportano di seguito, in estrema sintesi, le differenti fattispecie penali appena analizzate:

- 635 *bis:* danneggiamento di informazioni, dati e programmi; pena base da 6 mesi a 3 anni, procedibile a querela. Pena da 1 a 4 anni e procedibilità d'ufficio nell'ipotesi aggravata.
- 635 *quater:* danneggiamento di sistemi informatici e telematici; pena base da 1 a 5 anni, procedibile d'ufficio.
- 635 *ter*: danneggiamento di informazioni, dati e programmi utilizzati dallo Stato o comunque di pubblica utilità; il mero compimento di atti diretti a

danneggiare il bene è punito con la reclusione da 1 a 4 anni. Se si verifica l'evento la pena è della reclusione da 3 a 8 anni.

- 635 *quinquies:* danneggiamento di sistemi informatici o telematici di pubblica utilità; il mero compimento di atti diretti a danneggiare il sistema è punito con la reclusione da 1 a 4 anni. Se si verifica l'evento la pena è della reclusione da 3 a 8 anni.

Alla luce di quanto sopra esposto è pertanto corretto ritenere integrato il delitto di danneggiamento tutte le volte in cui la condotta criminosa di un soggetto provochi la distruzione di un bene ovvero un deterioramento tale da diminuire, anche solo parzialmente, il valore e l'utilizzabilità del bene stesso e tale da ritenersi necessario un intervento di ripristino del sistema.

L'elemento oggettivo del reato di danneggiamento consiste, quindi, in una modificazione, strutturale o funzionale, della cosa che determina la necessità di un intervento in grado di ripristinare la funzionalità della cosa stessa.

Alla stessa stregua, sembrerebbe doversi richiedere un periodo minimo di reale inutilizzabilità del sistema informatico in assenza del quale non potrebbe seriamente parlarsi di danneggiamento; andrebbe, quindi, ritenuto danneggiato il sistema non più in grado di svolgere, sia pure per un periodo limitato, i propri compiti ovvero in grado di svolgerli soltanto con eccessiva difficoltà.

Dovrebbe pertanto potersi ravvisare il reato di danneggiamento di sistema informatico in presenza di un attacco DdoS[76], ma non in presenza della semplice disconnessione del cavo di rete o di spegnimento di un *router wifi*. Infatti anche in questo secondo caso il *server* non risulta più raggiungibile ma, stante la facilità con cui è possibile ripristinare la connessione, non si potrà configurare un danneggiamento.

Per meglio comprendere la portata della norma risulta inoltre molto importante stabilire con precisione quali beni risultino essere essenziali e quali, invece, debbano essere considerati elementi esterni o accessori del bene informatico principale. Si pensi, per esempio, alla tastiera, al *mouse* o al *monitor*, dispositivi che fanno sicuramente parte di un sistema informatico, ma che non ne

[76] DdoS, o DoS, scritto con la maiuscola al primo e terzo posto, indica un particolare tipo di attacco informatico definito *denial of service* (negazione del servizio). L'attacco consiste nel tentativo di portare il funzionamento di un sistema informatico che fornisce un servizio, ad esempio un *server ftp* o un *server web*, al limite delle prestazioni, fino a renderlo non più in grado di erogare il servizio. In genere l'attacco viene effettuato inviando molti pacchetti di richieste, di solito ad un *Server Web*, *FTP* o di posta elettronica, saturandone le risorse e rendendolo o "instabile" o, comunque, incapace di continuare ad erogare il servizio.

pregiudicano l'effettivo funzionamento; infatti, qualora si ritenessero tali periferiche di *input/output* parti di un sistema informatico in senso giuridico, ai sensi della norma in trattazione, rompere un *mouse* o una tastiera configurerebbe il reato di danneggiamento di sistema informatico mentre, nel caso di sistema di pubblica utilità, sarebbe sufficiente compiere atti idonei a rompere la periferica perché l'autore possa essere ritenuto colpevole del reato di cui all'articolo 635 *quinquies* c.p. Sarà pertanto necessario restringere il campo di azione della norma in trattazione, limitando la sua applicazione alle sole fattispecie in cui l'azione è effettivamente idonea a danneggiare un componente essenziale del sistema identificando come tali tutti quei componenti che caratterizzano il sistema stesso, rendendolo capace di acquisire ed elaborare dati.

In conclusione, perché possa configurarsi il reato di danneggiamento di sistema informatico o telematico, è necessario che oggetto dell'attacco sia effettivamente un sistema informatico (ovvero dati o programmi in esso contenuti) e che, in conseguenza dell'attacco, le funzionalità informatiche del sistema siano state in tutto o in parte pregiudicate in maniera tale da non poter essere ripristinate senza interrompere o comunque ostacolare le funzionalità del sistema stesso.

2.12. *La frode informatica*.

Ai sensi dell'art. 640 *ter* c.p., "*chiunque alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno è punito con la reclusione da sei mesi a tre anni e la multa da 51 a 1302 euro"*.

Il reato di frode informatica potrebbe essere considerato un reato informatico *in senso proprio,* nella misura in cui il sistema informatico o telematico sembrerebbe rappresentare l'oggetto su cui necessariamente ricade l'azione criminosa, e quasi sempre anche il mezzo che la consente.

Tuttavia, sotto altro e diverso aspetto, la fattispecie di reato in esame potrebbe essere ricompresa tra i reati *eventualmente informatici,* ovvero, tra quei reati che non proteggono un *bene informatico.*

Parte degli studiosi sostengono che la norma tuteli la regolarità ed il buon funzionamento dei sistemi informatici, altri sostengono che sia stata posta a tutela del patrimonio; vi è, infine, chi sostiene che il reato di frode informatica debba

essere considerato un reato *plurioffensivo*, poiché la condotta di cui all'articolo 640 *ter* c.p. apporta una concreta lesione ad una pluralità eterogenea di beni giuridici, come, ad esempio, il regolare funzionamento dei sistemi informatici, la riservatezza ed il patrimonio altrui. Al fine di prospettare una soluzione al problema appena delineato, sarebbe opportuno che venisse correttamente ponderata la collocazione del reato, introdotto dal Legislatore subito dopo il reato di truffa e modellato sullo schema di quest'ultima fattispecie. Risulta peraltro dubbio che il regolare funzionamento di un sistema informatico, in sé considerato, possa godere di una legittima e giustificata protezione da parte dell'ordinamento, infatti, risulta evidente che la norma penale ha sempre il compito di tutelare interessi umani, individuali o collettivi che siano.

Se a tutto ciò aggiungiamo che esistono altre e puntuali disposizioni a tutela della *privacy* e, soprattutto, la constatazione per cui il titolare del sistema informatico danneggiato non necessariamente debba essere anche titolare del patrimonio saccheggiato, diviene evidente come l'interesse protetto dalla disposizione sia da rintracciare esclusivamente nell'integrità patrimoniale del soggetto passivo.

Le difficoltà interpretative appena accennate risultano amplificate dal fatto che la condotta descritta nel reato in parola sembrerebbe integrare una mera modalità attuativa della truffa, piuttosto che una condotta criminale autonoma ed indipendente. Senza ombra di dubbio, il reato di truffa è un reato a *forma vincolata*, altrettanto certamente, gli "artifici" ed i "raggiri" a cui fa riferimento l'art. 640 c.p. possono essere realizzati secondo molte ed eterogenee modalità attuative: affinché possa configurarsi il reato, non rileva in quale modo sia stato ingannato il soggetto passivo, ma il fatto che, in base a tale inganno, il reo sia riuscito ad estorcere il consenso che gli abbia poi permesso di ottenere un ingiusto profitto con altrui danno. Ad una prima lettura risulta difficile comprendere il motivo che ha spinto il Legislatore ad elevare ad autonoma figura di reato una condotta criminale che pare essere ricompresa ed integrare una delle numerose modalità commissive previste nell'art. 640 c.p..

Si potrebbe ritenere che la previsione dell'art. 640 *ter*. c.p. dipenda dalla maggiore pericolosità sociale avvertita rispetto al reo, che non sarebbe in questo caso un comune delinquente, ma un *hacker*, oppure un *cracker*[77].

[77] Per la descrizione di *hacker* e *cracker*: https://it.wikipedia.org/wiki/Cracker_%28informatica%29

Il soggetto attivo quindi sarebbe un esperto di informatica, una mente criminale talmente raffinata e tecnologicamente competente da riuscire a manipolare un sistema informatico, intervenendo sui dati, sulle informazioni o sui programmi in esso contenuti, per questo motivo andrebbe punito in maniera più severa, o comunque diversa, rispetto a chi commette una "semplice" truffa.

Evidentemente, se la *ratio* che ha portato alla creazione dell'articolo in esame fosse questa, risulterebbe alquanto debole e poco significativa. Anzitutto perché grazie alle infinite guide, *tool* informatici liberamente scaricabili dalla Rete e *forum* di discussione, presenti soprattutto nel c.d. "*deep web*"[78], nella realtà dei fatti il reato *de quo* viene commesso spesso anche da soggetti che non possiedono particolari competenze informatiche, quindi non necessariamente veri e propri *hacker* o *cracker*, ma spesso comuni internauti, con pochi scrupoli, entrati in qualche modo in possesso degli strumenti *hardware* e/o *software* necessari ad interferire con il corretto funzionamento di un sistema informatico.

Il reato di frode informatica, è a tutti gli effetti un reato comune, non avendo alcuna rilevanza se il soggetto agente sia un *hacker*, un *cracker* o un comune cittadino, l'unica cosa che rileva è che lo stesso abbia agito in maniera illecita, così come descritto nella norma, ottenendo così l'ingiusto profitto con l'altrui danno.

Per comprendere il motivo che ha spinto il Legislatore a prevedere *la frode informatica* come autonoma figura di reato, occorre dunque prendere spunto dalla Relazione alla Legge n. 547/1993 nella quale si rileva espressamente che l'introduzione del reato di frode informatica è dovuta alla discussa configurabilità del reato di truffa in caso di "analogo illecito informatico". Questa difficoltà deriverebbe dal fatto che il reato di truffa si caratterizza in senso necessariamente *relazionale* ed *intersoggettivo.* Gli artifici ed i raggiri di cui all'articolo 640 c.p. sono normalmente indirizzati a condizionare il consenso di un altro essere umano, mentre, in caso di frode informatica, il contegno del soggetto passivo non viene preso minimamente in considerazione, infatti, come spesso accade, quest'ultimo potrebbe non essere nemmeno consapevole dell'attività posta in essere dal reo.

[78] Il *Web* sommerso (o *deep web*), spesso erroneamente confuso con il *Dark Web* (che è invece riferito alla navigazione del *web* sommerso in anonimato), è l'insieme delle risorse informative del *World Wide Web* non segnalate dai normali motori di ricerca. Secondo una ricerca sulle dimensioni della rete condotta nel 2000 da Bright Planet un'organizzazione degli Stati Uniti d'America, il *web* è costituito da oltre 550 miliardi di documenti mentre Google ne indicizza solo 2 miliardi, ossia meno dell'uno per cento. (Fonte: Wikipedia).

E’ tipico in questo senso il fenomeno criminale del *phishing*[79] precedentemente analizzato o dei sempre più frequenti fenomeni di manomissione di *bancomat*, dove al malcapitato utente del servizio bancario viene illecitamente clonata la carta *bancomat* e carpito il *PIN code*[80]. Esiste pertanto, tra la frode informatica e la truffa un rapporto di specialità, di conseguenza, ma si deve escludere che tra le due fattispecie possa configurarsi un concorso formale. Le espressioni “*alterando in qualsiasi modo*" e “*intervenendo con qualsiasi modalità*" dimostrano che il Legislatore non ha inteso descrivere con eccessiva precisione la condotta del reo: come nel caso del reato di accesso abusivo a sistema informatico, vi sono anche qui molteplici ed imprevedibili modalità attuative. Tuttavia, dobbiamo considerare che l'art. 640 *ter* c.p. fa esplicito riferimento a due condotte - l'alterazione e l'intervento - che non possono in alcun modo mancare affinché si configuri una frode informatica.

2.13. *La frode informatica nella certificazione di firma elettronica*.

Una nuova ulteriore fattispecie di reato introdotta nel nostro ordinamento con la ratifica della Convenzione di Budapest del 23 novembre 2001 è contenuta nell'art. 640 *quinquies* c.p., inserito nel codice penale dall'art. 5 comma 3 della Legge n. 48/2008 e prevede che: "*Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro*". Tale nuovo articolo segue il reato di frode informatica e si pone in rapporto di specialità con il reato di truffa, *ex* art. 640 c.p., per la maggiore gravità della condotta del soggetto agente, nonché per il suo delicato ed importante ruolo di certificatore[81]. Il Legislatore ha ritenuto opportuno

---

[79] Il *phishing* è un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso. Si tratta di un’attività illegale che sfrutta una tecnica di ingegneria sociale: il malintenzionato effettua un invio massivo di messaggi di posta elettronica che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi; tali messaggi fraudolenti richiedono di fornire informazioni riservate come, ad esempio, il numero della carta di credito o la *password* per accedere ad un determinato servizio. Per la maggior parte è una truffa perpetrata usando la posta elettronica, ma non mancano casi simili che sfruttano altri mezzi, quali i messaggi SMS. Il termine *phishing* è una variante di *fishing* (letteralmente "pescare" in lingua inglese), probabilmente influenzato da *phreaking* e allude all'uso di tecniche sempre più sofisticate per "pescare" dati finanziari e *password* di un utente. (Fonte Wikipedia: https://it.wikipedia.org/wiki/Phishing).

[80] PIN *code*, (*Personal Identification Number*), *password* numerica di 4 o 5 cifre, utilizzata per autenticare un utente ad un sistema o per accedere a servizi bancomat su un ATM.

[81] L'art. 1, comma 1, lett. g) del D.Lgs. n. 82/2005 *(Codice dell'Amministrazione digitale)* definisce

adeguare la normativa esistente, con l'inserimento della fattispecie di frode informatica compiuta dal "certificatore qualificato[82]; tale fattispecie non poteva essere in alcun modo ricompresa nel reato di frode informatica, *ex* art. 640 *ter* c.p., stante la differenza di presupposti sui quali si basano, rispettivamente, le due figure di reato. La condotta dell'agente, nel reato in esame, deve essere dolosa, poiché lo stesso deve intenzionalmente violare gli obblighi previsti dalla legge per il rilascio di un certificato al fine di conseguire un ingiusto profitto.

Gli obblighi di legge cui si riferisce la norma sono quelli previsti dall'art. 32 del codice dell'amministrazione digitale. Con l'art. 640 *quinquies* c.p., il Legislatore ha voluto introdurre nel codice penale una norma contenente specifiche sanzioni riservate al certificatore qualificato, in aggiunta ai profili di responsabilità civile, già previsti nello stesso art. 32, codice dell'amministrazione digitale.

2.14. *Gli altri reati previsti nella lista facoltativa della raccomandazione del Consiglio d'Europa del 1989.*

Dopo aver esaurito l'esame delle ipotesi di reato ricomprese nella lista minima contenuta nella Raccomandazione del 1989, è opportuno accennare alle

---

certificatore: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime. Lo stesso Codice dell'Amministrazione digitale, nel comma 1 dell'art. 26, prevede che: L'attività dei certificatori stabiliti in Italia o in un altro Stato membro dell'Unione europea è libera e non necessita di autorizzazione preventiva. Detti certificatori o, se persone giuridiche, i loro legali rappresentanti ed i soggetti preposti all'amministrazione, devono possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche di cui all'articolo 26 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385, e successive modificazioni. I requisiti per l'esercizio dell'attività di certificatore, pertanto, sono quelli di onorabilità previsti dal testo unico bancario per i soggetti che svolgono funzione di amministrazione, direzione e controllo presso le banche.

[82] L'art. 27 del Codice dell'Amministrazione digitale stabilisce competenze ed obblighi del certificatore qualificato: I certificatori che rilasciano al pubblico certificati qualificati devono trovarsi nelle condizioni previste dall'articolo 26.

2. I certificatori di cui al comma 1, devono inoltre:

a) dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere attività di certificazione;

b) utilizzare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia delle firme elettroniche e della dimestichezza con procedure di sicurezza appropriate e che sia in grado di rispettare le norme del presente codice e le regole tecniche di cui all'articolo 71;

c) applicare procedure e metodi amministrativi e di gestione adeguati e conformi a tecniche consolidate;

d) utilizzare sistemi affidabili e prodotti di firma protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo e internazionale e certificati ai sensi dello schema nazionale di cui all'articolo 35, comma 5;

fattispecie indicate nella lista facoltativa, per verificare se nell'ordinamento italiano esistono figure criminose ad esse corrispondenti. A tale proposito, da una attenta lettura della norma e delle relazioni sui lavori preparatori alla Legge n. 547/1993, si può affermare che il Legislatore ha rivolto la propria attenzione unicamente all'accoglimento dei suggerimenti contenuti nella lista minima, non occupandosi dunque di quelli presenti nella lista facoltativa.

In quest'ultima erano proposte come fattispecie da sanzionare penalmente, le seguenti condotte criminose:

1. alterazione di dati o programmi informatici;
2. spionaggio informatico;
3. utilizzazione non autorizzata di un *computer*;
4. utilizzazione non autorizzata di un programma informatico protetto.

Tra le previsioni di reato presenti nella lista facoltativa, solo quella relativa allo spionaggio informatico può trovare una tutela minima all'interno del codice penale italiano. Il Legislatore non ha voluto creare una norma esplicita per assicurare una tutela specifica per lo spionaggio informatico, tuttavia si può fare riferimento alle norme già presenti nel codice penale italiano, che abitualmente si applicano a quelle fattispecie, ossia alle norme che regolano le ipotesi di spionaggio industriale o scientifico. Occorrerà pertanto, osservare quanto previsto degli Artt. 621 - 623 del codice penale. Queste norme sono ricomprese nella Sezione V «Delitti contro l'inviolabilità dei segreti» del Capo III, dedicato ai delitti contro la libertà individuale del Titolo XII. L'art. 621 c.p. è stato modificato proprio dalla Legge n. 547/1993 che ha introdotto un nuovo comma, nel quale viene specificato che la rivelazione di documenti segreti riguarda anche i documenti informatici. L'art. 623 c.p. contiene invece disposizioni specifiche in materia di spionaggio industriale e scientifico. Nell'articolo non si fa esplicito riferimento a beni informatici ma, secondo la dottrina è applicabile ai dati e ai programmi che possono definirsi un'invenzione scientifica o una applicazione industriale. In mancanza di tali requisiti, si potrà applicare all'autore del reato solo l'art. 622 c.p. "Rivelazione del segreto professionale", ossia si avrà una diversa configurazione di reato. Da quanto riportato si può osservare che buona parte dei principi contenuti nella Raccomandazione del Consiglio d'Europa del 1989 sono stati recepiti dall'ordinamento penale italiano, anche se l'adeguamento normativo

proposto dalla Raccomandazione si è verificato con notevole ritardo rispetto agli altri stati membri dell'Unione Europea.

Rimangono tuttavia ad oggi prive di sanzione penale alcune figure criminose di rilievo, come ad esempio quelle previste nella lista facoltativa nonché l'ipotesi di furto informatico, al di là dei casi che possono essere ricompresi nella fattispecie generale regolata dall'art. 624 c.p.[83].

Al riguardo, è auspicabile un intervento da parte del Legislatore per colmare lacune legislative ed assicurare una tutela completa in materia di crimini informatici.

[83] E. GIANNANTONIO, *Manuale di diritto dell'informatica*, Cedam, Padova, 1994, 419 e ss.; C. SARZANA, *Informatica e diritto penale*, Giuffrè Editore, Milano, 1994. Sarzana, in particolare sostiene che la costruzione di una fattispecie penale relativa al furto dell'informazione crea notevoli difficoltà e, pertanto, si è cercato di ovviare a questa lacuna in modo indiretto con l'introduzione di una norma che punisce l'accesso non autorizzato.

CAPITOLO III

Pedopornografia online, attività indagine e analisi forense

3.1. Premessa – 3.2. La Legislazione italiana – 3.3. L'attività di contrasto – 3.3.1. Attività di monitoraggio di siti *web* – *3.3.2.* Strumenti di contrasto e monitoraggio delle *chat line* – *3.3.3.* Strumenti di contrasto e *filesharing* – 3.4. L'identificazione delle vittime – 3.5. Analisi dei supporti informatici e attività forense.

3.1. *Premessa*.

Il fenomeno criminale dell'abuso sessuale dei minori è decisamente mutato a seguito della continua evoluzione tecnologica e dell'espansione della Rete internet. Purtroppo sul *web* circolano centinaia di migliaia di immagini e video pedo-pornografici, molti dei quali facilmente accessibili a chiunque. La natura complicata e articolata di questa problematica, i diversi livelli interpretativi, rendono particolarmente difficile il lavoro degli operatori impegnati nella valutazione sistematica e nella gestione di queste condotte.

Il fenomeno in questione costituisce, infatti, un evento eterogeneo: diverse sono le cause che possono costruire tale comportamento, differenti sono i contesti in cui ha maggiori possibilità di emergere, molteplici sono gli operatori e le istituzioni coinvolte ma anche gli strumenti e le tecniche utilizzate per il contrasto, diversi sono gli esiti giudiziari ed istituzionali ed, infine, differenti sono gli attori di volta in volta coinvolti e i profili comportamentali ad essi riferibili.

La pornografia infantile racchiude una molteplicità di reati tra loro collegati, quali l'abuso e la corruzione di minori, la loro riduzione in schiavitù[84], unitamente alla produzione, detenzione e diffusione di materiale ottenuto mediante lo sfruttamento di minori di anni diciotto.

Il primo problema che si pone rispetto alla pornografia infantile, è la sua definizione. Non è facile a volte distinguere, a meno che non si sia in presenza di immagini fortemente esplicite, tra una fotografia pornografica ed una non pornografica. L'immagine osservata deve pertanto essere sempre contestualizzata. Per stabilire delle caratteristiche significative e universali mediante le quali riconoscere materiali inerenti alla pornografia minorile a partire dal 1999 lo

[84] Quando si tratta di minori degli anni 14, art. 600 *bis* C. P., e Legge 15 febbraio 1996, n. 66 sulla violenza sessuale.

Standing Working Group on Offenses Against Minors dell'Interpol ha fornito una prima definizione "*Child pornography is the consequence of the exploitation or sexual abuse perpetrated against a child. It can be defined as any means of depicting or promoting sexual abuse of a child, including print and/or audio, centered on sex acts or the genital organs of children*" seguita l'anno successivo dalla definizione fornita dall'ONU nella Convenzione sui diritti del fanciullo che stabilisce "*per pornografia rappresentante bambini si intende qualsiasi rappresentazione, con qualsiasi mezzo, di un bambino dedito ad attività sessuali esplicite, concrete o simulate o qualsiasi rappresentazione degli organi sessuali di un bambino a fini sopratutto sessuali*"[85]. L'elemento principale di analisi riguarda dunque tutti quegli aspetti di sessualità esplicita che coinvolgono i minorenni; proprio per la difficoltà di definizione univoca di materiale pornografico e pedofilo, può trattarsi di fotografie, filmati, o anche di immagini modificate e costruite al *computer*: è questo il caso della pedo-pornografia virtuale[86] che la Legge 6 febbraio 2006 n. 38, modificando la Legge n. 269/98, ha introdotto tra le nuove fattispecie di reato. Il primo Paese europeo a introdurre una disciplina penale per la pornografia minorile è stata l'Inghilterra[87], oggi *regolamentata dal Sexual Offences Act* del 2003[88], ed anche la prima nazione a prevedere l'incriminazione della c.d. "*pedopornografia virtuale*" con il *Criminal Justice and Public Order Act* del 1994. Le macchine fotografiche digitali, hanno dato a chiunque la possibilità di produrre immagini digitali che per loro natura non necessitano di essere sviluppate e conseguentemente spesso riprodotte da terzi, risultando invece immediatamente fruibili e utilizzabili *online* dall'autore; viene a mancare, in questo modo, un primo possibile filtro di controllo sul materiale prodotto e diviene molto più difficile risalire all'identità dei minori ritratti nelle foto o nei filmati. Detto materiale ha normalmente tre possibili origini:

- **Produzione amatoriale**: si tratta di bambini fotografati dal pedofilo durante le sue attività di molestia, nell'ambito famigliare o successivamente all'adescamento, in altri luoghi;

---

[85] Protocollo opzionale alla Convenzione sui diritti del fanciullo concernente la vendita di bambini, la prostituzione dei bambini e la pornografia rappresentante bambini, New York (USA) 25 maggio 2000, art. 2 comma c.

[86] Legge 6 febbraio 2006 n. 38, art. 4, *(Pornografia virtuale).* Le disposizioni di cui agli articoli 600 *ter* e 600 *quater* si applicano anche quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse, ma la pena e' diminuita di un terzo.

[87] Si tratta del Protection of Children Act del 1978.

[88] Disponibile all'URL: http://www.legislation.gov.uk/ukpga/2003/42/contents.

- **Produzione professionale**: è frutto dell'attività di vere e proprie organizzazioni criminali che operano prevalentemente in Paesi con alto tasso di disagio minorile e di povertà. Il materiale fotografico viene collocato su siti *web* specializzati e venduto direttamente *online*;
- **Pseudo fotografie**: vengono utilizzati alcuni *software* per creare immagini di bambini inesistenti (o artefatti), impegnati in comportamenti esplicitamente sessuali, che sono talvolta indistinguibili dalle immagini di bambini reali[89].

Lo studio del fenomeno dello sfruttamento ed abuso sessuale dei minori rappresenta una realtà poco chiara: gran parte degli episodi di abuso sui minori, purtroppo, per diversi motivi, non vengono denunciati e pertanto sfuggono a alle rilevazioni statistiche. Pertanto i dati emergenti dall'analisi delle segnalazioni che giungono all'Autorità Giudiziaria non possono essere rappresentative dell'intero fenomeno. Per tali motivi, sempre la Legge n. 38 del 2006, allo scopo di contrastare più efficacemente questi crimini ha istituito presso il Servizio Polizia Postale e delle Comunicazioni il Centro Nazionale per il Contrasto alla Pedo-pornografia Online (C.N.C.P.O.)[90]: questa struttura, inaugurata l'1 febbraio 2008, ha il compito di raccogliere segnalazioni ed informazioni sui siti di natura pedo-pornografica, sui nominativi dei gestori e dei beneficiari degli stessi e, quando possibile, di favorire la cooperazione internazionale con le altre forze di polizia impegnate nella lotta alla pedo-pornografia *online*.

Allo stesso modo, la Legge n. 172 dell'1 ottobre 2012, che ha ratificato la convenzione di Lanzarote, ha istituito presso la Presidenza del Consiglio dei Ministri, Dipartimento per le Pari Opportunità, l'Osservatorio per il contrasto della pedofilia e della pornografia minorile, che svolge numerose attività di carattere tecnico e scientifico dirette a conoscere il fenomeno dell'abuso e dello sfruttamento sessuale sui minori e delle relative azioni di prevenzione e contrasto che vengono attuate sia in ambito nazionale sia internazionale.

Ancora oggi, le difficoltà da superare risultano essere tante, e la strada da percorrere molto lunga, a causa delle difficoltà poste in essere dalla trans nazionalità del fenomeno criminale della pedopornografia *online*.

---

[89] Si tratta qui della fattispecie di reato di "pedopornografia virtuale", introdotta dalla Legge 6 febbraio 2006 n. 38.

[90] http://www.poliziadistato.it/articolo/23399/.

L'adozione della direttiva 2011/93/UE[91] da parte del Consiglio UE, che doveva essere recepita dai ventisette Stati membri entro il 18 dicembre 2013, recepita tuttavia dallo Stato Italiano con il D.Lgs. 4 marzo 2014 n. 39, rappresenta un ulteriore passo in avanti nel processo di armonizzazione delle normative penali degli Stati membri in tema di adescamento, abuso e sfruttamento sessuale dei minori, stabilendo norme minime relative alla definizione dei suddetti reati e sanzioni. Per quanto concerne i reati sessuali commessi tramite le nuove tecnologie dell'informazione, merita attenzione la previsione contenuta nell'art. 25 della direttiva 2011/93/UE nella quale si definiscono i metodi per impedire la visione dei siti *web* che contengono o diffondono materiale pedo-pornografico, obbligando gli Stati membri ad adottare le misure necessarie per la rapida rimozione delle pagine *web* che contengono o diffondono tale materiale illecito, ospitate su *server* ubicati nel loro territorio e ad attivarsi per ottenere la rimozione di dette pagine qualora le stesse siano ospitate fuori dal loro territorio. Il medesimo articolo, inoltre, nel secondo comma, prevede la possibilità per gli Stati membri di adottare misure per bloccare l'accesso da parte degli utenti della rete presenti nel loro territorio ai siti *web* che contengono e diffondono detto materiale[92].

3.2. *La legislazione italiana*.

Il primo intervento legislativo teso a disciplinare il reato della pedofilia è contenuto nella Legge 15 febbraio 1996 n. 66, titolata *Norme contro la violenza sessuale*, Legge che ha introdotto nel Codice Penale gli Artt. 609 *bis* e seguenti[93]; tuttavia tale norma, non presenta aspetti di particolare rilievo, nonostante preveda un aggravamento delle pene per il reato di violenza compiuta in danno di un minore, poiché non si configura quale norma mirata a contrastare specificatamente

[91] La direttiva 2011/93/UE sostituisce la decisione quadro 2004/68/GAI del Consiglio d'Europa, relativo alla lotta contro lo sfruttamento sessuale dei bambini e la pornografia infantile, quest'ultima rappresentava per l'Unione solo un primo passo nella lotta all'abuso e allo sfruttamento sessuale dei minori e prevedeva un livello minimo di armonizzazione delle legislazioni nazionali, stabilendo disposizioni comuni in materia di criminalizzazione, sanzioni, circostanze aggravanti, assistenza alle vittime e giurisdizione.

[92] Direttiva 2011/93/UE del Parlamento Europeo e del Consiglio del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio, art. 25.
http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:32011L0093.

[93] Si tratta, nello specifico dei seguenti articoli: art. 609 *bis*, Violenza sessuale; art. 609 *ter* Violenza sessuale aggravata; art. 609 *quater*, Atti sessuali con minorenne; art. 609 *quinquies*, Corruzione di minorenne; art. 609 *sexies*, Ignoranza dell'età della persona offesa; art. 609 *octies*, Violenza sessuale di gruppo; art. 609 *decies*, Comunicazione dal tribunale per i minorenni.

il fenomeno criminale dello sfruttamento dei minori di anni diciotto.

Di maggior importanza e portata risulta essere invece la Legge 3 agosto 1998 n. 269 *contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù*: essa nasce con l'obiettivo di dare attuazione alla Convenzione stipulata il 20 dicembre 1989 a New York, ed è la prima e fondamentale norma di riferimento all'interno del nostro ordinamento, nell'ambito del contrasto al fenomeno criminoso dello sfruttamento dei minori. Questa Legge ha introdotto nel nostro Codice Penale nuovi illeciti in materia sessuale previsti nell'art. 600 *bis* riguardante la "*prostituzione minorile*", nell'art. 600 *ter* "*pornografia minorile*", nell'art. 600 *quater* Detenzione materiale pedo-pornografico, nell'art. 600 *quinquies* Iniziative turistiche volte allo sfruttamento della prostituzione minorile. Altro segnale forte deriva dal fatto che queste nuove fattispecie di reato siano inserite nel Capo del Codice Penale dedicato ai "delitti contro la libertà individuale"; secondo alcuni autori, con questa Legge, diversamente a quanto avvenuto in precedenza con altre norme, sono state previste delle fattispecie penali ontologicamente autonome[94], ove i soggetti passivi sono appunto i minori d'età.

La Legge n. 269/1998 è stata successivamente aggiornata dalla Legge n. 38 del 6 febbraio 2006 recante il titolo "*Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedo-pornografia anche a mezzo internet*" che modifica e aggiorna la precedente normativa adeguandola ai successivi accordi internazionali nonchè alla decisione quadro europea.

La Legge n. 38/2006, infatti, viene promulgata successivamente alla decisione quadro 2004/68/GAI del 22 dicembre 2003 con la quale l'Unione Europea ha stabilito le regole per una efficace lotta contro lo sfruttamento sessuale dei bambini e la pornografia infantile al fine di superare le discordanze nelle impostazioni giuridiche degli Stati membri e di contribuire allo sviluppo di una cooperazione efficace. In particolare la decisione stabiliva che ciascun Stato dovrà prevedere sanzioni "*effettive, proporzionate e dissuasive*" contro gli autori dei reati in questione, nonché sanzioni di natura penale e non da applicare anche alle persone giuridiche coinvolte. Alla eccessiva diffusione del fenomeno della pedopornografia *online*, il Legislatore è intervenuto predisponendo una legge *ad hoc* che punisce con pene severe coloro che commettono reati di abuso sessuale e

[94] O. FORLENZA, Un pacchetto di misure a tutto campo per una legge dalle grandi aspettative, in Guida al Diritto, fascicolo 33, 1998, pag. 40 e segg.

sfruttamento dei minori, coloro che si procurano o detengono "materiale pornografico realizzato mediante lo sfruttamento di minori di anni diciotto" ed infine chiunque partecipi a viaggi finalizzati alla fruizione di attività di prostituzione in danno di minori.

In questa norma viene ampliato l'ambito di applicazione e della tutela contro il fenomeno della pedo-pornografia e viene introdotta per la prima volta nel Codice Penale italiano una nuova fattispecie di reato, quella della pedo-pornografia virtuale[95]. Le pene e le sanzioni previste dagli Artt. 600 *ter* e 600 *quater* del Codice Penale riguardanti la detenzione e la divulgazione di materiale pedo-pornografico si possono applicare, anche se diminuite di un terzo, anche alle immagini virtuali, cioè a quelle immagini realizzate ritoccando con tecniche e programmi di elaborazione grafica preesistenti immagini raffiguranti minori o parti di esse, facendo apparire come vere situazioni non reali.

Viene introdotto per la prima volta anche per i reati di detenzione e diffusione di materiale pedo-pornografico il concetto di "*ingente quantità*": infatti, negli Artt. 600 *ter* e 600 *quater* c.p. viene previsto un aumento della pena fino a due terzi ove il materiale pedopornografico detenuto o ceduto sia di quantità ingente.

La presente norma prevede infine tutta una serie di obblighi e responsabilità a carico dei fornitori di servizi di rete, *service providers*[96] e *access providers*[97]: in particolare, per i primi, l'obbligo di segnalare al "Centro Nazionale per il Contrasto alla Pedo-pornografia sulla rete internet" i soggetti e le imprese che distribuiscono o commercializzano materiale ottenuto mediante lo sfruttamento di minori fornendo ogni informazione utile alla loro individuazione; per i secondi impedire l'accesso ai siti segnalati utilizzando idonei strumenti di filtraggio.

E' ovvio, quindi che queste previsioni siano del tutto giustificate ed opportune, perché riescono a colmare alcune gravi lacune che la Legge n. 269/1998 aveva manifestato proprio in ordine ai soggetti appena indicati, al punto che la giurisprudenza precedente alla novella del 2006 aveva escluso ogni responsabilità in capo agli stessi, per omesso controllo, su quanto contenuto nei

---

[95] L'Inghilterra è stata la prima nazione ad introdurre nel proprio Codice Penale la fattispecie di reato della pedopornografia virtuale con il *Criminal Justice and Public Order Act* del 1994.

[96] Termine mutuato dalla lingua inglese che, tradotto letteralmente in italiano, significa "fornitore di servizi internet", abbreviato in sigla ISP. L'ISP, una volta avvenuto l'accesso alla rete, consente all'utente di compiere determinate operazioni, quali la gestione della posta elettronica, la suddivisione e la catalogazione delle informazioni ed il loro invio a soggetti determinati.

[97] L'*access provider*, consente all'utente l'allacciamento alla rete telematica.

siti Internet interessati. Il 23 ottobre 2012 è entrata in vigore la Legge italiana di ratifica della Convenzione del Consiglio d'Europa sulla protezione dei bambini contro l'abuso e lo sfruttamento sessuale, anche conosciuta come "Convenzione di Lanzarote"[98]. Detta Convenzione rappresenta il primo strumento giuridico internazionale ad imporre agli Stati firmatari di prevenire e criminalizzare ogni forma di abuso e sfruttamento sessuale sui minori, allo scopo di elevare lo standard di tutela. Tra le numerose novità introdotte dalla Legge 1 ottobre 2012 n. 172, le principali riguardano l'introduzione di una nuova fattispecie di reato di "adescamento di minorenni", che consiste nel conquistare conquistare la fiducia di un minore di anni sedici attraverso artifici, lusinghe o minacce posti in essere anche mediante l'utilizzo della rete internet, c.d. "*grooming*", o altri mezzi di comunicazione per commettere reati connessi all'abuso ed allo sfruttamento sessuale dei minori.

Le novità introdotte prevedono anche l'introduzione nel Codice Penale di nuove condotte e un sostanziale aggravamento delle pene per chi compie tali reati, novità che possiamo riassumere come segue:

1. Il nuovo reato di "adescamento di minorenni" anche a mezzo internet finalizzato all'abuso ed allo sfruttamento sessuali dei minori, previsto dall'art. 609 *undecies* del Codice Penale;
2. Nuove condotte ad integrazione del reato di "prostituzione minorile" quali il reclutamento, gestione e controllo della prostituzione di un minore di anni diciotto;
3. Istigazione a pratiche di pedofilia e pedopornografia previsto dall'art. 414 *bis* del Codice Penale, che consiste nell'istigare o promuovere pubblicamente, con qualsiasi forma di espressione e con qualsiasi mezzo, a commettere in danno di un minorenne uno dei delitti previsti dagli artt. 600 *bis*, 600 *ter*, 600 *quater*, 600 *quinquies* C.P. e dagli artt. 609 *bis*, 609 *quater* e 609 *quinquies*;
4. Modifica della fattispecie di "corruzione di minorenne" previsto dall'art. 609 *quinquies* del Codice Penale ed aggravamento delle pene per chi compie atti sessuali alla presenza di un minore di anni quattordici al fine di farlo assistere;

[98] La Convenzione di Lanzarote è stata ad oggi firmata da 41 Stati e finora ratificata da 10 Paesi membri. L'Italia ha sottoscritto la Convenzione in data 7 novembre 2007.

5. Raddoppio dei termini di prescrizione per i reati di abuso sessuale e sfruttamento dei minori.

La Convenzione di Lanzarote, per contrastare il turismo sessuale che coinvolge bambini, ha previsto inoltre che per questo tipo di fenomeno criminale gli autori possano essere perseguiti in Italia anche se il reato è stato commesso all'estero, oltre a istituire dei programmi di sostegno alle vittime.

Infine, il recepimento della Convenzione in parola da parte di molti degli Stati sottoscrittori è la dimostrazione dell'inevitabile ed incessante processo di integrazione degli ordinamenti giuridici.

3.3. *L'attività di contrasto*.

La Legge 3 agosto 1998 n. 269, "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù" che, come affermato nel paragrafo precedente, costituisce la prima norma di riferimento nel contrasto alla pedopornografia, all'art. 14 affida alla Polizia delle Telecomunicazioni una specifica competenza nell'attività di indagine e repressione del fenomeno criminale inerente lo sfruttamento sessuale dei minori sulla rete geografica internet. Così come la successiva Legge 6 febbraio 2006 n. 38, affida al Centro Nazionale per il Contrasto della Pedopornografia sulla rete Internet[99] istituito presso il Servizio Polizia Postale e delle Comunicazioni di Roma un ruolo importante e strategico di raccolta delle segnalazioni provenienti dalle altre Forze di Polizia anche straniere, e di coordinamento dell'attività di indagine e contrasto.

Il fatto che la Legge n. 269/1998 abbia demandato alla competenza esclusiva della Polizia delle Telecomunicazioni la possibilità di attivare siti civetta su Internet, realizzare o gestire aree di comunicazione o di scambio tramite *chat* o *email*, con la partecipazione alle stesse di agenti sotto copertura, evidenzia con particolare significatività il ruolo primario e fondamentale che riveste la Polizia di Stato, ed in particolare la Polizia Postale e delle Comunicazioni, nella lotta e nel contrasto di questo odioso quanto terribile fenomeno criminale.

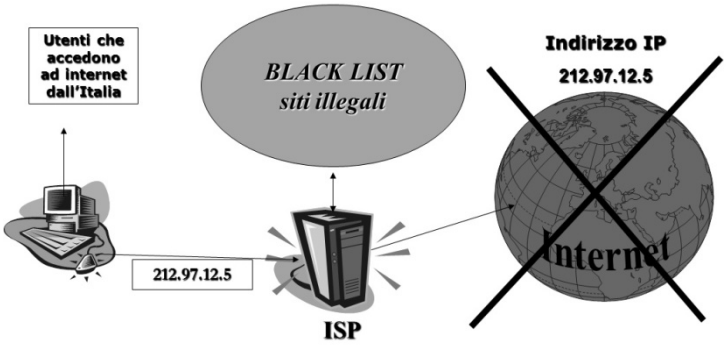
[99] Centro Nazionale per il Contrasto della Pedopornografia Online (C.N.C.P.O.) istituito dall'art. 19 della Legge 6 febbraio 2006 n. 38 presso il Servizio Polizia Postale e delle Comunicazioni di Roma.

3.3.1. *Attività di monitoraggio dei siti web*.

A fini preventivi la Polizia Postale e delle Comunicazioni e le altre Forze di Polizia svolgono da sempre un'intensa attività di monitoraggio del *web*, delle *chat line*, dei *newsgroup*, etc.: di fatto gli investigatori agiscono come delle vere e proprie pattuglie telematiche che, analogamente alle automobili delle Forze di Polizia che presidiano quotidianamente il territorio, pattugliano il cyberspazio[100].

L'attività di monitoraggio ha luogo normalmente su iniziativa degli investigatori, o nell'ambito di una più ampia attività di monitoraggio coordinata a livello nazionale dal Servizio Polizia Postale e delle Comunicazioni che spesso coinvolge tutti gli Uffici periferici per determinati periodi con turnazioni H24.

Questo monitoraggio della rete internet può avvenire anche a seguito di una o più segnalazioni giunte dalla Procura delle Repubblica, dall'Interpol, da altre Forze di Polizia, dalle Associazioni attive nel contrasto del fenomeno criminale della pedo-pornografia *online* o da singoli cittadini che, personalmente o mediante l'invio di *email*, segnalano la presenza *online* di siti contenenti immagini e/o video di natura pedo-pornografica. Successivamente gli indirizzi telematici (*URL*)[101] di tutti i siti *web* positivi, individuati nell'ambito delle attività di monitoraggio o segnalati, vengono così come previsto dalla normativa vigente inviati al Centro Nazionale per il Contrasto alla Pedo-pornografia Online e inseriti in uno speciale *database* dal quale deriva un'apposita "*black list*" periodicamente inviata a tutti gli Internet Service Provider operanti sul territorio nazionale al fine di impedire, con l'utilizzo di appositi sistemi di filtraggio, l'accesso a tali siti illeciti da parte degli utenti della rete.



[100] Cyberspazio è il dominio caratterizzato dall'uso dell'elettronica e dello spettro elettromagnetico per immagazzinare, modificare e scambiare informazioni attraverso le reti informatiche.

[101] *Uniform Resource Locator* (in acronimo URL), nella terminologia delle telecomunicazioni e dell'informatica, è una sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa internet, tipicamente presente su un *host server*, rendendola accessibile ad un *client* che ne faccia richiesta attraverso l'utilizzo di un *web browser*.

Alla fine di questa procedura i siti *web* illegali individuati e presenti nella *black list* non saranno più raggiungibili dai navigatori della Rete internet presenti all'interno del territorio nazionale; sui loro schermi, al posto dell'*homepage*, comparirà di norma la seguente schermata che ha il compito di avvisare l'utente che ha tentato consapevolmente o meno di accedervi, dell'avvenuto oscuramento e delle relative motivazioni.


Ministero dell'Interno
Dipartimento della Pubblica Sicurezza
Servizio Polizia Postale e delle Comunicazioni

STOP !!

PAGINA INTERDETTA DAL CENTRO NAZIONALE PER IL CONTRASTO ALLA PEDOPORNOGRAFIA SULLA RETE INTERNET

Il tuo browser sta tentando di raggiungere un sito Internet contenente immagini e filmati pedopornografici.
La detenzione, la distribuzione, la produzione, la commercializzazione di tale materiale prevedono l'applicazione di gravi sanzioni in base alla legge penale italiana e sono perseguibili anche ad opera di forze di polizia estere.

Nessun dato relativo al tuo ip address od altra traccia utile ad identificarti verrà registrato.

L'inibizione dell'accesso a questo sito è prevista dalla legge n. 38/2006 ed è stata operata al fine di impedire la commissione e la documentazione di violenze sessuali a minori degli anni diciotto. Questo servizio di protezione della navigazione sulla rete Internet è predisposto grazie alla collaborazione tra il "Centro Nazionale per il Contrasto alla Pedopornografia sulla rete Internet" e gli Internet Service Provider italiani.

Your browser is trying to contact an Internet site that is used in connection with distribution of photos depicting sexual abuse of children. This is a criminal offence in accordance with the italian penal code.

No information about your ip address or any other information that can be used to identify you will be stored when you this page is displayed.

The purpose of blocking access to these pages is only to prevent the commission of criminal dissemination of documented sexual abuse, and to prevent the further exploitation of children who have already been abused and photographed. This is a prevention service provide from italian Internet Service Provider and the italian "National Centre for Combating On-line child pornography".

C.I.R.C.A.M.P.
Cospol Internet Related Child Abusive Material Project

Il filtro antidistribuzione del materiale pedopornografico è parte dell'iniziativa "CIRCAMP" (Cospol Internet Related Child Abusive Material Project).
Tale progetto è stato avviato dalla "Task-Force" dei capi delle polizie europee per combattere la criminalità organizzata che gestisce il commercio di materiale prodotto mediante l'utilizzo sessuale dei minori.
The Child sexual abuse anti-distribution filter is part of the "CIRCAMP" (Cospol Internet Related Child Abusive Material Project). The project is initiated by the european police chief task-force - aimed at combating organized criminal group behind commercial sexual exploitation of children.

Rispetto allo specifico "ambito" Internet di volta in volta interessato, emerge che la percentuale più elevata di segnalazioni si riferisce a siti *web* (86,5%); rilevanti sono anche i valori riconducibili all'attività di *file sharing* (6,4%) ed alle *chat line* (4%).

Tipologia di ambiente Internet segnalato
Periodo: luglio 2007 – febbraio 2010
Valori percentuali

Ambiente	%
Sito web	86,5
File sharing	6,4
Chat	4,0
E mail	2,0
Indicazione assente	0,4
Newsgroup	0,3
Blog	0,2
Forum	0,2
Totale	100,0

Fonte: Telefono Azzurro su dati Hot114, 2010

In tutti i casi l'attività di monitoraggio è finalizzata ad individuare e ad accertare l'effettiva presenza di siti *web* che offrono immagini e/o video ottenuti mediante lo sfruttamento sessuale di minori.

I siti *web* individuati diventano oggetto di indagini mirate ad accertare dove gli stessi siano fisicamente ubicati e quali risulti essere la persona fisica o la

società che li gestisce e se gli stessi risultino essere ubicati all'interno del territorio italiano. Nella realtà operativa questi siti illegali sono quasi sempre ubicati all'estero, in particolare in nazioni extra europee ove l'allarme sociale è decisamente più contenuto rispetto a quanto non sia in Europa e, principalmente, ove la legislazione penale in materia risulta essere estremamente carente.

La ricerca dei beneficiari finali degli enormi flussi di denaro che vengono realizzati dai gestori di detti siti *web* illeciti, ha sempre suscitato particolare interesse investigativo. Questo perché spesso i siti che offrono materiale pedopornografico si appoggiano a società di mediazione finanziaria, aventi sede in nazioni extra europee ove è in vigore una normativa fiscale estremamente conveniente e che spesso non offrono alcun tipo di collaborazione giudiziaria e investigativa alle Forze di Polizia straniere, al punto che troppo frequentemente le richieste di assistenza giudiziaria internazionale (c.d. *rogatorie internazionali*) rimangono ignorate, senza alcun tipo di risposta.

Recentemente vi è stata una progressiva diminuzione di segnalazioni di detti siti *web*, a riprova che la continua evoluzione della normativa atta a contrastare questo fenomeno criminale, unitamente ad un controllo sempre più severo ed efficace da parte delle Forze di Polizia, comincia a rappresentare una difficoltà seria per coloro i quali intendono utilizzare il *web* per lo scambio e la diffusione di materiale pedo-pornografico. Tuttavia se da un lato è vero che si è riscontrato un calo significativo di tali segnalazioni, d'altra parte si assiste ad una continua espansione del c.d. *Deep Web*, cioè della parte più sommersa e nascosta della rete geografica internet che comprende l'insieme delle risorse informative non segnalate dai normali motori di ricerca[102].

3.3.2. *Strumenti di contrasto e monitoraggio delle chat line*.

Come già affermato, la Legge n. 269/1998, in relazione all'elevato tecnicismo richiesto dalle attività in Internet e per evitare inutili e costose duplicazioni d'indagini in una materia così delicata e complessa, affida in via esclusiva alla Polizia Postale e delle Comunicazioni alcuni specifici poteri e strumenti investigativi.

In conformità con quanto stabilito dalle normative a contrasto del traffico di

[102] Secondo una ricerca condotta nel 2000 da Bright Panel, un'organizzazione statunitense, il *web* è costituito da oltre 550 miliardi di documenti, mentre il motore di ricerca Google ne indicizza solo 2 miliardi, ossia meno dell'uno per cento (Fonte Wikipedia).

droga e di armi, per il contrasto e la repressione della diffusione d'immagini pedo-pornografiche *online* e del turismo sessuale, viene data facoltà alla Polizia Postale e delle Comunicazioni, previa autorizzazione dell'Autorità Giudiziaria, di:

1. effettuare acquisti simulati di materiale pedo-pornografico;
2. svolgere attività "sotto copertura" durante i monitoraggi e la navigazione *online*;
3. realizzare siti *web* "civetta" per adescare i pedofili ed i "consumatori" di pornografia minorile.

Le più importanti operazioni di contrasto al fenomeno criminale dello sfruttamento sessuale dei minori, hanno avuto origine da attività "sotto copertura" svolte dal personale tecnico della Polizia Postale e delle Comunicazioni talvolta anche con la collaborazione di altre Forze di Polizia nell'ambito delle *chat*. Ciò ha portato a centinaia di perquisizioni in abitazioni ed uffici, nonché all'arresto di parecchie decine di persone. Gli operatori, preventivamente autorizzati dall'Autorità Giudiziaria procedente, assumevano l'identità di minori di giovane età, normalmente tra i 10 ed i 14 anni e, frequentando determinate *chat line*, attendevano di essere contattati ed eventualmente adescati da utenti adulti. Una volta individuati i potenziali "pedofili" l'operatore accertava inequivocabilmente le intenzioni dell'adulto dichiarandosi esplicitamente minorenne e registrando la sessione della *chat* in svolgimento; spesso l'adescatore offriva spontaneamente immagini e/o filmati di natura pedo-pornografica, che l'operatore accettava, e durante il *download* del *file* illecito provvedeva con tecniche idonee a rilevare l'indirizzo IP del mittente. Lo sviluppo dell'indirizzo IP rilevato, associato alla data e all'ora dell'invio, forniva inequivocabilmente il numero dell'utenza di telefonia fissa o mobile utilizzata per lo svolgimento della *chat* e per l'invio del materiale illecito; di qui risultava spesso agevole risalire all'identità dell'utente adescatore. Alla conclusione dell'attività investigativa quest'ultimo veniva indagato ed era richiesto a suo carico un decreto di perquisizione personale e locale, normalmente nella sua abitazione ma non solo, al fine di trovare ulteriori elementi utili per le indagini in corso. Tale perquisizione, inoltre, consentiva di trovare evidenza, sul *computer* dell'indagato, dell'avvenuto invio di materiale di natura pedo-pornografica. L'adescamento *online* in danno di minori è un fenomeno che consiste nel tentativo, da parte di una persona malintenzionata o di

un pedofilo, di avvicinare un bambino o un adolescente per scopi sessuali, conquistandone la fiducia attraverso l'utilizzo della rete internet, in particolare tramite *chat* e *social networks*. Come accennato in precedenza, recentemente è stato introdotto nel nostro Codice Penale il reato di adescamento di minorenni *online*, (c.d. *grooming*), che consiste nel conquistare la fiducia di un minore di età inferiore a sedici anni per scopi sessuali, attraverso artifici, lusinghe o minacce; tale reato si configura anche nel caso in cui l'incontro con il minore non avvenga, essendo sufficiente il tentativo da parte di un adulto di conquistare la fiducia del minore.

Aspetti ricorrenti e comuni messi in atto dall'adulto potenziale abusante durante l'adescamento *online* (*grooming*):

1. Seleziona tra i profili-utenti di una *chat*, *social network*, servizi di *instant messaging*, il target di età e sesso preferiti;
2. Utilizza conversazioni su tematiche banali e tipiche del minore, offrendo disponibilità a rispondere e ad ascoltare;
3. Spesso mente sulla propria età anagrafica;
4. Fa dichiarazioni di trasporto sentimentale;
5. Richiede confidenze sessuali, spesso precedute dalla richiesta di immagini trasgressive;
6. Invia immagini trasgressive sempre più "esplicite", con l'intento di abituare e normalizzare la sessualità adulto/minore agli occhi dello stesso;
7. Talvolta avanza la richiesta di un incontro *offline*;
8. Richiede sempre di mantenere segrete le conversazioni e le immagini inviate.

Tuttavia, non sempre gli adulti interessati sessualmente ai minori li adescano al fine di poterne abusare sessualmente: sono sempre più diffuse forme di abuso che avvengono attraverso l'utilizzo dei nuovi media, quindi senza che, di fatto, vi sia un contatto fisico reale tra adulto e minore, ma che possono comunque avere conseguenze devastanti sulla giovane vittima.

L'abuso perpetrato attraverso le nuove tecnologie costituisce un fenomeno relativamente recente e, conseguentemente, sono poche le ricerche e gli studi effetti e sulle ricadute a lungo termine. In compenso sono presenti molti dati sugli

effetti a breve termine: essi individuano le conseguenze sulle vittime, conseguenze che variano in relazione alle caratteristiche della vittima, all'età, alle forme e alla durata dell'evento traumatico[103].

Fattori di vulnerabilità e caratteristiche delle vittime dell'adescamento on-line

Esistono pochi studi quantitativi su larga scala riguardo la prevalenza dell'adescamento sessuale online. Uno tra gli studi più significativi in questo ambito rimane l'Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study[20] realizzato nel 2004 dal Crimes against Children Research Center, presso l'Università del New Hampshire. Tale studio ha consentito di raccogliere una grande mole di dati provenienti dalle autorità giudiziarie, in merito ai crimini sessuali contro i minori avviati attraverso l'utilizzo dei Nuovi Media.

Di seguito si evidenziano alcuni dati significativi emersi dalla studio:
- il 99% delle vittime aveva un'età compresa tra i 13 e 17 anni;
- nessuna delle vittime aveva un'età inferiore ai 12 anni;
- il 75% delle vittime era di sesso femminile, il 25% maschile;
- il 76% degli abusanti aveva un'età media di 26 anni; il 47% aveva almeno 20 anni in più rispetto all'età delle vittime. La maggior parte degli abusanti non ha nascosto il fatto di essere più vecchio delle vittime e le sue intenzioni;
- il 73% delle vittime ha incontrato offline gli abusanti più di una volta. Di queste, il 13% almeno due volte e il 39% più volte;
- il 50% delle vittime non si percepiva come tale e nutriva forti sentimenti di affetto/amore verso l'adulto;
- il 5% dei casi registrati ha previsto una qualche forma di violenza e il 16% una forma di coercizione da parte dell'abusante.

Aspetti di vulnerabilità:
Sulla base dei risultati di questa ricerca - confermati dall'esperienza maturata in questi ultimi anni e relativa ai casi giunti all'attenzione del CISMAI - è possibile ipotizzare alcune tipologie di minori a rischio per questa forma specifica di abuso:
a) minori con storie di abusi fisici o sessuali e con esiti psicopatologici;
b) minori con problemi di solitudine, depressione, con problemi relazionali e con difficoltà nella relazione con i genitori, che trovano nella Rete uno strumento utile per far fronte ai loro problemi, soprattutto di relazione;
c) minori maschi e femmine omosessuali o con incertezze sulla loro identità sessuale, che utilizzano la Rete per cercare contatti e informazioni su un tema ancora molto stigmatizzato socialmente;
d) minori che - non necessariamente rientrano nelle tipologie precedenti - utilizzano la Rete in modo spregiudicato: caricano online foto di se stessi/e allusive o esplicite sul piano sessuale, accettano di parlare in chat di sesso o avviano sessioni di cyber sex con sconosciuti (anche dietro una ricompensa), ecc.

Il settore dove si manifesta il maggior rischio per i minori è rappresentato dalle *chat line*. Tali strumenti di comunicazione, infatti, implicano la mediazione di un *computer* tra i due interlocutori, consentono talvolta rapporti umani estremamente intimi, neutralizzando anche alcuni gap di età e culturali che normalmente limitano o selezionano le comunicazioni dirette tra minori e adulti. I rapporti telematici non hanno elementi identificativi aggiuntivi (paraverbali, visivi, ecc.) e l'identità dichiarata può essere verosimilmente falsa. La tecnologia della *chat* offre quindi una certa facilitazione ai pedofili nella fase di contatto iniziale con la possibile vittima e consente loro forme di molestia di tipo verbale e tentativi di incontro al di fuori della Rete.

3.3.3. *Strumenti di contrasto e filesharing.*

Per *file sharing* s'intende la condivisione di *file* all'interno di una rete di *computer* collegati tra loro, che comporta appunto una messa in comune di risorse

[103] *The Online Project Children sexually abused* via IT, Linda Jonsson, Christina Warfvinge, Lena Banck – BUP Elephanten, SE, 2009.

attraverso una rete *client-server* oppure *peer-to-peer*, tramite *software* dedicati.

A differenza del sistema *client-server* ove tutti gli utenti connessi scaricano il materiale ricercato dagli stessi *server*, nel sistema *peer-to-peer* tutti i *computer* connessi alla stessa rete di scambio sono equivalenti e paritari ed agiscono contemporaneamente sia da servente che da cliente verso gli altri terminali cui sono connessi.

Uno dei programmi di *file sharing* più diffuso in Italia è *eMule*, *software* per la condivisione di *file*[104] che si appoggia alle reti *peer-to-peer eDonkey* e *Kad*; con il sistema di condivisione di *eMule*, un utente, nel momento stesso in cui cerca e scarica i *file* desiderati dai vari *server* connessi alla rete, mette contestualmente a disposizione di tutta la rete i *file* scaricati contenuti nella cartella, o nelle cartelle, poste in condivisione presenti nel proprio *hard disk*[105].

Quindi, il *file sharing* è quel sistema che permette a più utenti di condividere tra loro, e all'interno di tale piattaforma, immagini e video, programmi e ogni tipo di informazioni presenti e registrati sulla parte di *hard disk* posta in comune dall'utente.

In considerazione della facilità d'utilizzo e dei costi esigui, questo sistema di condivisione risulta essere molto diffuso tra gli utenti della Rete internet per lo scambio di programmi, film, brani musicali, ecc..

Tali programmi, del tutto leciti, per l'anonimato dei soggetti che agiscono, per la transnazionalità degli stessi e per la conseguente impossibilità da parte delle Autorità Giudiziarie di tutto il mondo di intervenire in maniera concreta ed efficace per bloccare detti scambi, divengono veri e propri canali preferenziali capaci di agevolare condotte illecite, soprattutto la diffusione di immagini e video di natura pedo-pornografica.

Il Legislatore italiano per contrastare e punire le condotte di diffusione di materiale pedopornografico, che trovano terreno fertile sulla Rete ed in particolare per mezzo dei programmi di *file sharing*, ha introdotto, con la Legge n. 269/1998, l'art. 600 *ter* che al comma 3 punisce chiunque "con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, diffonde o pubblicizza materiale pornografico di cui al primo comma, ovvero distribuisce o divulga notizie o informazioni

---

[104] Il termine *file*, traducibile dall'inglese come "archivio", viene utilizzato per definire un contenitore d'informazioni in formato digitale presente su un supporto digitale di memorizzazione opportunamente formattato in un determinato *file system*.

[105] *Hard Disk*, traducibile dall'inglese come "disco rigido", è un dispositivo di memoria di massa di tipo magnetico che utilizza uno o più dischi magnetizzati per l'archiviazione dei dati. Si tratta di una periferica di *input/output* presente nella maggior parte dei *computer* ed anche in altri dispositivi elettronici.

finalizzate all'adescamento o allo sfruttamento sessuale di minori di anni diciotto" e l'art. 600 *quater* che punisce "Chiunque, al di fuori delle ipotesi previste nell'articolo 600 *ter*, consapevolmente si procura o detiene materiale pornografico realizzato utilizzando minori (…). La pena è aumentata in misura non eccedente i due terzi ove il materiale detenuto sia di ingente quantità".

L'attività investigativa e di contrasto in quest'ambito informatico verte principalmente nell'attività sotto copertura e nella ricerca del materiale illecito posto in condivisione dagli utenti di questi programmi di *file sharing*. Al fine di identificare la reale identità di questi ultimi, bisogna per prima cosa individuare l'indirizzo IP[106] utilizzato dagli stessi per accedere al *web*; questo processo è più semplice quando sono gli stessi utenti ad effettuare il *download,* cioè lo "scarico" sul proprio *computer*, del materiale posto in condivisione dall'investigatore che opera sotto copertura. Egli provvede quindi a redigere un elenco degli indirizzi IP associati alla data e all'ora della rilevazione. Individua, tra questi, quelli assegnati dagli *Internet Service Provider* operanti nel territorio nazionale, ai quali previa notifica del necessario decreto di acquisizione dati emesso dalla Procura operante, ai sensi dell'art. 256 del Codice di Procedura Penale, verrà richiesta la cosiddetta "*risoluzione*" dell'indirizzo IP, cioè l'individuazione dell'intestatario dell'utenza fissa o mobile utilizzata per effettuare il *download* attenzionato. Individuato l'utente, normalmente a conclusione dell'attività investigativa sotto copertura, si effettua una perquisizione dei luoghi ove è avvenuta la condotta criminosa.

Mentre, gli indirizzi IP rilevati afferenti ad *Internet Provider* stranieri verranno comunicati per il tramite di Europol o Interpol alle Forze di Polizia straniere competenti per territorio.

3.4. *L'identificazione delle vittime*.

L'identificazione delle giovani vittime abusate e sfruttate nelle immagini e nei filmati pedo-pornografici rappresenta il traguardo più difficile e la sfida più importante per le Forze di Polizia.

Le immagini pedo-pornografiche rappresentano la registrazione visiva della violenza sessuale subita da un minore e costituiscono la prova di un crimine orrendo: i minori che appaiono in queste immagini e nei filmati sono sottoposti ad azioni abusanti, degradanti, di natura criminale. Come affermato anche dalla

[106] Indirizzo IP (dall'inglese *Internet Protocol address*) è un valore numerico che identifica univocamente un dispositivo collegato alla rete geografica Internet.

Legge che ha recepito nel nostro ordinamento la Convenzione di Lanzarote, l'identificazione delle vittime risulta essere di notevole importanza per porre fine ad abusi e violenze che potrebbero essere ancora in corso. L'analisi delle immagini e dei video in questione, opportunamente e accuratamente analizzate, possono talvolta consentire di ricostruire la storia dell'abuso e anche di localizzare territorialmente l'ambito nel quale è avvenuto.

Purtroppo dei minori ritratti in centinaia di migliaia di immagini e filmati presenti in Rete solo una minoranza viene compiutamente identificata e posta sotto tutela. La diffusa criticità di questo fenomeno criminale emerge anche sotto questo aspetto, a causa della difficoltà di assegnare una titolarità territoriale delle indagini da compiere sulle specifiche immagini, cioè di individuare la nazione ove le stesse siano state effettivamente realizzate. Tutte le immagini pedo-pornografiche rilevate e raccolte dovrebbero essere analizzate per identificare le vittime raffigurate e assicurare alla giustizia i responsabili degli abusi. Purtroppo solo una minima parte delle immagini analizzate contiene tracce visive che ne consentano una georeferenziazione almeno parziale: si pensi ad esempio a libri o a poster presenti sullo sfondo, contenenti dei riferimenti linguistici o spazio temporali. Alcune immagini possono contenere più informazioni rispetto ad altre, aumentando così le possibilità di giungere all'identificazione dei minori coinvolti: è il caso dei "metadati"[107] contenuti nel *file* digitale della fotografia che riportano, pur senza certezza di riscontro, la data e l'ora dello scatto o delle riprese, il modello della macchina fotografica digitale o della videocamera.

Negli ultimi anni l'Interpol ha assunto un ruolo guida e di coordinamento e raccordo, sollecitando tutte le Forze di Polizia ad attivarsi e ad attrezzarsi in termini di risorse tecniche e umane necessarie a quest'ambito investigativo.

Proprio presso il Segretariato Generale dell'Interpol con sede a Lione, un team di investigatori gestisce un *database*[108] internazionale di immagini pedopornografiche denominato ICSE (*International Child Sexual Exploitation*) a cui possono accedere le Forze di Polizia di tutto il mondo per condividere immagini e informazioni. Sono 48 le nazioni al momento collegate a questo *database*, tra le quali l'Italia, attraverso il C.N.C.P.O. (Centro Nazionale per il Contrasto alla Pedopornografia Online). Tale *database* presente *online* dal 2009,

[107] I metadati sono informazioni descrittive sui dati stessi: nel caso delle immagini fotografiche descrivono la data e l'ora dello scatto, la marca ed il modello della macchina fotografica.

[108] Il termine *database* indica un archivio di dati; le informazioni contenute sono strutturate e collegate tra loro secondo un modello logico tale da consentire la gestione efficiente degli stessi e l'interfacciamento con le richieste degli utenti.

interconnesso con il sistema di comunicazione globale denominato I-247, utilizza programmi sofisticati che svolgono una veloce comparativa delle immagini acquisite, cercando collegamenti e/o analogie con le oltre 900.000 immagini già presenti all'interno dell'archivio al fine di individuare eventuali connessioni e corrispondenze tra le vittime raffigurate. Il fatto di poter condividere tale materiale attraverso un'unità centralizzata ed efficiente offre parecchi vantaggi, come quello di riscontrare se altre Forze di Polizia stiano già portando avanti indagini su determinate immagini o filmati, fornendo così un quanto mai opportuno coordinamento ed evitando inutili duplicazioni di indagini e spreco di tempo, ed ottenendo così maggiori informazioni utili alla sua identificazione.

Questo sistema ha consentito al 31 dicembre 2015 di individuare compiutamente l'identità di oltre 8000 minori, vittime di questo fenomeno criminale, appartenenti a circa 50 differenti nazioni, e al conseguente arresto di oltre 3800 adulti abusanti.

3.5. *Analisi supporti informatici e attività forense*.

Con la Legge 18 marzo 2008 n. 48, come si è già detto, è stata ratificata nel nostro ordinamento la Convenzione di Budapest del 23 novembre 2001 sulla criminalità informatica, il primo importante accordo internazionale riguardante i crimini commessi attraverso Internet o altre reti informatiche, avente l'obiettivo di realizzare una politica comune tra gli Stati membri nel contrasto della criminalità informatica. Questa Legge ha introdotto importanti modifiche sia al Codice Penale quanto al Codice di Procedura Penale, le novità più importanti sono sicuramente quelle introdotte al Codice di Procedura Penale negli Artt. 244, 247, 352 e 354, inerenti le perquisizioni, le ispezioni e il sequestro di dati informatici: la Legge di recepimento ha di fatto positivizzato alcune prassi già consolidate in tema di investigazioni informatiche e di *computer forensics*[109].

Comunque, a prescindere dal fatto che si tratti di attività disposte dall'Autorità Giudiziaria oppure intraprese su iniziativa della Polizia Giudiziaria, la Legge in oggetto, come meglio vedremo nei prossimi capitoli, ha introdotto un preciso *modus operandi* da seguire nell'espletare le azioni di accesso al sistema informatico, con particolare riguardo alle "misure tecniche dirette ad assicurare la

[109] La *computer forensics* è l'applicazione del metodo investigativo ai sistemi informatici e ai nuovi media, con particolare attenzione alla conservazione, all'estrazione e alla documentazione del dato informatico al fine di ricavarne informazioni e prove da portare in giudizio.

conservazione dei dati originali e ad impedirne l'alterazione".

Viene in questo modo riconosciuta la natura ontologicamente volatile ed alterabile del dato digitale, sul quale possono talvolta incidere condotte involontarie atte a generare fenomeni di "inquinamento" e la conseguente necessità di adottare delle *best practice*[110] per garantire la genuinità dell'accertamento tecnico. Non si utilizza una singola modalità operativa, ma si rinvia a quelle che saranno considerate nel tempo le migliori pratiche seguite all'interno del panorama scientifico internazionale, affidando all'organo giudicante l'onere di verificare, di volta in volta, la validità dei criteri e delle tecnologie utilizzate. Nella pratica operativa, come previsto dagli Artt. 247 e 354 del Codice di Procedura Penale, gli Ufficiali di Polizia Giudiziaria nel corso della ricerca delle tracce pertinenti al reato, nel caso vi siano i presupposti, provvedono nell'immediatezza ad eseguire una perquisizione informatica dei supporti mediante l'utilizzo di strumenti tecnici quali il *write blocker*[111], un dispositivo *hardware* che, collegato tra il *computer* dell'esaminatore ed il supporto oggetto di investigazione, garantisce l'accesso impedendo elettronicamente qualsiasi scrittura sul supporto stesso.

La perquisizione informatica è volta alla ricerca dei dati, delle informazioni e delle tracce pertinenti al reato contestato all'interno dei supporti informatici sequestrati, adottando le tecniche idonee ad assicurare la conservazione dei dati presenti ed impedendo l'alterazione degli stessi. Si tratta di un'attività particolarmente complessa e delicata che richiede elevate competenze tecniche, dovendo assicurare al processo penale le fonti ed i mezzi di prova delle indagini svolte. A volte accade che durante lo svolgimento di queste operazioni sia possibile imbattersi in tracce relative ad altri reati, persino più gravi rispetto a quelli per cui si sta procedendo, oppure è possibile cogliere in flagranza gli autori dei reati per i quali si procede. Come vedremo meglio negli ultimi capitoli della presente ricerca, la prassi investigativa di fare una copia clone o *bit-stream image*, copia *bit* a *bit* dei supporti magnetici ed elettronici presenti negli elaboratori attenzionati dalle indagini, in modo da cristallizzare il quadro probatorio, così come previsto dall'art. 354 C.P.P. risulta essere molto importante per la conservazione dei dati garantendone la loro inalterabilità. La copia *bit-stream*,

[110] Dall'inglese *best practice*, migliore pratica o buona prassi, si intendono le migliori esperienze operative, o comunque quelle che hanno permesso di ottenere i migliori risultati.

[111] Dispositivo utilizzato dagli investigatori nel campo dell'informatica forense per prevenire eventuali scritture accidentali su *hard disk* o dispositivi di memoria di massa (chiavette USB, schede di memoria, ecc.) oggetto di indagine.

anche detta copia forense, consente di creare un duplicato perfettamente uguale all'originale sia dal punto di vista logico che fisico rispettando l'esatta collocazione dei dati presenti sul supporto originale. Praticamente questo tipo di copia comporta la clonazione di tutte le zone del supporto originale, sia le aree allocate che quelle non allocate e quindi anche di quelle che non contengono alcun dato direttamente visibile all'utente. Gli inquirenti e gli investigatori potranno quindi ricercare le informazioni ed i dati rilevanti per le indagini, anche successivamente, agendo non più sul supporto originale ma sulla sua copia forense. Tutta l'attività di analisi ed estrazione dei dati sarà eseguita esclusivamente sulla copia, garantendo l'assoluta ripetibilità di ogni accertamento svolto, in quanto il supporto originale non verrà mai utilizzato, rimanendo in qualunque momento del processo a disposizione dell'organo giudicante e della difesa per ogni verifica successiva. La norma in esame prevede che gli Ufficiali di Polizia Giudiziaria, "ove possibile", provvedano alla "immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità" delle memorie presenti nell'elaboratore e non solo. Tale previsione, tuttavia, risulta essere spesso alquanto astratta poiché nella realtà operativa la quantità di memorie di massa nella disponibilità dell'indagato e presenti nei luoghi ispezionati, nonché la sempre maggiore capacità di memorizzazione di detti supporti ormai assestati nell'ordine di parecchie centinaia di *gigabyte*[112] o addirittura di alcuni *terabyte*[113], anche nell'eventualità che si utilizzino le migliori tecnologie ad oggi disponibili, richiederebbero tempi lunghissimi per effettuare perfette copie *bit to bit* di tutti i supporti di memoria normalmente presenti sul posto. Nei fatti, quindi, detti supporti di memoria verranno sequestrati dagli investigatori intervenuti e successivamente clonati ed analizzati in ambienti idonei utilizzando specifici *software* come "Encase" della Guidance Software Inc., che, oltre ad eseguire perfette copie forensi dei supporti originali, certificate dalla presenza di un algoritmo *hash*[114] attestante la perfetta corrispondenza della copia all'originale, consente tramite appositi filtri di recuperare dai supporti ogni tipo di informazione utile e talvolta anche *file* precedentemente cancellati o soprascritti.

---

[112] Come già evidenziato nell'introduzione, rappresenta l'unità di misura della quantità di dati che le memorie di massa possono contenere, 1 *gigabyte* corrisponde a circa 1 miliardo di *byte*.

[113] Come già evidenziato nell'introduzione, rappresenta l'unità di misura della quantità di dati che le memorie di massa possono contenere, 1 *terabyte* corrisponde a circa 1000 miliardi di *byte*.

[114] Gli algoritmi di *hash*, in particolare SHA1 e MD5, sono utilizzati nell'ambito dell'informatica forense per validare e firmare digitalmente i dati acquisiti, tipicamente le copie forensi.

CAPITOLO IV

Digital forensics e indagini penali

4.1. Ricerca della *Digital Evidence* - 4.1.1. Indirizzo IP e *file* di *log* - 4.1.2. Ispezione informatica - 4.1.3. Perquisizione Informatica - 4.1.4. Accertamenti urgenti sui luoghi e sequestro - 4.1.5. La disciplina "*search and seizure*" statunitense - 4.1.6. Modalità operative nell'individuazione del dato digitale - 4.2. Acquisizione della *Digital Evidence* - 4.2.1. Il sequestro della *Digital Evidence* - 4.2.2. Sequestro della corrispondenza - 4.2.3. Modalità operative nel sequestro della prova digitale - 4.2.4. La *Remote forensics* - 4.2.5. Intercettazioni telematiche: disciplina italiana e statunitense - 4.2.6. Intercettazioni telematiche.

4.1. *Ricerca della digital evidence.*

4.1.1. *Indirizzo IP e file di log.*

Per gli illeciti commessi sulla Rete Internet, l'attività investigativa si attua attraverso la collaborazione degli *Internet Service Provider*, cioè di tutte quelle società di telefonia fissa e mobile e comunicazione dati che forniscono connettività ai propri utenti. La Polizia Giudiziaria richiede per lo sviluppo delle indagini due tipi di dati digitali: quelli che consentono l'identificazione di un potenziale criminale (Indirizzo IP)[115] e quelli che ne determinano la sua attività *online (file di log)*[116].

L'indirizzo IP si ottiene generalmente attraverso una richiesta da parte dell'Autorità Giudiziaria, ai *providers* o alle società che offrono servizi in Rete, relativi alla creazione di un determinato account di posta elettronica o di un determinato profilo utente, e gli indirizzi IP utilizzati per gli accessi a detta casella di posta elettronica o a detto profilo. Una volta ottenuto tali informazioni, sarà possibile ottenere, dai fornitori di connettività, l'esatta ubicazione dell'intestatario della fattura da cui è avvenuta la connessione. I *file* di *log*, invece, saranno richiesti agli *Internet Service Provider* in base al tipo di esigenza investigativa.

Dette richieste si esplicitano tecnicamente mediante emissione da parte dell'Autorità Giudiziaria procedente, di un Decreto di Acquisizione Dati, solitamente effettuata sotto la forma di "ordine di esibizione di documenti e atti

[115] L'indirizzo IP è un numero che identifica un dispositivo collegato a una rete telematica: esso può essere paragonato a un indirizzo stradale o a un numero telefonico. Il fornitore di connettività, infatti, dato un indirizzo IP e l'ora di accesso a tale indirizzo, è in grado di fornire i dati personali di chi ha sottoscritto il contratto per usufruire dei servizi di connessione.

[116] Il *file* di *log*, invece, è un *file* in cui sono memorizzate le attività compiute da un determinato utente e consente, pertanto, di ricostruire la sua attività all'interno del *computer* in Rete.

rilevanti" ai sensi degli art. 256 c.p.p. e art. 132, comma 1 e 3, D.Lgs. n. 196/03.

La mancanza di una prassi consolidata e di un protocollo operativo ben delineato ovviamente, non aiuta la collaborazione degli *Internet Service Provider*, soprattutto se stranieri, i quali si trovano a dover rispondere a richieste molto differenti tra loro, provenienti sia dalla Polizia Giudiziaria, sia dagli stessi avvocati che svolgono le previste attività d'indagine difensive ai sensi dell'art. 132, comma 3, D.Lgs. n. 196/03[117].

A questo riguardo è utile richiamare una interessante pronuncia del Tribunale di Chieti relativa ad un caso in cui la persona offesa aveva, spontaneamente, consegnato alla Polizia Giudiziaria i *file* di *log* in grado di dimostrare la colpevolezza dell'imputato. Detto Tribunale in detta circostanza invalidò tali elementi di prova rilevando che «il dato acquisito fosse minimo e del tutto insufficiente a fondare qualsivoglia affermazione di responsabilità al di là del ragionevole dubbio». In particolare, si ritenne che le indagini non fossero state adeguatamente approfondite, poiché ci si era limitati ad interpellare la ditta senza alcuna formale acquisizione di dati e senza alcuna verifica circa le modalità della conservazione degli stessi allo scopo di assicurarne la genuinità e l'attendibilità nel tempo. Venendo così a mancare le necessarie garanzie di genuinità ed integrità dei *file di log* acquisiti, definiti nella sentenza «dati tecnici di particolare delicatezza e manipolabilità», provenienti oltretutto dalla stessa persona offesa e pertanto da considerare in maniera ancor più rigorosa[118].

La conservazione di questi dati da parte degli *Internet Service Provider* e dei fornitori di connettività, più spesso definita con il termine inglese "*data retention*", è di fondamentale importanza sotto il profilo investigativo.

La Comunità Europea ha scelto di adottare una disciplina comunitaria molto analitica sulla c.d. "*data retention*" (Direttiva 06/24/CE)[119], tale direttiva prevede un minimo di 6 mesi fino ad un massimo di due anni di memorizzazione degli

---

[117] Art. 132, comma 3, D.Lgs. 196/03: «Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto motivato del Pubblico Ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391 *quater* del codice di procedura penale, ferme restando le condizioni di cui all'articolo 8, comma 2, lettera f), per il traffico entrante».

[118] Tribunale di Chieti, 30 maggio 2006, Sentenza n. 175, disponibile in versione integrale al seguente URL: http://www.interlex.it/testi/giurisprudenza/ch060530.htm.

[119] Direttiva UE 06/24/CE, disponibile all'URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

indirizzi IP e *dei file* di *log* di tutto il traffico internet[120].

Negli Stati Uniti, tuttavia, non è stata mai emanata una normativa specifica sul tema, anche se sono stati fatti dei tentativi di regolamentazione riguardo alla conservazione dei dati come quella contenuta nel "*The Internet Safety Act*"[121], anche a causa delle numerose proteste mosse sia da EPIC *(Electronic Privacy Information Center)*[122] che da EFF[123] *(Electronic Frontier Foundation).* Uno dei motivi di tale forte opposizione fu costituito dallo scandalo scoppiato durante l'amministrazione Bush circa l'accordo segreto della *National Security Agency* con i principali gestori di telefonia statunitensi, finalizzato a creare un *database* di tutte le telefonate e le attività *online* compiute dai cittadini americani[124].

Le critiche, tuttavia, non sono mancate nemmeno in Europa, lo dimostra il fatto che, ad oggi, ben 14 Stati membri su 27 abbiano espressamente richiesto una dilazione, per l'applicazione della stessa[125].

La Corte di Giustizia è dovuta intervenire, nel marzo del 2009, rigettando il ricorso promosso da Irlanda e Slovacchia, le quali avevano chiesto l'annullamento della direttiva in oggetto[126]. Nonostante questa decisione la Corte Costituzionale tedesca, nel marzo del 2010, riteneva incostituzionale la legge riguardante l'archiviazione di massa di dati telefonici e di navigazione su Internet, derivante dal recepimento di detta direttiva europea.

La Corte, nella sua sentenza, ha affermato che tale legge viola la segretezza delle comunicazioni, archivia dati sensibili in mancanza di parametri di sicurezza

---

[120] In Italia la Direttiva 06/24/CE del 15 marzo 2006 è stata recepita con il D.Lgs. 30 maggio 2008, n. 109 che ha stabilito un periodo di conservazione del traffico telematico pari a 12 mesi.

[121] Da anni si discute, infatti, della possibilità di adottare una normativa specifica che preveda un determinato periodo di tempo di conservazione dei dati digitali. Tra le varie proposte si può citare il "*The Internet Safety Act*", proposto nel 2009 da due Senatori Repubblicani (Lamar Smith e John Cornyn) menzionato all'interno del seguente URL: http://www.pcmag.com/article2/0,2817,2341476,00.asp. A questo proposito va ricordato inoltre, che il "*Sarbanes Oxley Act*" del 2002, che obbliga a conservare le *email* della propria società per almeno 5 anni, reperibile alla seguente URL: https://www.sec.gov/about/laws/soa2002.pdf.

[122] Si veda il seguente URL: http://epic.org/privacy/intl/data_retention.html.

[123] E. KATZ, *The Beginning of the End of DataRetention Commentary*, in EFF, 10 marzo 2010, disponibile al seguente URL: https://www.eff.org/deeplinks/2010/03/beginning-end-data-retention.

[124] Articolo del New York Times del 16 dicembre 2005, J. RISEN - E. LICHTBLAU, *Bush Lets U.S. Spy on Callers Without Courts,* disponibile al seguente URL: http://www.wired.com/threatlevel/2008/03/times-reporter/.

[125] Significativo anche il fatto che tra questi Stati Membri vi sia anche il Granducato di Lussemburgo, Stato in cui ha sede Skype Europa.

[126] Il ricorso per l'annullamento della direttiva era fondato sul presupposto che la stessa fosse stata emanata non per armonizzare le legislazioni al fine di favorire il mercato interno nel settore delle comunicazioni elettroniche, bensì per favorire la raccolta di questi dati per scopi di sicurezza pubblica e lotta al terrorismo. Questi scopi, infatti, fanno parte della "cooperazione giudiziaria e di polizia in materia penale" e non dovrebbero essere regolati attraverso una direttiva comunitaria, secondo quanto sostenuto dai due Stati membri.

per i cittadini ed è carente di informazioni precise in merito a come i dati verranno utilizzati[127]. Analoga decisione era stata raggiunta pochi mesi prima dalla Corte Costituzionale Romena[128] precedendo di poco quella della medesima Corte della Repubblica Ceca. Quanto detto rischia di pregiudicare seriamente l'attività investigativa internazionale, da un punto di vista pratico: un ufficiale di Polizia Giudiziaria delegato a svolgere un'indagine dove è coinvolto un *provider* di servizi statunitense, tedesco, ceco o rumeno, non potrà mai sapere a priori se i dati che sta cercando siano già stati cancellati oppure se gli stessi siano ancora memorizzati e utilizzabili per le indagini.

Una possibile variante alla c.d. "*data retention*", è la c.d. "*data preservation*" prevista dall'art. 16 della Convenzione *Cybercrime* sottoscritta a Budapest il 23 novembre 2001. Quest'ultima risulta essere radicalmente diversa, in quanto non obbliga i *provider* ed i fornitori di connettività di conservare tutti i dati di traffico, ma solo di conservare e congelare, "*quick freeze procedure*", i dati, qualora gli stessi siano espressamente richiesti dall'Autorità Giudiziaria.

L'art. 10 della Legge n. 48/2008 ha dato applicazione all'art. 16 della Convenzione *Cybercrime* stabilendo che il Ministro dell'Interno, e su sua delega, le Forze dell'Ordine, possono ordinare agli *Internet Service Provider,* anche in relazione alle eventuali richieste avanzate da autorità giudiziarie straniere, di conservare e proteggere, per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni.

I provvedimenti adottati sono comunicati entro quarantotto ore al Pubblico Ministero del luogo di esecuzione che, se ne ricorrono i presupposti, li convalida.

In caso mancanza di convalida, tali provvedimenti assunti perdono ogni efficacia. La "*data preservation*" è indubbiamente meno invasiva della "*data retention*", tuttavia per gli stessi motivi, la "*data preservation*" non permette il recupero di informazioni relative ad attività illecite accadute prima della richiesta di "congelamento", risultando quindi fortemente inefficace ai fini dell'attività investigativa. Ai problemi di natura giuridica, si aggiungono spesso anche quelli di carattere tecnico. Infatti, dopo aver ottenuto l'indirizzo IP dinamico[129] ricercato,

---

[127]Il comunicato stampa della Corte Costituzionale tedesca dal titolo "*Konkrete Ausgestaltung der Vorratsdatenspeicherung nicht verfassunggemass*", è disponibile al seguente URL: www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2010/bvg10-011.html.

[128]Decisione della Corte Costituzionale Rumena n. 1258 dell'8 ottobre 2009.

[129] Gli indirizzi IP possono essere assegnati in maniera permanente (per esempio un *server* che si trova sempre allo stesso indirizzo) oppure in maniera temporanea, da un intervallo di indirizzi disponibili. Nel primo caso vengono definiti indirizzi IP statici, mentre nel secondo caso, indirizzi

l'Ufficiale o l'Agente di Polizia Giudiziaria si trovano molto spesso di fronte a due ulteriori problemi di natura tecnica che rischiano di vanificare tutta l'attività investigativa svolta o anche talvolta di indirizzare le indagini nei confronti della "persona sbagliata". Ogni secondo, si collegano alla Rete Internet milioni di utenti: gli *Internet Service Provider* e i fornitori di connettività conservano tutte le informazioni di accesso di attività svolta dagli stessi.

È evidente, quindi, che se la Polizia Giudiziaria effettua una richiesta riferendosi ad una data e/o ad un'ora errata, le risultanze fornite potrebbero essere completamente sbagliate e vanificare tutti gli sforzi investigativi posti in atto.

Un altro serio problema di carattere tecnico è quello dell'occultamento dell'identità. La tecnica più conosciuta e diffusa per rendere anonima la propria navigazione in Rete è data dall'utilizzo di un *proxy server*[130]. Programmi di navigazione come *TOR Browser* permettono con grande semplicità di navigare in maniera anonima anche agli utenti della Rete sprovvisti di particolari conoscenze tecniche. Vi sono inoltre gli "*anonymous remailer*", essi sono *server* che ricevono messaggi di posta elettronica e li inviano nuovamente seguendo apposite istruzioni incluse nei messaggi stessi, senza rivelare la loro provenienza originaria[131].

Particolarmente diffuse sono, infine, diverse tecniche di utilizzo fraudolento degli identificativi dell'elaboratore di un soggetto: in questi casi l'autore del comportamento illecito non soltanto nasconde la propria identità, ma addirittura crea le condizioni perché il comportamento sembri attribuibile ad un altro utente effettivamente esistente. L'*hacker* acquisisce, così, l'identificativo e la *password* di un utente ignaro, e si collega in Rete sotto mentite spoglie.

L'acquisizione dell'identificativo e della *password* avvengono normalmente o carpendo gli estremi direttamente dall'utente, o accedendo ad una Rete *wireless* non protetta, ovvero acquisendole per via telematica attraverso l'uso di specifici programmi denominati "*trojan horses*": essi sono particolari programmi

---

IP dinamici. La grande maggioranza degli utenti della Rete, quando si collega, utilizzerà un indirizzo IP dinamico assegnato dal *Provider* di volta in volta sulla base degli "spazi disponibili".

[130] *Proxy:* programma che si interpone tra il *client* e il *server*. Il *client* si collega al *proxy* anziché al *server* e inoltra la richiesta, riceve la risposta e la invia al *client.* I *server* a cui ci si collega mediante *proxy* vedranno l'indirizzo IP di quest'ultimo e non quello del *client* garantendo un maggior livello di *privacy* poiché il *server* di destinazione conserverà i dati relativi al *proxy* e non al *client*.

[131] Per un approfondimento si veda G. DANEZIS, R. DINGLEDINE, N. MATHEWSON, *Mixminion: Design of a Type III Anonymous Remailer Protocol*, in IEEE *Security* & *Privacy*, 2003, disponibile al seguente URL: http://www.mixminion.net/minion-design.pdf. Si vedano anche i progetti TOR ai Seguenti URLs: http://www.torproject.org/index.html e Progetto Winston Smith http://pws.winstonsmith.info/.

appartenenti alla categoria dei *malware*, che si installano sull'elaboratore in maniera trasparente, con lo scopo di controllare e spiare il funzionamento del sistema, in modo da acquisirne le credenziali di accesso[132].

4.1.2. *Ispezione informatica*.

Accertata l'utenza telefonica o la linea dati, associata all'indirizzo IP attenzionato e conseguentemente il luogo dove l'utente si è collegato per commettere l'attività illecita, il passo successivo da compiere è quello di individuare il supporto informatico contenente la c.d. *"digital evidence"* (prova digitale) e, conseguentemente, individuare l'autore dell'illecito. Questa attività investigativa può assumere diverse forme. La *digital evidence*, può consistere in una immagine contenuta in un telefono, in un *file* di testo presente all'interno di un *computer*, un *record* in un *database*, in un filmato digitale presente all'interno di una memoria USB, e così via[133].

Inoltre la prova ricercata, potrebbe trovarsi memorizzata "su una piattaforma *cloud*", visto il crescente investimento dei *provider* nel *cloud computing*[134]. Il Codice di Procedura Penale prevede, quali mezzi di ricerca della prova, l'ispezione e la perquisizione. L'ispezione, che può avere ad oggetto persone, luoghi o cose, viene disposta su richiesta da parte dell'Autorità Giudiziaria e consente, a quest'ultima, di acquisire direttamente elementi utili alla ricostruzione del fatto. Se il reato non ha lasciato tracce o altri effetti materiali, ovvero se questi si sono deteriorati o sono stati cancellati, dispersi, alterati o rimossi, la Polizia Giudiziaria descrive lo stato attuale dei luoghi e se possibile quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni[135]. Nel corso dell'ispezione, la Polizia Giudiziaria può ordinare che nessuno si allontani prima che le operazioni siano concluse e se necessario può far

---

[132] F. TESTA, *Cybercrime, intercettazioni telematiche e cooperazione giudiziaria in materia di attacchi ai sistemi informatici*, Incontro di Studio sul tema "Criminalità organizzata transnazionale: strumenti di contrasto e forme di cooperazione giudiziaria", 6/8 giugno 2005, Roma. Si veda il rapporto annuale del CERT (*Computer Emergency Response Team*), 2014, URL: http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2014.pdf.

[133] A. GHIRARDINI, G. FAGGIOLI, *Digital Forensics*, Apogeo, Milano, 2013.

[134] Per un approfondimento sul tema si veda: UC Berkeley Reliable Adaptive Distributed Systems Laboratory, *Above the Clouds: A Berkeley View of Cloud Computing*, disponibile al seguente URL: https://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

[135] L'ispezione personale, che rileva marginalmente nell'ambito informatico è l'atto diretto ad osservare la persona, al fine di accertare le tracce o gli altri effetti materiali del reato (art. 245 c.p.p.). Circa le modalità di svolgimento dell'ispezione personale il codice ha stabilito che l'operazione debba essere eseguita nel rispetto della dignità e del pudore di chi vi è sottoposto.

ricondurre coattivamente sul posto il trasgressore (art. 246 c.p.p.); può altresì disporre che siano effettuati rilievi segnaletici, descrittivi, fotografici ed eventuali altre operazioni tecniche (art. 244 c.p.p.).

Tali attività, inoltre, sono per loro natura irripetibili ed è, pertanto, necessario che i relativi verbali siano dettagliati e che agli stessi sia allegata tutta la documentazione utile al fine di provare la commissione dell'illecito[136].

A questo riguardo è utile richiamare quanto disposto dal Tribunale di Savona che ha assolto con formula piena un soggetto imputato del reato di duplicazione abusiva di *software*, ai sensi dell'articolo 171 *bis* della Legge sul diritto d'autore, in quanto l'indagine svolta appariva assolutamente lacunosa, non essendo stata effettuata né la duplicazione delle memorie dei *computer*, né un sequestro degli stessi, né le fotocopie delle licenze esibite. Le uniche prove erano pertanto costituite dalla scarna relazione del Consulente Tecnico, che dichiarava: "Non essendo stata presentata alcuna documentazione comprovante il regolare possesso del *software* rinvenuto durante l'ispezione e indicato come sprovvisto di licenza d'uso, si conferma quanto precedentemente indicato nel verbale di ispezione"; inoltre, nel verbale di ispezione richiamato non era allegata alcuna documentazione comprovante l'effettiva duplicazione del *software*.

Qualora, dunque, siano applicate delle corrette metodologie operative, l'ispezione risulta essere un prezioso e fondamentale strumento di indagine, in particolare riguardo l'analisi di materiale informatico[137]. La Polizia Giudiziaria, dopo aver trovato le tracce informatiche del reato commesso, ha, infatti, la possibilità non solo di redigere il verbale di ispezione, ma anche di acquisire, attraverso una copia *bit-stream* del supporto di memorizzazione, i dati utili alla prosecuzione dell'indagine[138]. La copia *bit-stream* è un particolare tipo di duplicazione che preserva anche l'allocazione fisica dei singoli *file,* oltre che la

---

[136] Tribunale di Savona, 17 gennaio 2004, Sentenza n. 844/04, disponibile all'URL: http://www.ictlex.net/?p=459.

[137] L'art. 364 c.p.p. al comma 5, prevede, infatti, che "nei casi di assoluta urgenza, quando vi è fondato motivo di ritenere che il ritardo possa pregiudicare la ricerca o l'assicurazione delle fonti di prova, il Pubblico Ministero può procedere a interrogatorio, a ispezione o a confronto anche prima del termine fissato dandone avviso al difensore senza ritardo e comunque tempestivamente. L'avviso può essere omesso quando il Pubblico Ministero procede a ispezione e vi è fondato motivo di ritenere che le tracce o gli altri effetti materiali del reato possano essere alterati. E' fatta salva, in ogni caso, la facoltà del difensore d'intervenire".

[138] Si noti, inoltre, che la Suprema Corte ha ritenuto che non costituisce sequestro probatorio l'acquisizione, mediante riproduzione su supporto cartaceo, dei dati informatizzati contenuti in un archivio informatico visionato nel corso di un'ispezione legittimamente effettuata, in quanto non vi è alcuna apprensione dell'archivio informatico, ma una semplice estrazione di copia dei dati in esso contenuti (Cass. Pen., Sez. III, 26 gennaio 2000, n. 384).

loro posizione logica[139].

Prima di effettuare questa operazione sarà tuttavia necessario garantire l'integrità dei dati attraverso:

1. La creazione di un'impronta di *hash*[140], che permetterà di dimostrare, se i contenuti del *file* oppure del supporto, abbiano subito o no modifiche;
2. L'utilizzo di un *"write blocker"* che consente di bloccare ogni tipo di scrittura sul supporto ispezionato.

Qualora l'attività investigativa venga svolta utilizzando metodi di acquisizione idonei a garantire l'integrità e la genuinità dei dati, gli stessi potranno essere pienamente utilizzati in dibattimento quale fonte di prova. A tal proposito, la Legge di ratifica della Convenzione *Cybercrime*, ha modificato l'art. 244 c.p.p., disponendo espressamente che: "in relazione a sistemi informatici o telematici, devono essere adottate misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione". L'ispezione, a differenza del sequestro non prevede un eventuale spossessamento dei beni dell'indagato, tuttavia dovendosi procedere ad un'analisi nell'immediatezza, risulta essere un'attività che esige specifiche competenze informatiche ed un'adeguata strumentazione tecnica. Per questo motivo, tale mezzo di ricerca della prova appare applicabile esclusivamente per reati facilmente identificabili, che impongano uno studio superficiale dello strumento informatico. Sarebbe, infatti, molto complesso procedere, in un ragionevole arco temporale, all'analisi di supporti sempre più capienti (in pochi anni si è passati dai *gigabye* ai *terabyte*) e di cui l'intero contenuto potrebbe risultare utile all'indagine. Basti pensare che, ad oggi, i tempi medi di copia sono di circa 2 *gigabyte* al minuto: da ciò consegue che per un *hard disk* di un *terabyte* saranno necessarie circa 8 ore per effettuare una copia *bit-stream image*[141]. Bisogna considerare inoltre che da un punto di vista strettamente processuale, l'irripetibilità dell'ispezione non consentirebbe all'indagato di poter effettuare, magari avvalendosi di un perito di parte, una successiva analisi del supporto informatico ispezionato.

---

[139] Per maggiori informazioni sui requisiti tecnici si veda: *The Computer Forensic Tool Testing* (CFTT), disponibile al seguente URL: http://www.cftt.nist.gov/disk_imaging.htm.

[140] L'impronta di *hash* verrà analizzata più approfonditamente nel paragrafo relativa al sequestro di materiale informatico.

[141] Per gli approfondimenti sugli aspetti pratici di un'acquisizione *bit-stream* di un *hard disk* si consiglia, N. BASSETTI, *Storia di un'analisi forense informatica*, disponibile *al seguente* URL: http://www.nannibassetti.com/dblog/articolo.asp?articolo=12.

4.1.3. *Perquisizione informatica*.

La perquisizione, a differenza dell'ispezione ha lo scopo di ricercare il corpo del reato o "le cose che ad esso si riferiscono", qualora si ritengano, con "fondati motivi", nascoste sulla persona o in un determinato luogo. La perquisizione locale è, inoltre, disposta anche quando deve eseguirsi l'arresto dell'imputato o dell'evaso e sussistono particolari motivi di urgenza che non consentono l'emissione di un tempestivo decreto di perquisizione[142].

La Suprema Corte ha precisato che per "fondati motivi" non si devono intendere ipotesi o sospetti ma "indizi di un certo rilievo" in relazione ad una concreta figura di reato, previa una corretta individuazione del "*thema probandum*" della ricerca. In caso contrario, la perquisizione e il conseguente sequestro si «trasformerebbero da mezzo di ricerca della prova in mezzo di acquisizione di una *notitia criminis*, in quanto, tale sequestro sarebbe inammissibile perché lesivo della libertà individuale *lato sensu*, che trova tutela negli articoli 13 e 14 della Costituzione»[143]. Qualora, all'interno dell'indagine, fosse necessario ricercare fonti di prova che coinvolgono l'elaboratore elettronico, saranno oggetto della perquisizione anche tutti i supporti ad esso dedicati, e quelli contenenti dati potenzialmente utili ai fini dell'indagine. Nel caso in cui la cosa ricercata venga consegnata spontaneamente dal soggetto, non si procede alla perquisizione, tranne si ritenga opportuno procedervi per la completezza delle indagini.

Prima di iniziare la perquisizione, viene notificato il relativo decreto autorizzativo all'interessato; questi ha facoltà di farsi assistere da persona di fiducia, purché sia prontamente reperibile e sia idonea ad assumere la veste di "testimone" di un atto del procedimento. Nella maggioranza dei casi, il decreto di perquisizione comprende anche quello di sequestro: sebbene, infatti, si tratti di due mezzi di ricerca della prova distinti, è evidente che, una volta trovato il corpo del reato o "le cose che ad esso si riferiscono", diventa necessario impedirne la disponibilità all'indagato, per evitare ogni possibile alterazione della prova. Anche la perquisizione, come l'ispezione richiede che ogni operazione avente ad oggetto

[142] Articolo 352 c.p.p.: Nella flagranza del reato o nel caso di evasione, gli ufficiali di polizia giudiziaria procedono a perquisizione personale o locale quando hanno fondato motivo di ritenere che sulla persona si trovino occultate cose o tracce pertinenti al reato che possono essere cancellate o disperse ovvero che tali cose o tracce si trovino in un determinato luogo o che ivi si trovi la persona sottoposta alle indagini o l'evaso.

[143] Cass. Pen., 29 ottobre 1993, in *Cassazione Penale*, 1995.

lo strumento informatico, sia uniforme ad una metodologia operativa che garantisca l'integrità e la genuinità dei dati, questo al fine di evitare eventuali contestazioni in sede dibattimentale riguardo alle modalità di acquisizione della prova durante le indagini[144].

E' qui il caso di richiamare nuovamente l'interessante pronuncia in tema di accesso abusivo e danneggiamento a un sistema informatico, del Tribunale di Bologna[145]. Come già accennato sommariamente nel secondo capitolo, il caso riguardava un *hacker* che, dopo aver creato un *malware* denominato "Vierika", lo aveva diffuso tramite un noto *provider* a circa 900 utilizzatori. Il *malware*, inviato come allegato di una *email*, una volta eseguito, andava ad agire sul registro di configurazione del sistema operativo Windows, portando al livello minimo le impostazioni di protezione del *browser* Internet Explorer e inserendo, come *home page* del predetto *browser*, una determinata pagina di un *social network* scelta dall'autore del *malware*. Quando l'utente accedeva in Rete, veniva automaticamente scaricato un comando che creava nella prima partizione del disco rigido del *computer il file* C:\Vierika.JPG.vbs, contenente la prima parte del codice, producendo un effetto di "*mass mailing*"; veniva, infatti, inviata agli indirizzi contenuti nella rubrica di Outlook una *email* contenente l'allegato sopra descritto, in modo che il *malware* si potesse replicare autonomamente. Il Giudice, per formulare la sentenza, si è basato principalmente sul verbale di perquisizione e contestuale sequestro, in quanto, in quella sede l'indagato aveva ammesso spontaneamente il fatto. Inoltre, egli aveva personalmente masterizzato un CD contenente i *file* incriminati, consegnandolo alla Polizia Giudiziaria. Tale *modus operandi*, non corrispondendo a nessuno dei protocolli tecnici ritenuti idonei a garantire l'autenticità e la genuinità dell'acquisizione, avrebbe dovuto far ritenere illegittimamente acquisita la prova del fatto. Il Giudice, tuttavia, ha ritenuto che non fosse suo compito determinare un protocollo relativo alle procedure informatiche forensi; pertanto, in forza del principio della libera valutazione della

[144] Anche in questo caso è intervenuta la Legge n. 48/08 che ha modificato l'art. 247 c.p.p. sancendo espressamente che: «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, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

[145] Tribunale di Bologna, 22 dicembre 2005, Sentenza n. 1823/05 disponibile al seguente URL: http://www.ictlex.net/?p=516; circa tre anni più tardi la Corte di Appello di Bologna con la Sentenza n. 369/08, ha riformato parzialmente la sentenza, senza intervenire tuttavia sugli aspetti procedurali, ma limitandosi solo a una diversa qualificazione giuridica dei fatti (Corte di Appello di Bologna, 30 gennaio 2008, disponibile al seguente URL: http://www.ictlex.net/?p= 692).

prova, previsto dall'art. 192 c.p., ha ritenuto, alla luce del contesto probatorio complessivo, che gli accertamenti compiuti dalla Polizia Giudiziaria fossero pienamente attendibili ed utilizzabili ai fini della decisione.

La dottrina ha criticato tale motivazione poiché, di fatto, ha portato ad un'inversione dell'onere della prova a carico dell'imputato. Rimane, tuttavia, il dubbio sulla decisione che il Giudice avrebbe adottato, se l'imputato non avesse immediatamente ammesso la sua piena colpevolezza circa i reati contestati[146].

Il Tribunale di Pescara, diversamente da quello di Bologna, ha ritenuto non attendibili le indagini informatiche svolte dalla Polizia Giudiziaria nel caso di un procedimento relativo al reato di pubblicazioni e spettacoli osceni, previsto dall'art. 528 c.p.: l'imputato era accusato di aver messo in circolazione immagini dal contenuto pornografico attraverso un apposito reindirizzamento al sito Internet denominato www.vallecupa.com"[147]. La giurisprudenza in materia, infatti, prevede che il commercio di materiale pornografico, purché realizzato nei confronti di acquirenti adulti, non integri alcuna fattispecie di reato, ma solo ove il Giudice di merito accerti che in relazione a tali modalità il comune senso del pudore non risulti offeso[148].

Le indagini avevano portato all'identificazione del titolare del sito, tramite il fornitore di servizi di *network hosting* statunitense e la stampa di alcune pagine del sito stesso. Nel corso della perquisizione, erano stati rinvenuti su un *personal computer* utilizzato come *server* DNS due *file* di *log*, i quali erano stati acquisiti mediante copia su supporto CD ed un *file* identificabile con il nome "vallecupa.com.dns", contenente il reindirizzamento della pagina *social network* vallecupa.com, allocata presso il *server* della società statunitense "50-megs.com".

Nessuna immagine relativa al sito vallecupa.com era presente, tuttavia, sul *personal computer*. Durante la perizia disposta in dibattimento, il perito incaricato ha rappresentato di essere impossibilitato ad ogni considerazione, non essendo riuscito ad acquisire le pagine *web* incriminate nel formato digitale al fine di valutarne contenuto e caratteristiche tecniche.

Lo stesso perito ha criticato, inoltre, la mancata acquisizione di copia

---

[146] L. LUPARIA, *Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova finale digitale - Profili processuali*, in *Diritto dell'Internet*, 2006, p. 153 e F. CATULLO, *Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova finale digitale - Profili sostanziali*, in *Diritto dell'Internet*, 2006.

[147] Tribunale di Pescara, 30 novembre 2006, Sentenza n. 1369, disponibile al seguente URL: http://www.scintlex.it/database/notizie/notizia_pdf.php?id=241.

[148] Cass. Pen. Sez. III, 12 maggio 1994, n. 5630.

certificata dei documenti informatici, con eventuale firma digitale, come prevista dalla normativa tecnica già all'epoca emanata dall'AIPA (Autorità per l'Informatica nella Pubblica Amministrazione, ora CNIPA Centro Nazionale per l'Informatica nella P.A.), riguardo alla diffusione e la conservazione della documentazione informatica. Lo stesso ha evidenziato, infine, la scarsa valenza probatoria delle riproduzioni a stampa (evidentemente non classificabili, quali "documenti analogici originali"), che, riportavano oltretutto date di consultazione delle pagine del sito www.vallecupa.com successive alla commissione del reato.

In quest'ultimo caso, il Giudice, ritenendo il quadro probatorio insufficiente a fondare una condanna, ha assolto l'imputato per insufficienza di prove ai sensi dell'articolo 530 comma 2 c.p.p. Qualora la Polizia Giudiziaria avesse acquisito l'intero sito *web* in formato digitale e avesse certificato la data dell'acquisizione attraverso alcuni opportuni accorgimenti tecnici (firma digitale del *file* mediante utilizzo della funzione di *hash*), avrebbe sicuramente fornito al Giudice degli elementi idonei per valutare diversamente l'intera vicenda. Alcuni informatici italiani hanno recentemente realizzato un *software* denominato *hashbot* (*www.hashbot.com*), in cui viene fornita la possibilità di validare ogni prova digitale reperita sul *web*, attraverso l'utilizzo della funzione di *hash.* Detto sito internet contiene, infatti, un *tool* efficace e sicuro per la validazione di prove digitali acquisite in Rete.

4.1.4. *Accertamenti urgenti sui luoghi e sequestro*.

Nel caso in cui vi sia il concreto rischio che le cose, le tracce e i luoghi pertinenti al reato si alterino e il Pubblico Ministero non possa intervenire tempestivamente, o non abbia ancora assunto la direzione delle indagini, gli ufficiali di Polizia Giudiziaria compiono i necessari accertamenti sullo stato dei luoghi e delle cose e, se del caso, sequestrano il corpo del reato e le cose a questo pertinenti[149].

Questa importante facoltà, concessa alla Polizia Giudiziaria ai sensi dell'art. 354 c.p.p., risulta essere di notevole importanza nell'ambito delle indagini informatiche, poiché accade frequentemente che la prova digitale divenga successivamente difficilmente recuperabile. Come accadrebbe nel caso in cui

[149] Anche se rileva marginalmente nell'ambito delle investigazioni digitali, l'accertamento urgente può essere anche nei confronti delle persone. In questo caso, gli ufficiali di Polizia Giudiziaria compiono i necessari accertamenti e rilievi sulle persone.

durante un accertamento urgente l'elaboratore fosse trovato in funzione, in questo caso potrebbe essere utile o addirittura indispensabile recuperare tutti i dati volatili presenti all'interno della RAM[150], dati che inevitabilmente verrebbero persi con l'arresto del sistema operativo. Analogamente, potrebbe essere utile verificare preliminarmente il contenuto dell'*hard disk* attraverso un'attività di *preview* che è possibile svolgere attraverso l'utilizzo di una distribuzione *live* di *software* di *digital forensics* o mediante l'utilizzo di dispositivi *hardware* che inibiscono elettronicamente l'accesso al supporto in esame, come ad esempio il dispositivo denominato *write blocker*.

Il Legislatore, consapevole dell'importanza di questo strumento processuale nelle investigazioni digitali, ha opportunamente precisato, con la Legge n. 48/2008, che "in relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità". Sarà quindi opportuno che la Polizia Giudiziaria adotti tutte le necessarie cautele per evitare il rischio di alterare il dato digitale, in assenza di una precisa delega del Pubblico Ministero. Una recente pronuncia della Corte di Cassazione ha ribadito un principio molto importante, afferente ad un caso in cui era stata effettuata un'attività di accertamento urgente, consistita nell'analisi di un *hard disk* sequestrato ad una persona diversa dall'indagato, senza che venissero adottate le cautele per garantire la non alterazione della prova digitale, erano emersi degli utili riscontri probatori che dimostravano che l'allora indagato faceva parte di un gruppo malavitoso legato alla "camorra" e che, in quanto detenuto, «riceveva uno stipendio di 15000 € all'anno». La Suprema Corte, in risposta alle eccezioni della difesa dell'indagato circa il fatto che tale prova sarebbe potuta essere stata alterata durante l'accertamento tecnico, avvenuto senza un adeguato contraddittorio, ha tuttavia precisato che tale eccezione sarebbe potuto essere fatta valere solo qualora fosse stata accertata l'alterazione del dato informatico. Alla

[150] R.A.M.: acronimo usato nell'informatica per *Random Access Memory*, è il supporto di memoria su cui è possibile leggere e scrivere informazioni con un accesso "casuale", ovvero senza dover rispettare un determinato ordine, come ad esempio avviene per un nastro magnetico. Caratteristica comune a tutti i tipi di RAM utilizzati per la memoria principale è quella di perdere il proprio contenuto nel momento in cui viene a mancare la corrente elettrica che le alimenta.

luce di quanto detto, appare evidente, che la Corte di Cassazione abbia ritenuto ripetibile tale operazione generando, di fatto, anche in questo caso una sorta d'inversione dell'onere probatorio a carico dell'indagato nonostante, nel caso di specie, il *computer* non fosse di sua proprietà[151].

4.1.5. *La disciplina "search and seizure" statunitense*.

Gli Stati Uniti rappresentano un modello di confronto particolarmente interessante, in quanto il tema dell'individuazione e acquisizione della prova digitale è stato oggetto di una vasta e dettagliata analisi giurisprudenziale. Il quarto emendamento della Costituzione americana risulta essere la fonte primaria che regola tale materia, in quanto afferma: "Il diritto dei cittadini ad essere sicuri nelle loro persone, case, carte ed effetti personali contro perquisizioni e sequestri non ragionevoli, non potrà essere violato, e non potranno essere emessi mandati se non sulla base di motivi fondati, sostenuti da giuramenti o solenni affermazioni e con una dettagliata descrizione del luogo da perquisire e degli oggetti da sequestrare"[152].

Occorre preliminarmente sottolineare che, a differenza della disciplina normativa italiana sui mezzi della ricerca della prova, la disciplina statunitense non distingue tra ispezione, perquisizione e sequestro, ma si limita ad identificare un unico mezzo che comprende la ricerca della prova e il suo successivo sequestro ("*search and seizure*"). La norma che regola la disciplina del "search and seizure" della *digital evidence* è la *Rule 41* delle *Federal Rules of Criminal Procedure*[153], mentre il *Title* 18 U.S.C. §§ 2701-12 dello *Stored Communication Act*[154] si applica in caso di sequestro presso un *provider*.

Le due disposizioni normative prevedono che sia necessario un search

---

[151] Cass. Pen., Sez. I, 16 marzo 2009, n. 11503.

[152] «*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*».

[153] *Rule 41 Federal Rules of Criminal Procedure (Search and Seizure):* [...] «*After receiving an affidavit or other information, a magistrate judge - or if authorized by Rule 41(b), a judge of a state court of record - must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device* [...]». La norma per esteso è disponibile al seguente URL: https://www.law.cornell.edu/rules/frcrmp/rule_41.

[154] *Title 18 U.S.C. §§ 2701-12 Stored Communication Act:* "(a) *A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction* [...]".

warrant, salvo che non ci sia il consenso del soggetto titolare di tali dati. La *Rule 41* chiarisce, inoltre, che per ottenere un mandato *(warrant)* di perquisizione e sequestro *(search and seizure),* è necessario che l'agente che ha svolto le indagini sottoscriva una dichiarazione (*affidavit*[155]) che dovrà essere sottoposta *(application)* al vaglio di un Giudice competente in materia (*magistrate*).

L'affidavit deve:

- Chiarire le ragioni per cui è necessaria tale attività;
- Descrivere con precisione i dati digitali che dovranno essere sequestrati, salvo che non si chieda il sequestro dell'intero *personal computer*.

Il richiedente deve indicare *nell'affidavit* quali attività d'indagine hanno permesso di identificare, in particolare, l'abitazione del potenziale criminale. La giurisprudenza, al riguardo, ha ritenuto che costituiscano validi presupposti per la concessione del *warrant*, l'acquisizione dell'indirizzo IP del soggetto indagato fornito dai provider[156] ovvero le credenziali delle carte di credito raccolte nel caso di un acquisto *online*[157].

La descrizione dei dati digitali da sequestrare dovrà essere fatta in modo preciso, al fine di evitare che siano sequestrati oggetti non rilevanti[158] e, in ogni caso, dovrà essere limitata agli oggetti per cui è stata ritenuta necessaria tale richiesta. In merito a tale ipotesi, un precedente storico è dato dal caso di due società statunitensi (Solid State Devices e Unisem Internation) indagate per aver fornito al Dipartimento della Difesa semi-conduttori non conformi a quanto previsto dal contratto. La Corte di Appello degli Stati Uniti ritenne illegittimo il provvedimento di *search and seizure,* in quanto il *warrant* non era dettagliato e l'attività svolta nella fase di indagine aveva violato i principi del 4° emendamento

---

[155] Negli ordinamenti di *Common Law*, l'*affidavit*, è una dichiarazione scritta, resa da una persona detta *affiant* o *deponent*, riguardo uno o più fatti giuridicamente rilevanti e confermata dal giuramento dinanzi un pubblico ufficiale, avvocato, giudice, o altro soggetto autorizzato.

[156] *United States vs. Perez, 484 F3d 735, 740 (5th Cir. 2007); United States vs. Grant, 218 F3d 72, 76 (1st Cir. 2000).*

[157] Nel caso *United States vs. Kelley, 482 F3d 1047, 1053 (9th Cir. 2007),* alcuni utenti del servizio America On Line erano stati identificati poiché avevano acquistato immagini pedopornografiche con la loro carta di credito.

[158] *Marron vs. United States, 275 U.S. 192, 296 (1927).* Nel caso *United States vs. Fleet Management Ltd., 521 F. Supp. 2d 436, 443-444 (E.D. Pa. 2007)* è stato osservato che «*a similarly dangerous phrase, 'any and all data, including but not limited to a list of items', has been held to turn a computer search warrant into an incostitutional general warrant*».

della Costituzione[159].

D'altro canto, ed esattamente come accade in Italia, negli Stati Uniti non vi sono chiare indicazioni sull'opportunità di procedere al sequestro del dato digitale attraverso la copia *bit-stream dell'hard disk* direttamente nel luogo dove è rinvenuto il supporto informatico. Nel caso vi sia il rischio che si protraggano le conseguenze del reato, ovvero qualora la copia *bit-stream* dell'immagine del disco dovesse comportare un eccessivo dispendio di tempo, sarà necessario disporre il sequestro dell'*hardware*[160]. In presenza di determinate circostanze, inoltre, la Corte potrà ritardare la notifica del *warrant* fino a 90 giorni dopo la perquisizione. Il codice di procedura penale statunitense (18 U.S.C. §§ 3103a) prevede che ciò possa avvenire qualora la notifica all'interessato dell'atto possa pregiudicare la salute o la vita di una persona, compromettere la prova o mettere in pericolo l'intera indagine. Nel caso *United States v. Grubbs*, ad esempio, il Giudice ritenne legittimo un *warrant* effettuato sulla futura consegna di un video contenente immagini pedo-pornografiche, ordinato *online* dall'indagato[161].

Sempre in tema di legittimità dell'attività di *search and seizure*, nel caso in cui gli agenti abbiano ragione di credere che i dati siano stati memorizzati in due o più luoghi all'interno del territorio degli Stati Uniti, dovranno chiedere ed ottenere un mandato per ogni luogo dove si ritiene che il dato risieda[162].

Sebbene i principi fissati dal quarto emendamento della Carta Costituzionale statunitense appaiano particolarmente stringenti e garantisti, è ammessa la perquisizione e il sequestro della prova digitale anche senza mandato, qualora il soggetto si trovi in una condizione in cui non si possa ragionevolmente pretendere che venga rispettata la sua aspettativa di *privacy*[163].

---

[159] *In re Grand Jury Investigation Concerning Solid State Devices, Inc., 130 F.3d 85 3,* 957 *(9th Cir. 1997).*

[160] *United States vs. Hay, 231 F3d 630, 637 (9th Cir. 2000).* In questo caso, la Corte aveva ritenuto legittimo il sequestro di materiale informatico, in quanto sarebbe stato impossibile effettuare una copia forense di tutto il materiale in tempi brevi.

[161] *United States vs. Grubbs, 547 U.S. 90, 98-99 (2006).*

[162] Sebbene la definizione di "proprietà" sancita dalla *Rules* 41 *del Federal Criminal Procedural Code* e come è interpretata dalla giurisprudenza statunitense, sembri limitare le perquisizioni finalizzate a ricercare una *digital evidence* al perimetro giurisdizionale indicato sul *warrant*, in alcune pronunce la Corte non è sembrata orientata a ritenere inutilizzabile una prova acquisita in un'altra giurisdizione, salvo che non vi sia stata una deliberata violazione della *Rule 41* o che la perquisizione non avrebbe avuto luogo o avrebbe potuto essere meno invasiva se si fosse rispettata la citata norma *(United States vs. Burke, 517 F2d 377, 386 2d Cir. 1975).*

[163] Viene definita dalla giurisprudenza statunitense una "*expectation of privacy constitutionally reasonable*". Ad esempio nel caso dei rifiuti lasciati fuori dalla propria abitazione *(California vs. Greenwood, 486 U.S. 35, 40-41 1988)* o nel caso in cui passeggi per strada *(Oliver vs. United States, 466 U.S. 170, 177 1984).*

La giurisprudenza statunitense, alla fine degli anni ottanta, ha più volte affrontato il principio della "*expectation of privacy constitutionally reasonable*", chiarendone i limiti: in un'indagine legata al traffico di stupefacenti, la Polizia Giudiziaria aveva ispezionato i rifiuti lasciati fuori dall'abitazione dell'indagato[164].

La Suprema Corte statunitense ha stabilito che tale attività d'indagine non viola i principi previsti dal quarto emendamento e non è quindi ragionevole ritenere che sia stata violata la *privacy* dell'indagato. Analogamente, la Suprema Corte, in un caso in cui un poliziotto aveva scoperto una piantagione di *marijuana* situata in un terreno distante alcune centinaia di metri dall'abitazione dell'imputato, ha statuito che la tutela offerta dal quarto emendamento riguarda solo l'abitazione e, al massimo, il giardino adiacente a essa[165].

Con l'avvento delle nuove tecnologie, le Corti statunitensi hanno applicato tale principio, stabilendo quando è possibile acquisire la *digital evidence* senza bisogno del mandato. Tale possibilità si verifica qualora:

- la prova digitale sia inviata a una terza persona *(Third-Party Possession)*[166];
- la prova digitale sia stata scoperta e comunicata all'Autorità Giudiziaria da parte di un privato *(Private Search)*[167];
- vi sia il consenso dell'indagato, della moglie/marito dello stesso[168], dei genitori se l'indagato è minorenne[169], o anche di una persona che condivide lo stesso *personal computer*[170] *(Consent)*;
- vi sia una situazione di pericolo e la prova digitale rischi di essere

---

[164] *California vs. Greenwood, 486 U.S. 35, 40-41 1988.*

[165] *Oliver vs. United States, 466 U.S. 170, 178 1984.*

[166] Nel caso *United States vs. Horowitz, 806 F.2d 1222 (4th Cir. 1986),* l'imputato aveva inviato un'*email* confidenziale rivelando il listino prezzi della società presso cui lavorava all'impiegato di una società concorrente. Il Giudice ha ritenuto che l'imputato avesse perso la sua "aspettativa di *privacy*" nel momento in cui ha comunicato a terze persone le informazioni confidenziali.

[167] Nel caso *United States vs. Grimes, 244 F.3d 375, 383 (5th Cir. 2001),* il tecnico di un centro assistenza di *personal computer* ha scoperto delle immagini pedopornografiche all'interno dell'*hard disk* del cliente. Anche in questo caso non è stata riconosciuta una legittima aspettativa di *privacy*.

[168] Nel caso *Trulock vs. Freeh, 275 E.3d, 391, 398, 403-404 (4th Cir. 2001)* un *ex* agente dell'FBI che aveva più volte criticato l'operato dell'Agenzia presso cui aveva lavorato, subì una procedura di *search and seizure* del suo *computer*. Poiché condivideva alcune *password* di accesso con la propria compagna la Corte statuì che la perquisizione era legittima con il consenso della moglie solo per quanto riguardava i *file* protetti da *password* condivise e non per quelli protetti da *password* in possesso del solo *ex* agente dell'FBI.

[169] La giurisprudenza statunitense ha riconosciuto valido anche il consenso dei genitori di un figlio maggiorenne nel caso in cui egli sia relativamente giovane e non paghi l'affitto. Sul punto si veda *United States vs. Andrus, 483, F. 3d 711, 720-21 (10th Cir.* 2007*).*

[170] *United States vs. Hudspeth, 459, F. 3d 922 (8th Cir. 2006).*

compromessa o distrutta[171];

- un *provider* e la polizia trovino un accordo per lo scambio di informazioni *(Exigent Circumstances)*[172];
- sia stato effettuato il legittimo arresto del soggetto indagato *(Search after a lawful arrest)*[173];
- la prova digitale emerga *ictu oculi (Plain View)*[174];
- la prova sia scoperta durante un controllo alla frontiera *(Border Search)*[175];
- i soggetti siano sottoposti a regimi di libertà controllata *(Probation and Parole)*[176];
- sia ricercata la prova all'interno di un ufficio pubblico *(Public-Sector Workplace Searches)*[177].

Le difficoltà di conciliare il quarto emendamento con le esigenze investigative trovano una chiara dimostrazione nel caso "*Quon*". Jerilyn Quon, un ufficiale di un'unità specializzata di forze di polizia *(SWAT),* aveva inviato numerosi messaggi erotici alla moglie, usando un sistema di *text messaging* gestito interamente dal Dipartimento di Polizia della città di Ontario. Anche se la Polizia aveva scoperto il messaggio durante un *audit* di verifica dei sistemi, causato dal sovraccarico dei messaggi che venivano effettuati sulla rete interna, la Corte di Appello sostenne che un pubblico dipendente ha una "ragionevole aspettativa di *privacy*" in merito alle proprie comunicazioni private, e considerò illegale il monitoraggio e successivo sequestro e trascrizione dei dati effettuato da parte del datore di lavoro, senza aver questi ottenuto un *warrant* da parte

---

[171] *Brigha City vs. Stuart, 547 U.S. 103, 117, 2006.* Nel valutare i casi di emergenza, l'agente deve considerare: (i) il grado di pericolo; (ii) il tempo necessario per chiedere un regolare mandato; (iii) se la prova rischi di essere modificata o distrutta.

[172] Nel caso *United States vs. Beckett, 544 F. Supp. 2d 1346, 1350,* si afferma il principio in forza del quale l'*Internet Service Provider,* che abbia prospettato nelle condizioni generali di contratto l'ipotesi che possano essere divulgate informazioni alle forze di polizia ai fini di una collaborazione durante l'indagine, è legittimato a fornirle. Questa facoltà costituisce un'eccezione alla *Section* 2702 dello *Stored Communications Act*.

[173] *Arizona vs. Gant, 129 S. Cr. 1710 (2009).*

[174] Nel caso *Horton vs. California, 496 U.S. 128, 136 (1990),* un agente che non aveva ottenuto un mandato per ricercare delle armi, ma solo della merce rubata, una volta arrivato presso l'abitazione, trova in bella mostra le armi.

[175] Nel caso *United States vs. Montoya de Hernandez, 473 U.S. 531, 538 (1985),* la Polizia di frontiera aveva perquisito senza mandato una donna che aveva ingerito degli ovuli di cocaina accompagnandola in ospedale per poter verificare l'effettiva presenza della droga all'interno del corpo della donna.

[176] *United States vs. Knights, 534 U.S. 112, 122 (2001).*

[177] *United States vs. Mancini, 8 F.3d 104, 109* (1st *Cir. 1997).*

dell'Autorità Giudiziaria[178]. Il Dipartimento di Polizia sosteneva che non fosse tenuto a rispettare la *privacy* dei suoi dipendenti per messaggi inviati durante l'orario di lavoro. I giudici, tuttavia, argomentarono che le garanzie offerte dal quarto emendamento creano attese di immunità da parte dei dipendenti e che, pertanto, l'azione intrapresa ne violava oggettivamente il diritto alla *privacy*.

Nel 2010, tuttavia, la Suprema Corte ha ribaltato il verdetto favorevole all'imputato, sostenendo che il dipendente era stato adeguatamente avvisato circa la possibilità che venissero effettuate delle verifiche a livello aziendale e che, inoltre, il controllo era stato fatto per motivi legittimi, ossia per verificare il sovraccarico di messaggi che la rete interna del Dipartimento stava subendo[179].

Infine, la giurisprudenza di merito statunitense ha ritenuto che configuri il reato di intralcio alla giustizia *(obstruction of justice)*[180] la distruzione da parte dell'indagato del proprio *hard disk*, prima che sia svolta l'attività di *search and seizure* da parte della polizia giudiziaria[181]. Nel caso in questione, un agente federale aveva compiuto un primo accesso presso l'abitazione dell'indagato sospettato di detenere immagini pedopornografiche e, non avendolo trovato, aveva lasciato il suo biglietto da visita al padre chiedendogli di farlo ricontattare quanto prima dal figlio. Quando, il giorno successivo l'agente era tornato presso l'abitazione dell'indagato, aveva trovato il suo *computer* privo di *hard disk*. La sera prima, infatti, l'indagato aveva deciso di distruggere e smagnetizzare il proprio *hard disk* al fine "di evitare a priori problemi con la giustizia".

La difesa ha sostenuto che il comportamento del proprio assistito era tutelato dai principi sanciti dal quarto e dal quinto emendamento: da un lato, infatti, l'indagato ha sempre il diritto di disporre a suo piacimento di un bene di sua proprietà, prima che s'instauri una valida azione legale nei suoi confronti, e, dall'altro, l'accesso da parte dell'agente federale era avvenuto senza un preciso mandato *(warrant)*.

---

[178] *Jerilyn Quon vs. Arch Wireless Operating Company, 07-55282 (9th Cir.2008).*

[179] *City of Ontario vs. Quon (No. 08-1332) 529 F.3d 892 (2010).*

[180] 1*8 U.S. Code § 1519* - Destruction, alteration, or falsification of records in Fed*eral* investigations and bankruptcy: «*Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both*».

[181] *United States vs. Hicks*, 2011 WI, 2728353.

La Corte di Appello ha, tuttavia, ritenuto che l'avviso effettuato il giorno prima avesse garantito la facoltà di esercitare i diritti previsti dal quinto emendamento e che l'indagato non avesse alcun rilevante diritto di proprietà su delle immagini pedopornografiche. La Corte, quindi, sembra aver dato per scontato che *l'hard disk* contenesse solo immagini pedo pornografiche e non anche altri *file* per cui l'interessato avrebbe potuto esercitare legittimamente il proprio diritto di proprietà.

In Italia una condotta simile avrebbe probabilmente configurato il reato di frode processuale, in forza del quale è punita ogni forma di alterazione dei luoghi in caso di ispezione o accertamento urgente da parte della polizia giudiziaria[182].

4.1.6. *Modalità operative nell'individuazione del dato digitale.*

La *digital evidence* presenta un'intrinseca caratteristica di fragilità, tale per cui può essere facilmente alterata, danneggiata o distrutta, anche per colpa degli stessi investigatori o esaminatori. Per questo motivo è importante, oltre ad un'ottima conoscenza dello strumento informatico, anche il rispetto di una corretta metodologia delle operazioni di raccolta degli elementi probatori, che dovrà comprendere sia le tecniche prettamente informatiche (acquisizione della copia *bit-stream dell'hard disk*, analisi *host*, analisi *file* di *log)*, che le tecniche investigative tradizionali (verbale di sommarie informazioni con le persone coinvolte, esame dello stato dei luoghi). È stato correttamente osservato, da alcuni autori, che la creazione di linee guida sulle modalità operative da utilizzare in caso di un'indagine informatica limita l'attività investigativa, sia perché esse potrebbero, in breve tempo, diventare obsolete, sia perché l'analisi di uno strumento così complesso come l'elaboratore elettronico è difficilmente riconducibile a rigidi schemi[183]. In questo senso, la giurisprudenza statunitense ha affermato che «l'investigazione digitale deve essere considerata più un'arte che una scienza», criticando ogni forma di limitazione alle metodologie investigative in ambito informatico[184]. Sarà, quindi, opportuno stabilire regole, protocolli e principi che consentano di garantire l'autenticità, l'accuratezza e l'attendibilità delle prove raccolte durante l'attività d'indagine, senza tuttavia specificare le

---

[182] Sull'estensibilità della frode processuale *ex* art. 374 c.p. agli accertamenti urgenti sui luoghi, sulle cose e sulle persone si veda Cass. Pen., Sez. III, 26 settembre 1996, n. 8699.

[183] G. COSTABILE, *Scena criminis, documento informatico e formazione della prova penale,* disponibile al seguente URL: http://www.penale.it/page.asp?mode=l&IDPag=72.

[184] *United States vs. Brooks, 427 F.3d 1246, 1252 (l0th Cir. 2005).*

tecniche investigative che sarebbero comunque soggette a una rapida obsolescenza[185].

Durante la fase dell'individuazione della prova digitale, sono necessarie tre operazioni preliminari: la corretta descrizione dell'ambiente, l'individuazione dei soggetti utilizzatori dei supporti e la valutazione del grado di competenza tecnica dell'indagato. L'analisi dell'ambiente in cui è collocato il *personal computer*, attraverso una documentazione fotografica e, ove possibile, riprese video, riveste una grande importanza in quanto, molto spesso, chi effettuerà la successiva perizia del materiale sequestrato potrebbe non aver partecipato alla relativa fase della perquisizione[186]. Anche in questo caso, tuttavia, si potrebbero porre dei legittimi dubbi su quali debbano essere le condizioni necessarie per ritenere scientifiche e non alterate le immagini e le riprese digitali effettuate durante la perquisizione[187].

Successivamente, sarà necessario comprendere, tramite l'ausilio dei verbali di sommarie informazioni testimoniali fornite da persone informate sui fatti, o di spontanee dichiarazioni da parte dell'indagato, quali soggetti avessero la concreta possibilità di accedere ai supporti informatici oggetto di indagine[188].

L'Autorità Giudiziaria, infatti, in vista di una corretta attribuzione delle responsabilità, non deve mai escludere l'ipotesi che il legittimo proprietario del *personal computer* possa essere assolutamente all'oscuro dell'illecito commesso[189].

L'ultima operazione preliminare da compiere è quella di ricercare elementi accessori ai supporti informatici, utili per dimostrare il livello di conoscenze informatiche dell'indagato e valutarne, quindi, il grado e il livello di colpevolezza.

La presenza, o meno, di appunti, diari, note, dai quali si possano

---

[185] O. SIGNORILE, *Computer Forensics Guidelines*: *un approccio metodico procedurale per l'acquisizione e l'analisi della digital evidence,* in *Ciberspazio e Diritto,* Enrico Mucchi Editore, Modena, 2009.

[186] Come nel caso dell'ispezione, è consigliabile allegare al verbale di perquisizione una documentazione fotografica dello stato dei luoghi.

[187] Sull'ampio tema dell'*image forensic*, si veda: S. BATTIATO, G. MESSINA, S. RIZZO, Im*age Forensics. Contraffazione Digitale e identificazione della camera d'acquisizione: status e prospettive*, in IISFA Memberbook, Experta Edizioni, Forlì, 2009, A. SWAMINATHAN, K. J. RAY Liu, *Digital Image Forensics via Intrinsic Fingerprints*, in *IEEE Transactions on Information Forensics and Security*, marzo 2008, disponibile al seguente URL: http://sig.umd.edu/publications/Swaminathan_TIFS_200803.pdf.

[188] Per approfondire si veda C. CHASKI, *Who's at the keyboard: Authorship attribution in digital evidence investigations*, in *International Journal of Digital Evidence*, disponibile al seguente URL: https://www.utica.edu/academic/institutes/ecii/publications/articles/B49F9C4A-0362-765C-6A235CB8ABDFACFF.pdf.

[189] L. CHIRIZZI, *Computer Forensic, la ricerca della fonte di prova informatica,* Laurus Robuffo, Roma, 2006, p. 20.

eventualmente ricavare *password* o chiavi di cifratura, o di riviste specializzate nel settore informatico, potrebbero essere degli utili indici per escludere o avvalorare l'ipotesi che il *computer* sia stato violato attraverso l'utilizzo di strumenti informatici, e che quindi il reato non sia stato compiuto dal soggetto indagato, ma da una terza persona che si sia introdotta nel suo *computer*[190]. Allo stesso modo, tali elementi possono consentire di valutare la reale volontà dell'utente di commettere l'illecito: il Tribunale di Brescia, ad esempio, in una pronuncia in tema di detenzione illecita di materiale pedopornografico, ha ritenuto che non vi fosse consapevolezza, da parte dell'imputato, dell'aver scaricato materiale pedopornografico, in quanto il *file,* protetto da *password,* poteva essere ragionevolmente scambiato per l'aggiornamento di un videogioco[191].

Questo esempio dimostra l'importanza di una seria verifica, durante la fase dell'ispezione e della perquisizione, di tutti gli elementi che possono dimostrare l'effettiva conoscenza dello strumento informatico da parte dell'indagato, al fine di portare utili elementi di valutazione durante la successiva fase dibattimentale. Dopo aver terminato queste tre importanti operazioni preliminari, sarà possibile concentrarsi sui supporti informatici oggetto della perquisizione.

In questa fase sarà opportuno verificare, preliminarmente, se l'elaboratore elettronico sia acceso oppure spento. Qualora l'elaboratore venga trovato spento, sarà necessario aprire il relativo carrello, per verificare la presenza all'interno di eventuali supporti ottici (cd o dvd), utilizzando l'apposito foro presente nella quasi totalità dei lettori ottici. Si dovrà, in seguito, aprire l'elaboratore per identificare il numero e le caratteristiche tecniche dei dischi fissi presenti al suo interno e, ove possibile, avere conferma da parte dell'indagato che i dati presenti in esso siano esclusivamente riconducibili alla sua persona. Nel caso, invece, in cui l'elaboratore sia trovato in funzione, l'indagine diventa più delicata, perché potrebbe essere utile o addirittura necessario recuperare tutti i dati volatili presenti all'interno della RAM che verrebbero persi con l'arresto del sistema operativo.

---

[190] Gli strumenti utilizzati per controllare da remoto un *computer* sono molti: a titolo esemplificativo si citano la *botnet* e il *rootkit.* La *botnet* è una rete di *computer* collegati a Internet controllato da un'unica entità, il *botmaster.* Per un approfondimento si veda E. KARAMATLI, *Modern Botnets: A Survey and Future Directions,* disponibile al seguente URL: http://documents.mx/documents/karamatli-modern-botnets.html. Ciò può essere causato da falle nella sicurezza o mancanza di attenzione da parte dell'utente e dell'amministratore di sistema, per cui i *computer* sono infettati da *malware* i quali consentono ai loro creatori di controllare il sistema da remoto. Il *rootkit* è un *software* che consente di assumere il controllo dell'utente *root,* ossia dell'amministratore del sistema. Dopo che un *hacker* ha installato un *rootkit* sul *computer,* potrà accedere in qualsiasi momento, senza temere di essere rilevato.

[191] Tribunale di Brescia, 22 aprile 2004, Sentenza n. 1619, disponibile al seguente URL: http://www.penale.it/giuris/meri_161.htm.

Le soluzioni possibili per l'acquisizione della RAM sono due:

I. Arrestare il sistema attraverso l'interruzione della corrente ed effettuare un'immediata analisi forense *dell'hard disk* dell'indagato *(guillotine method)*[192];
II. Utilizzare, a *computer* acceso, particolari *software* che consentono di acquisire la memoria volatile senza alterare la prova digitale.

Sempre nel caso in cui l'elaboratore fosse acceso, potrebbe essere determinante l'analisi dell'attività di *download* e delle informazioni relative agli utenti connessi nel caso di utilizzo di *software* di *filesharing*[193]. In tutti questi tipi di operazioni, la Polizia Giudiziaria può avvalersi, ai sensi dell'articolo 348, comma 3, c.p.p., di consulenti tecnici. La loro presenza è particolarmente utile poiché alcune tracce sfuggono agli operatori non professionali: è il caso, ad esempio, dei residui di memoria che hanno subito solo una parziale reimpressione *(slack)*, dei *file* cancellati (per l'utente, non per il sistema), quelli temporanei ancora presenti in memoria, degli *swap* (aree di disco rigido intervenute a supporto della RAM) e dei *dump* (foto della RAM in caso di malfunzionamento).

Durante un'ispezione, qualora fosse necessario acquisire alcuni messaggi di posta elettronica che non sono presenti all'interno dei normali *client* utilizzati per la loro gestione *(Microsoft Outlook, Thunderbird, Mail)*, dovrà essere contattato il *provider* al fine di bloccare tempestivamente l'accesso all'indirizzo di posta elettronica, per poi richiedere l'estrazione delle *email* presenti sul *server*.

Diversamente, l'indagato potrebbe accedere, anche tramite terzi, all'indirizzo di posta elettronica al fine di cancellare i messaggi "sospetti". Al termine di tali operazioni si procederà allo spegnimento dell'*hard disk* staccando la spina dell'alimentazione elettrica in modo da ottenere il più possibile una "fotografia del sistema" così com'era, evitando la cancellazione e l'alterazione di tutti i dati temporanei. Ogni operazione dovrà essere documentata dettagliatamente. Alcuni esperti suggeriscono, a tale scopo, di utilizzare due distinti documenti: uno per la

[192] Per approfondire le modalità di acquisizione della RAM, si veda J. RUTKOWSKA, Beyond The CPU: Defeating Hardware Based RAM Acquisition, disponibile al seguente URL: http://www.blackhat.com/presentations/bh-dc-07/Rutkowska/Presentation/bh-dc-07-Rutkowska-up.pdf.

[193] Per un approfondimento si veda E. HUEBNER, D. BEM, F. HENSKENS, M. WALLIS, *Persistent System Techniques in forensic acquisition of memory*, in *Digital Investigation*, 2007.

descrizione cronologica di tutte le operazioni compiute *(timeline* degli eventi) e l'altro per identificare i supporti informatici e riportare tutte le azioni intraprese per preservare la "catena di custodia" *(chain of custody)* di ogni singolo supporto[194]. È consigliabile, infine, che la redazione del verbale documenti le operazioni compiute con appositi *screenshot:* tutte le attività svolte durante l'eventuale analisi forense devono essere accuratamente registrate in un *file di log*, che consenta di evidenziare se vi siano stati tentativi di alterazione dei dati originali.

4.2. *Acquisizione della Digital Evidence*.

Nei paragrafi che seguono, si andrò ad analizzare l'acquisizione del dato digitale sia utilizzando il "tradizionale" mezzo di ricerca della prova del sequestro, sia attraverso le possibili soluzioni tecnologiche che, se da un lato semplificano la vita all'investigatore, dall'altro rischiano di minare alcuni diritti costituzionalmente protetti a tutela dell'individuo.

4.2.1. *Il sequestro della Digital Evidence*.

Il codice di procedura penale prevede tre distinte forme di sequestro: il sequestro "probatorio"[195] (art. 253 c.p.p.), il sequestro preventivo[196] (art. 321 c.p.p.) ed il sequestro conservativo[197] (art. 316 c.p.p.).

Il primo è collocato tra i mezzi di ricerca della prova, mentre gli altri due sono misure cautelari.

Caratteristica comune ai tre tipi di sequestro, è quella di creare un vincolo di indisponibilità su una cosa mobile od immobile, attraverso uno spossessamento coattivo[198].

---

[194] O. SIGNORILE, *Computer Forensics Guidelines: un approccio metodico procedurale per l'acquisizione e l'analisi della digital evidence*, in Ciberspazio e Diritto, Enrico Mucchi Editore, Modena, 2009.

[195] Il sequestro probatorio ha il compito di assicurare le prove necessarie per l'accertamento del reato assumendo nell'ambito della fase investigativa una notevole importanza. Nel corso delle indagini preliminari è disposto con decreto dal Pubblico Ministero d'ufficio o su richiesta della persona offesa dal reato, mentre durante la successiva fase dibattimentale è ordinato dal Giudice.

[196] Il sequestro preventivo è disposto dal Giudice su richiesta del Pubblico Ministero, quando vi è pericolo che la libera disponibilità di una cosa pertinente al reato possa aggravare o protrarre le conseguenze del reato stesso, o agevolare la commissione di altri reati; inoltre è disposto sulle cose di cui è consentita la confisca.

[197] Il sequestro conservativo ha lo scopo di assicurare l'adempimento delle obbligazioni relative alle pene pecuniarie, alle spese processuali ed alle obbligazioni civili derivanti dal reato.

[198] P. TONINI, *Manuale di procedura penale*, Giuffrè Editore, Milano, 2004.

Il sequestro probatorio è generalmente disposto con decreto motivato da parte del Pubblico Ministero; come già visto in precedenza, ove quest'ultimo non possa intervenire tempestivamente, la Polizia Giudiziaria può fare accertamenti urgenti su luoghi, cose e persone e disporre il sequestro (art. 354, comma 2, c.p.p.). Il verbale è trasmesso entro quarantotto ore al Pubblico Ministero del luogo dove il sequestro è stato eseguito e questi, nelle quarantotto ore successive, convalida il sequestro con decreto motivato, se ne ricorrono i presupposti (art. 355, comma 2, c.p.p.).

Durante la fase delle indagini, invece, il sequestro preventivo è disposto dal Giudice per le indagini preliminari su richiesta del Pubblico Ministero (art. 321 c.p.p.). Anche in questo caso, il Pubblico Ministero e la Polizia Giudiziaria possono disporre il sequestro in casi di urgenza (art. 321, comma 3 *bis*, c.p.p.).

Il Pubblico Ministero, tuttavia, dovrà chiedere al Giudice la convalida del provvedimento entro quarantotto ore dal sequestro o dalla ricezione del verbale se il sequestro è stato eseguito su iniziativa della Polizia Giudiziaria. Il sequestro conservativo, come nel caso precedente, è disposto dal Giudice competente, con ordinanza, su richiesta del Pubblico Ministero o della parte civile. Oggetto del sequestro sono, come già detto, il corpo del reato e le cose pertinenti al reato necessarie per l'accertamento dei fatti.

Il corpo del reato è configurato, secondo la definizione data dall'art. 253, comma 2, c.p.p., non solo dalle cose sulle quali o mediante le quali il reato è stato commesso, ma anche da quelle che ne costituiscono il prodotto, il profitto o il prezzo. Questa seconda locuzione comprende sia le cose acquisite direttamente con il reato o da questo create, sia qualsiasi vantaggio patrimoniale e non patrimoniale ricavato dal reato.

Sono pertinenti al reato, invece, le cose che, per la particolare relazione intercorrente fra cosa e reato, sembrano dotate di una specifica potenzialità probatoria e consentono di accertare, anche indirettamente, la consumazione dell'illecito, il suo autore e le circostanze del reato[199]. In un'indagine informatica, il corpo del reato o le cose pertinenti a esso sono, nella gran parte dei casi, costituiti dai dati digitali contenuti all'interno di un dispositivo di memorizzazione. Ciò pone un problema, in quanto l'art. 253, comma 2, c.p.p. presuppone la materialità del corpo del reato o delle cose pertinenti ad esso,

[199] D. SIRACUSANO, A. GALATI, G. TRANCHINA, E. ZAPPALA, *Diritto processuale penale,* Giuffrè Editore, Milano, 1996.

mentre la *digital evidence* è connotata dall'immaterialità[200]. Alcuni autori hanno agevolmente superato tale assunto, sostenendo che il dato contenuto all'interno di un *computer* è assimilabile a quello presente in un documento cartaceo con l'unica differenza del tipo di supporto su cui tale dato è stato impresso[201]. L'art. 19 della Convenzione sul *Cybercrime* chiarisce espressamente che il sequestro di strumenti informatici può riguardare indistintamente sia l'*hardware* (sistema informatico, o supporto di memorizzazione) sia dati digitali in esso contenuti e presenti all'interno del territorio nazionale[202]. La giurisprudenza di merito, non soffermandosi neppure sulla *vexata quaestio* dell'immaterialità del dato informatico, ha considerato l'*hard disk* l'unico elemento utile da acquisire durante la fase di indagine[203]. Nella stessa pronuncia, il Giudice aveva chiarito, inoltre, che tra *hard disk* e *software* in esso contenuto «sussiste un rapporto di stretta pertinenza, in quanto il *software* necessita dell'*hard disk* per funzionare. Non rileva che il *software* possa funzionare su un altro *hard disk:* sarebbe come dire che un furgone utilizzato dagli autori del furto per trasportare i mobili della casa derubata non sia cosa pertinente al reato, perché gli autori avrebbero potuto usare un altro furgone o semmai un autoveicolo». La giurisprudenza di legittimità si è concentrata sulla distinzione tra il sequestro probatorio della memoria fissa di un *computer* e quello del materiale informatico "neutro" rispetto alle indagini in corso: il caso fu dato da una decisione del Tribunale del Riesame di Siracusa che, in un'indagine legata alla diffusione di materiale pedo-pornografico, aveva qualificato come "cosa pertinente al reato" il materiale informatico utilizzato per "scaricare" i *file* in questione, tra cui lo schermo, la stampante e lo *scanner*

---

[200] S. ATERNO, *La computer forensics tra teoria e prassi,* in *Ciberspazio e diritto,* Mucchi Editore, 2006.

[201] L. CHIRIZZI, *op. cit.,* Laurus Robuffo, Roma, 2006, p. 18.

[202] *Explanatory Report della Convention on Cybercrime*, disponibile al seguente URL: http://conventions.coe.int/treaty/en/reports/html/185.htm chiarisce che l'articolo 19 della Convenzione sul *Cybercrime* è stato scritto proprio perché in molte giurisdizioni è previsto esclusivamente il sequestro di "oggetti fisici". «*This article aims at modernizing harmonising domestic laws on search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law includes powers for search and seizure of tangible objects. However, in a number of jurisdictions stored computer data per se will not be considered as a tangible object, and therefore cannot be secured on behalf of criminal investigations and proceedings in a parallel manner as tangible objects other than by securing the data medium upon which it is stored. The aim of Article 19 of this Convention is to establish an equivalent power relating to stored data*».

[203] La sezione del Riesame del Tribunale di Torino, ha osservato che *«l'hard-disk* è certamente un oggetto pertinente al reato, poiché anche tramite *quell'hard disk*, sia stato utilizzato il *software* necessario per porre in essere i fatti contestati». Tribunale di Torino, Ordinanza del 7 febbraio 2000, disponibile al seguente URL: http://www.ictlex.net/?p=889. Per un commento si veda A. MONTI, *Sequestri di computer. Dal Tribunale di Torino un provvedimento controtendenza,* 15 aprile 2000, disponibile al seguente URL: http://www.ictlex.net/?p=626.

dell'indagato[204]. Nel successivo ricorso in Cassazione, l'indagato aveva, da un lato, sostenuto che uno *scanner* o uno schermo non potevano avere alcuna utilità sotto il profilo probatorio e, dall'altro, aveva lamentato l'illegittimità del sequestro dello stesso *hard disk*, in quanto sarebbe stato sufficiente prelevare una copia forense del suo contenuto. La Suprema Corte ha parzialmente accolto il ricorso, in quanto la motivazione data dal Tribunale di Siracusa sulla sussistenza, in concreto, delle finalità proprie del sequestro probatorio di cose pertinenti al reato, non era adeguata a quella richiesta: non venivano, infatti, minimamente indicate le esigenze probatorie che legittimassero il permanere del vincolo su parte del materiale informatico sequestrato. La stessa Corte, tuttavia, ha ritenuto legittimo il vincolo sulla memoria fissa del *computer*, non prendendo in considerazione l'ipotesi fornita dall'indagato di effettuare una copia dei dati in esso contenuti[205].

Sotto questo ultimo aspetto, il Tribunale di Torino, nell'ordinanza sopra citata, aveva deciso diversamente, in quanto «nulla avrebbe potuto impedire agli agenti di Polizia Giudiziaria, per di più appartenenti a Sezione specializzata nell'ambito dei reati informatici, di procedere a copia integrale dell'*hard disk*, con specificazione a verbale di ogni singola operazione». Il tema è particolarmente dibattuto anche dalla dottrina e vede due differenti orientamenti. Da un lato vi è chi sostiene che potrebbe essere sufficiente garantire la non alterabilità dei dati digitali apponendo, in presenza di testimoni e con le dovute cautele, un sigillo elettronico (impronta di *hash)* sulle cartelle incriminate o sull'intero *hard disk* e poi procedere alla copia sicura *(bit-stream image)* del suo contenuto, lasciando al legittimo proprietario l'originale. Altri autori, tuttavia, sostengono che una simile procedura non tiene conto delle innumerevoli variabili che costituiscono l'espletamento delle indagini e che richiedono di avere a disposizione le cose sotto sequestro per un tempo necessario a un'adeguata ricerca delle fonti di prova[206].

---

[204] Cass. Pen., Sez. III, 18 novembre 2003, n. 1778, disponibile al seguente URL: http://www.ictlex.net/?p=119.

[205] La Suprema Corte ha così motivato la sua decisione: «Considerato che, nel caso in esame è stato sequestrato anche materiale informatico del tutto "neutro" rispetto alle indagini in corso (quale, ad esempio, stampante, *scanner*, schermo); che non vengono minimamente indicate le esigenze probatorie che legittimano il permanere del vincolo sullo stesso; che anche il corpo di reato, quando non appaia più necessario il mantenimento del vincolo per finalità probatorie, deve essere restituito all'avente diritto, *ex* art. 262 c.p.p.; che l'Autorità Giudiziaria può prescrivere, sempre ai sensi della ricordata norma, di presentare a ogni richiesta le cose restituite, e a tal fine può anche imporre cauzione; che la prova in ordine alla sussistenza del reato de quo è verosimilmente tutelabile limitando il sequestro alla memoria fissa del *computer* o ad eventuali supporti (*floppy*, CD) contenenti elementi utili, alle indagini, ritiene il Collegio che non sia legittima l'impugnata ordinanza (peraltro affatto immotivata sul punto) in relazione al sequestro probatorio di tutto il materiale informatico, ad eccezione della memoria fissa del *computer*».

[206] L. CHIRIZZI, *op. cit.*, p. 20.

La Legge di ratifica della Convenzione sul *Cybercrime* ha introdotto l'art. 254 *bis* c.p.p., il quale prescrive che, quando l'Autorità Giudiziaria dispone un sequestro presso i fornitori di servizi informatici, telematici o di telecomunicazioni dei dati da questi detenuti, compresi quelli di traffico e di ubicazione, può stabilire, per esigenze di regolare fornitura dei servizi medesimi, di acquisire tali dati mediante copia, lasciando al fornitore l'onere della conservazione degli originali. Tale norma sembra propendere per l'adozione di una procedura meno invasiva in caso di sequestro di dati digitali; tuttavia va rilevato che tale procedura è solo facoltativa ed è limitata ad una determinata categoria di soggetti *(provider* di servizi e fornitori di connettività). Nella prassi, tre ragioni portano l'Autorità Giudiziaria a propendere per un sequestro integrale *dell'hard disk* senza alcuna copia *bit-stream image* del supporto. La prima risiede nel fatto che, molto spesso, si procede al sequestro di materiale informatico nell'ambito di indagini legate al contrasto della pirateria informatica (Legge 22 aprile 1941 n. 633 e successive modifiche) o della pedopornografia (artt. 603 *ter* e *quater* c.p.): in entrambi i casi è prevista, in caso di condanna, la confisca degli strumenti e dei materiali utilizzati per compiere i relativi reati (art. 171 *sexies* Legge n. 633/41 e art. 600 *septies* c.p.). La seconda è che l'indagato, ai sensi dell'art. 258 c.p.p., ha diritto di chiedere all'Autorità Giudiziaria che sia estratta gratuitamente la copia dei dati contenuti all'interno dell'*hard disk*, a condizione che sia in grado di dimostrare la legittimità del possesso del supporto: in questo modo viene meno anche il possibile pregiudizio che scaturisce nel momento in cui all'interno del *computer* fossero presenti anche dati indispensabili, ad esempio, per la prosecuzione della propria attività lavorativa[207]. Sul tema è opportuno rilevare che la giurisprudenza di legittimità ha ritenuto ammissibile l'istanza di riesame del sequestro, anche qualora sia stata precedentemente fornita una copia di dati digitali all'indagato. Infatti, permane nel richiedente «l'interesse a far verificare che il sequestro sia stato disposto nei casi ed entro i limiti previsti dalla legge»[208].

La terza, già menzionata, è che un procedimento di copia forense di un *hard disk* può avere una durata incompatibile con l'esecuzione, in tempi ragionevoli, del mezzo di ricerca della prova[209].

---

[207] Articolo 258 c.p.p. Copie dei documenti sequestrati: «L'Autorità Giudiziaria può fare estrarre copia degli atti e dei documenti sequestrati, restituendo gli originali, e, quando il sequestro di questi è mantenuto, può autorizzare la cancelleria o la segreteria a rilasciare gratuitamente copia autentica a coloro che li detenevano legittimamente».

[208] Cass. Pen., Sez. VI, 31 maggio 2007, n. 40380.

[209] S.D. WILLIGER, R.M. WILSON, *Negotiating the Minefields of Electronic Discovery*, in

L'incertezza sulle modalità operative del sequestro di supporti informatici sembra comunque destinata a proseguire: emblematica, in tal senso, è l'ordinanza del Tribunale del Riesame di Venezia, con la quale è stato rigettato il ricorso proposto dall'indagato avverso il decreto di sequestro probatorio emesso dal Pubblico Ministero in relazione al reato di divulgazione di materiale pedo-pornografico[210]. Tra le argomentazioni a sostegno del ricorso, il difensore ha contestato la sussistenza della finalità probatoria del sequestro esteso a componenti ulteriori rispetto all'*hard disk*, con richiesta di limitare il sequestro solo a questo. Il Tribunale, non aderendo all'indirizzo della giurisprudenza di legittimità in precedenza descritta, ha rigettato la richiesta, ritenendo che il decreto del Pubblico Ministero avesse spiegato sufficientemente che «nel *personal computer*, nelle relative periferiche nonché nei supporti informatici si sarebbero potute trovare le immagini di pornografia infantile costituenti prove dell'ipotizzato reato *sub* indagine». A tal fine, il Tribunale ha giudicato necessario «un approfondito esame tecnico della strumentazione informatica [...] non potendosi escludere che la disponibilità di tutto il materiale sequestrato possa consentire, o comunque facilitare, operazioni tecniche più complesse quali, ad esempio, la ricerca di tracce *di file* già scaricati e, successivamente, cancellati». Sostenere che all'interno di un *monitor* o di un *mouse* possano annidarsi delle immagini di natura pedopornografica non vuol dire, come è stato sostenuto da alcuni autori[211], "negare la civiltà del diritto", ma è solo un esempio concreto di quanto la cultura delle nuove tecnologie sia ancora del tutto sconosciuta agli operatori del diritto.

Molto più rassicurante è la giurisprudenza di legittimità che ha ritenuto illegittimo il sequestro di un intero "*server*" aziendale disposto in relazione al reato di turbata libertà dell'industria o del commercio, sostenendo che «il Giudice del riesame di un sequestro probatorio deve accertare l'esistenza del vincolo di pertinenzialità tra il reato ipotizzato ed i diversi beni o le diverse categorie di beni oggetto del provvedimento di sequestro»[212].

L'altalenante casistica giurisprudenziale descritta ha, tuttavia, una sua ragion d'essere: ogni indagine è diversa dall'altra e, per questa ragione, le modalità

Richmond Journal of Law and Technology, 2004, Vol. X, Issue 5, disponibile al seguente URL: http://jolt.richmond.edu/v10i5/article52.pdf.

[210] Tribunale di Venezia, Sezione distrettuale del riesame, Ordinanza n. 62/05 del 31 marzo 2005, disponibile al seguente URL: http://www.interlex.it/testi/giurisprudenza/ve050331.htm.

[211] M. CAMMARATA, *Sequestri: se la Polizia viola il domicilio informatico*, in Interlex, 2005, disponibile al seguente URL: http://www.interlex.it/regole/tribvebz.htm.

[212] Cass. Pen., Sez. III, 18 novembre 2008, n. 12107.
Disponibile all'URL: http://www.penale.it/page.asp?mode=1&idpag=764.

operative del sequestro informatico sono da valutare caso per caso. A questo proposito è consigliabile l'utilizzo di una distribuzione *live* di alcuni *software* di forensics (*Helix* o *Caine*) al fine di verificare, preliminarmente e senza alterarlo, il contenuto di un *hard disk* prima di decidere se sequestrare o no[213].

4.2.2. *Sequestro di corrispondenza*.

Sempre sul tema dell'oggetto del sequestro probatorio è opportuno rilevare come la giurisprudenza prima, e il codice di procedura penale poi, abbiano equiparato la corrispondenza tradizionale alla posta elettronica. In altre parole, si è ritenuta applicabile la disciplina dell'art. 254 c.p.p., in forza del quale le carte e gli altri documenti sequestrati che non rientrano fra la corrispondenza sequestrabile, sono immediatamente restituiti all'avente diritto e non possono comunque essere utilizzati. Sul punto, il Tribunale di Torino ha sostenuto come l'inviolabilità della corrispondenza sia espressione di un principio generale, che trova la sua legittimazione nell'art. 15 della nostra Carta Costituzionale[214].

Lo stesso Tribunale ha osservato, tuttavia, che il concetto d'immediatezza, previsto dall'art. 254 c.p.p., debba considerarsi come un concetto relativo, soprattutto qualora il numero delle *email* non consenta un'agevole individuazione di quelle da restituire. Sullo stesso tema è intervenuto il Tribunale del Riesame di Brescia, sostenendo che «il sequestro di un intero *hard disk* consente certamente l'acquisizione di elementi probatori, ma implica anche l'acquisizione di dati che esulano dal contesto per. il quale l'atto è disposto, sicché, come è immediatamente percepibile, tale genere di sequestro esige un ambito di corretta e ristretta operatività per evitare connotazioni di spropositata afflittività e di lesione di beni costituzionalmente protetti. Sotto questo profilo, merita particolare attenzione la compressione della libertà e segretezza della corrispondenza conservata nel disco fisso, con conoscenza di tutti i messaggi inviati o ricevuti, compresi quelli destinati a soggetti del tutto estranei alle indagini»[215].

Tale decisione è stata avallata dalla Suprema Corte, che ha ritenuto illegittimo il sequestro del *computer* in uso ad una giornalista e dell'area del "*server*" dalla stessa gestita, con la conseguente acquisizione dell'intero contenuto

---

[213] G. COSTABILE, *Sicurezza e Privacy: dalla carta ai bit. Manuale per aziende, studi professionali, pubblica amministrazione*, Experta Edizioni, Forlì, 2005.

[214] Trib. Torino, 7 febbraio 2000, disponibile al seguente URL: http://www.ictlex.net/?p=889.

[215] Trib. Brescia, 4 ottobre 2006, disponibile al seguente URL: http://www.ictlex.net/?p=566. Decisione confermata dalla Suprema Corte (Cass. Pen., Sez. VI, 31 maggio 2007, n. 40380).

dell'*hard disk* e di un'intera cartella personale presente nell'area del sistema operativo. Le motivazioni della Corte di Cassazione richiamano quelle del Tribunale del Riesame di Brescia: «il sequestro probatorio, disposto nei confronti di un giornalista professionista, deve rispettare con particolare rigore il criterio di proporzionalità tra il contenuto del provvedimento ablativo di cui egli è destinatario e le esigenze di accertamento dei fatti oggetto delle indagini, evitando, quanto più è possibile, indiscriminati interventi invasivi nella sua sfera professionale»[216]. Lo strumento investigativo del sequestro di corrispondenza sia, da un punto di vista pratico, appare come un'attività molto più simile ad un'intercettazione che non ad un provvedimento ablativo[217]. Dietro un apparente provvedimento di sequestro si celerebbe, infatti, una vera e propria attività captativa di comunicazioni epistolari, che non rispetta, però, le regole stabilite a pena di nullità o inutilizzabilità dagli Artt. 266 e ss. c.p.p., né, ancor prima, la riserva di giurisdizione di cui all'art. 15 della Costituzione così come attuata dal codice di rito. L'art. 8 della Legge di ratifica della Convenzione sul *Cybercrime* ha comportato la modifica del primo comma dell'art. 254 c.p.p. prevedendo, in capo all'Autorità Giudiziaria, di procedere al sequestro presso «i fornitori di servizi postali, telegrafici, telematici o di telecomunicazioni di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica». Anche se il dettato letterale del nuovo art. 254 c.p.p. sembra estendere al sequestro di corrispondenza cartacea quella telematica, parte della dottrina ritiene ancora preferibile ricorrere alle intercettazioni telematiche, poiché tale secondo strumento risulta essere più garantito per l'indagato, essendo necessario l'intervento del Giudice per le Indagini Preliminari.

4.2.3. *Modalità operative nel sequestro della prova digitale*.

Negli ultimi anni le competenze della Guarda di Finanza (che dal 2001 ha istituito il "G.A.T.", Gruppo Anticrimine Tecnologico, oggi denominato Nucleo Speciale Frodi Tecnologiche)[218], dei Carabinieri (con alcuni reparti del "R.O.S.", Raggruppamento Operativo Specializzato)[219], e della Polizia di Stato mediante il

[216] Cass. Pen., Sez. VI, 31 maggio 2007, n. 40380, in *Dir. pen. proc.*, 2008.

[217] Cass. Pen., Sez. II, 23 maggio 2006, n. 20228.

[218] Per ulteriori informazioni sul Gruppo Anticrimine Tecnologico si veda il seguente URL: http://www.gdf.gov.it/reparti-del-corpo/territorio/lazio/roma/nucleo-speciale-frodi-telematiche.

[219] Per ulteriori informazioni sul Raggruppamento Operativo Specializzato si veda il seguente URL: http://www.carabinieri.it/arma/oggi/reparti/organizzazione-mobile-e-speciale/ros.

Servizio Polizia Postale e delle Comunicazioni[220], sono notevolmente cresciute ed hanno raggiunto un livello adeguato ai più alti standard previsti in campo internazionale. Al grado di eccellenza raggiunto dai citati nuclei specializzati, non sempre corrisponde uno standard di conoscenza minimo dello strumento informatico da parte di tutti gli altri componenti delle Forze dell'Ordine. Il risultato è che i nuclei specializzati si trovano talvolta a dover investire del tempo prezioso in indagini che potrebbero essere svolte anche da altri pubblici ufficiali i quali, se adeguatamente formati, potrebbero raggiungere gli stessi risultati, soprattutto nei casi in cui il pericolo sociale non è particolarmente elevato (ad esempio nei casi di diffamazione online o di violazione penale della normativa sulla privacy). Sempre più spesso, la Polizia Giudiziaria si avvale di consulenti nominati in qualità di propri ausiliari, qualora si debbano compiere atti od operazioni che richiedono specifiche competenze tecniche (art. 348 c.p.p.). Questo comporta un potenziale aggravio di costi e di risorse per lo Stato e non sempre garantisce un'esperienza investigativa "tradizionale", che è necessario mantenere anche nel mondo del *cybercrime.*

Le operazioni che dovrebbero essere compiute, durante la fase del sequestro, per garantire la tutela dell'integrità e della genuinità del dato informatico ed evitare successive contestazioni da parte dell'indagato o del suo difensore, sono principalmente due[221].

In primo luogo, una volta individuati i supporti da sequestrare, è necessaria una loro identificazione attraverso le loro caratteristiche tecniche (marca, modello, numero seriale ed etichette apposte). In questa fase, oltre a far siglare dall'indagato il singolo supporto sequestrato, è consigliabile effettuare anche alcune fotografie o una ripresa video, in modo da rendere il più possibile esaustiva la fase dell'identificazione.

---

[220] Per ulteriori informazioni sulla Polizia Postale e delle Comunicazioni, si veda il seguente URL: http://www.poliziadistato.it/articolo/23393-Polizia_postale_e_delle_comunicazioni/.

[221] Per un ulteriore approfondimento a livello statunitense sul tema si veda: E. CASEY, *Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence Invest.,* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.63.7643&rep=rep1&type=pdf;

O. KERR, *Searches and Seizures in a digital world,* in *Harvard Law Review, 2005,* Vol. 119, p. 531; R. NOLAN, C. O'SULLIVAN, J. BRANSON, C. WAITS, *First Responders Guide to Computer Forensics, 2005*; State of Maryland, Maryland State Police, Criminal Enforcement, Command, Computer Crime Unit, Computer Forensics Laboratori, *General Guidelines for Seizing Computers and Digital Evidence*; State of New Jersey, Department of Law and Public Safety, Division of Criminal Justice, *New Jersey Computer Evidence Search and Seizure Manual,* disponibile al seguente URL: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

In ambito Europeo, si consiglia la lettura delle linee guida inglesi dell'Association of Chief Police Officers disponibile al seguente URL: http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.

I supporti devono, successivamente, essere opportunamente imballati e conservati; su di essi devono essere apposte etichette e sigilli indicando il soggetto che ha raccolto le prove e le modalità ed il luogo in cui esse sono state reperite. In secondo luogo, sarà necessario distinguere tra supporti non alterabili (cd e dvd non riscrivibili) e supporti soggetti a modifiche, quali *hard disk, pen drive,* cd e dvd riscrivibili.

Il sequestro di supporti alterabili presuppone il compimento di un'operazione preliminare, che costituisce requisito indispensabile al fine di garantire l'intangibilità dei dati in essi contenuti: l'impronta di *hash*[222].

L'*hash* è una funzione univoca operante in un solo senso (ossia, che non può essere invertita), attraverso la quale viene trasformato un documento di lunghezza arbitraria in una stringa di lunghezza fissa, relativamente limitata. Tale stringa rappresenta una sorta di "impronta digitale" del testo in chiaro, ed è conosciuta come valore di *hash* o *Message Digest.* Se il documento fosse alterato anche in minima parte, cambierebbe di conseguenza anche l'impronta. In altre parole, calcolando e registrando l'impronta, e successivamente ricalcolandola, è possibile mostrare, al di là di ogni dubbio, che i contenuti del *file,* oppure del supporto, abbiano subito o no modifiche, anche solo accidentali. Pertanto, la registrazione e la ripetizione costante del calcolo degli *hash* sui reperti sequestrati costituiscono l'unico metodo scientificamente valido per garantire l'integrità e la catena di custodia dei reperti.

La Polizia Giudiziaria, prima di apporre i sigilli al materiale informatico, ha il compito di collegare il supporto oggetto del sequestro a un *computer* portatile, sul quale dovrà essere eseguito il comando che consente il calcolo dell'impronta di *hash.* Al termine dell'analisi del supporto, sarà generata una sequenza di caratteri (tipicamente 16 oppure 20) che dovrà necessariamente venire trascritta sul verbale di sequestro, al fine di garantire la massima trasparenza nella successiva fase di analisi. Nella pratica, gli algoritmi di *hash* più utilizzati sono il MD2, MD4, MD5 e SHAl; in particolare, il calcolo dell'algoritmo MD5 *(Message Digest 5)* permette di generare una stringa di 128 *bit,* mentre l'algoritmo SHAl genera una stringa a 160 *bit.* L'abbinamento di questi due algoritmi dovrebbe evitare qualsiasi contestazione da parte del difensore, anche se sono stati riscontrati problemi di

[222] Riguardo all'*hash* si veda, S. ARORA, S. SACHDEVA, *Lecture 2: Hashing*, lezione della Princeton University dell'ottobre 2008 finalizzata alla definizione della funzione di *hash,* disponibile al seguente URL: http://www.cs.princeton.edu/courses/archive/fall08/cos521/hash.pdf; V. KLIMA, *Tunnels in Hash Functions: MD5 Collisions Within a Minute,* ricerca del 18 marzo 2006, disponibile al seguente URL: https://eprint.iacr.org/2006/105.

vulnerabilità, che rendono assai più facile del previsto la scoperta di collisioni al suo interno[223]. Per tutte le operazioni di *hashing*, sarebbe opportuno utilizzare *software open source*, ovvero programmi di cui sia conosciuto il "codice sorgente" del *software*, al fine di consentire al consulente o al perito la verifica passo per passo delle operazioni di analisi, validazione ed eventuale confutazione[224]. È consigliabile, inoltre, conservare una copia del *software* usato nella fase dell'acquisizione, perché solitamente i programmi sono aggiornati di frequente, e potrebbero non essere più reperibili durante la fase del dibattimento. Una procedura adottata molto raramente, ma non per questo meno utile, è quella di filmare, con almeno due telecamere, tutte le operazioni effettuate utilizzando un riferimento orario certo, in modo che sia le telecamere sia *l'hardware* usato per l'estrazione dei dati siano sincronizzati con tale riferimento. Inoltre, sarebbe utile effettuare una registrazione digitale dell'*output* dello schermo *(screencast)* di ogni operazione di acquisizione utilizzando uno dei numerosi *software open source* facilmente reperibili in Rete[225].

Ove non fossero adottate le procedure per garantire una corretta "catena di custodia" nella fase investigativa, i dati informatici contenuti nel supporto non avranno più i requisiti di certezza, genuinità e paternità. È, quindi, necessario avere un'elevata conoscenza informatica e disporre di una strumentazione tecnica adeguata, pianificando correttamente le attività di indagine da compiere, definendo in modo circostanziato gli obiettivi, il flusso di lavoro e le varie fasi.

Un cenno a parte meritano i casi in cui debbano essere acquisiti, interamente o no, dei siti *web*. Si è già detto in precedenza del progetto di ricerca denominato *hashbot* che consente di effettuare non solo il *download* delle pagine *web*, ma anche di validare la prova digitale attraverso l'utilizzo della funzione di *hash*.

Alternativamente, sarà sempre possibile acquisire il sito *web* attraverso appositi *tools* liberamente disponibili in Rete *(HTTrack o Wget)* oppure accedendo al *file system* del *server* del sito da remoto.

---

[223] C. GIUSTOZZI, Hash *sempre più vulnerabili, ma la firma digitale non è a rischio* in Interlex n. 314 del 7 marzo 2005, URL: http://www.nightgaunt.org/testi/interlex/sha1.htm.

[224] S. ZANERO, E. HUEBNER, *The Case for Open Source Software in Digital Forensics*, in *Open Source Software for Digital Forensics*, 2010, Springer; C. ALTHEIDE, H. CARVEY, *Digital Forensics with Open Source Tools*, Elsevier, Waltham, 2011. Il codice sorgente è un insieme di istruzioni appartenenti ad un determinato linguaggio di programmazione, utilizzato per realizzare un programma per *computer*.

[225] Alcuni dei *software* più utilizzati sono: RecordMyDesktop disponibile al seguente URL: http://recordmydesktop.sourceforge.net/about.php.

4.2.4. *La Remote forensics*.

E' stata fonte di dibattito la possibilità di introdurre sia in Europa che negli Stati Uniti la possibilità di introdurre un mezzo di ricerca della prova che consenta alle forze di polizia l'accesso remoto sugli strumenti informatici *(notebook, server, smartphone)* in uso alla persona sottoposta ad indagini. Sempre più spesso accade che la Polizia Giudiziaria non conosca il luogo in cui è collocato il *server* che contiene i dati incriminati, in quanto l'indagato ha utilizzato risorse *hardware* o *software* distribuite in remoto per memorizzare ed elaborare i dati digitali[226]. La popolarità del fenomeno del *cloud computing*[227], inoltre, ha reso ancor più difficile l'investigazione tradizionale: se è vero, infatti, che grazie al *cloud computing* chiunque può accedere a un determinato dato da qualunque parte del mondo, od utilizzare un determinato applicativo senza averlo installato nel proprio *computer*, è anche vero che un criminale informatico può decidere di memorizzare i suoi dati all'interno di un *server* dislocato al di fuori del territoriale nazionale e, magari, in uno Stato che non ha accordi di cooperazione giudiziaria con quello in cui risiede. Per contrastare tale fenomeno, gli Stati firmatari della Convenzione sul *Cybercrime* hanno dettato numerose disposizioni per contrastare tale fenomeno, tra cui vanno ricordati gli Artt. 18 *(Production order),* 19 *(Search and seizure of stored computer data)* e 20 *(Real-time collection of traffic data).* L'art. 18 della Convenzione sul *Cybercrime*[228] ha introdotto la possibilità per l'Autorità Giudiziaria, di ordinare *(production order)* a qualunque soggetto (inclusi quindi i *provider)* di fornire i dati digitali presenti all'interno di un sistema informatico o di un *server* in suo possesso o sotto il suo controllo[229].

Nella convenzione vengono utilizzati i termini '*possession*' e '*control*' per indicare che sono obbligati a fornire i dati sia i soggetti che vi possono accedere

---

[226] O. KERR, *Searches and Seizures in a digital world,* in Harvard Law Review, 2005, Vol. 119.

[227] Per un approfondimento sulla tecnologia "*Cloud Computing*", si suggerisce una ricerca del centro di ricerca Pew, della Elon University, dal titolo *The Future of cloud computing,* disponibile al seguente URL: http://www.pewinternet.org/2010/06/11/the-future-of-cloud-computing/.

[228] Art. 18 Convenzione sul *Cybercrime*: «*Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: (a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and (b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control*».

[229] M. GERCKE, *Understanding Cybercrime: A Guide For Developing Countries,* p. 192, disponibile al seguente URL: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.

fisicamente, sia quelli che hanno la possibilità di accedervi da remoto[230].

L'ordine di produzione riguarda sia le informazioni di registrazione dell'utente a un determinato servizio (indirizzi IP e i *file* di *log)* sia i contenuti dei dati. È stato osservato che tale misura potrebbe riguardare dati relativi a soggetti che si trovano al di fuori del territorio dello Stato, purché essi risultino abbonati con un fornitore che offre i propri servizi (anche) nello Stato richiedente[231].

Questa interessante interpretazione, tuttavia, è in contrasto con il principio di sovranità e in ogni caso potrebbe applicarsi ai soli dati di registrazione dell'utente (art. 18 *sub* b), poiché, per quanto riguarda i contenuti dei suoi *file* (art. 18 *sub* a), emerge chiaramente che l'ordine può essere eseguito solo nei confronti di *provider* presenti all'interno del territorio dello Stato richiedente[232].

L'art. 19 stabilisce che, nel caso in cui la Polizia Giudiziaria scopra che i dati digitali ricercati risiedono all'interno di un altro *server,* è autorizzata ad estendere la ricerca su di esso, salvo che non si trovi al di fuori del territorio nazionale[233]. Tuttavia, anche nel caso in cui i dati siano memorizzati in un *server* che si trova all'interno del confine nazionale, si possono incontrare notevoli difficoltà nell'individuare il dato ricercato a causa del volume di dati in esso contenuti.

---

[230] Sul tema si veda l'art. 171 dell'*Explanatory Report* «[...] *The term 'possession or control' refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory (for example, subject to applicable privileges, a person who is served with a production order for information stored in his or her account by means of a remote online storage service, must produce such information). At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute 'control' within the meaning of this provision. In some States, the concept denominated under law as 'possession' covers physical and constructive possession with sufficient breadth to meet this 'possession or control' requirement*».

[231] F. LICATA, *La Convenzione del Consiglio d'Europa sul cybercrime e le forme della cooperazione giudiziaria: una risposta globale alle nuove sfide della criminalità transnazionali,* in *Atti dell'incontro di Studio del Consiglio Superiore della Magistratura tenutosi a Roma il 19 settembre 2005*.

[232] Sul tema si veda l'art. 170 *dell'Explanatory Report*: «*Paragraph 1 of this article calls for Parties to enable their competent authorities to compel a person in its territory to provide specified stored computer data, or a service provider offering its services in the territory of the Party to submit subscriber information. The data in question are stored or existing data, and do not include data that has not yet come into existence such as traffic data or content data related to future communications. Instead of requiring States to apply systematically coercive measures in relation to third parties, such as search and seizure of data, it is essential that States have within their domestic law alternative investigative powers that provide a less intrusive means of obtaining information relevant to criminal investigations*».

[233] A questo proposito si veda l'art. 193 *dell'Explanatory Report* sul *Cybercrime*: «*Paragraph 2 allows the investigating authorities to extend their search or similar access to another computer system or part of it if they have grounds to believe that the data required is stored in that other computer system. The other computer system or part of it must, however, also be 'in its territory'*».

In questo caso, la Convenzione ha stabilito che gli investigatori possono ordinare all'amministratore di sistema di quel *server* di collaborare con la Polizia Giudiziaria e di fornire, ove possibile "*as is reasonable*"[234], le informazioni necessarie[235].

L'art. 20, infine, prevede la possibilità di raccogliere in tempo reale i *traffic data*[236], che servono a monitorare in tempo reale l'attività dell'indagato in Rete (siti *web* visitati, intestazione delle *email* scambiate, *downloads* effettuati).

La Convenzione sul *Cybercrime* indica due distinte metodologie finalizzate allo sviluppo della normativa nazionale: la prima prevede che i *provider* siano obbligati a fornire un'interfaccia *software* alla Polizia Giudiziaria, che gli consenta di prelevare direttamente i dati utili all'indagine; la seconda stabilisce uno specifico obbligo per i *provider* di raccogliere i *traffic data* su richiesta della Polizia Giudiziaria. Come già osservato per il caso del sequestro della corrispondenza telematica, le misure previste dagli Artt. 18 ("*Production order*") e 20 ("*Real-time collection of traffic data*") presentano delle caratteristiche molto simili all'attività di intercettazione, per la quale sono previste specifiche limitazioni conformemente all'articolo 8 della Convenzione europea per la tutela dei diritti dell'uomo[237]. Questi tre importanti strumenti offerti dalla Convenzione sul *Cybercrime* non sono stati presi in considerazione dalla normativa italiana in modo adeguato.

Se è vero che le attuali previsioni del codice di procedura penale offrono gli strumenti processuali per raggiungere i medesimi risultati (nomina dell'ausiliario di Polizia Giudiziaria ai sensi dell'art. 348, comma 4, richiesta di consegna ai sensi

---

[234] Sul tema si veda l'art. 202 *dell'Explanatory Report* della Convenzione sul *Cybercrime*: «*The provision of this information, however, is restricted to that which is "reasonable". In some circumstances, reasonable provision may include disclosing a password or other security measure to the investigating authorities. However, in other circumstances, this may not be reasonable; for example, where the disclosure of the password or other security measure would unreasonably threaten the privacy of other users or other data that is not authorised to be searched. In such case, the provision of the "necessary information" could be the disclosure, in a form that is intelligible and readable, of the actual data that is being sought by the competent authorities*».

[235] Un approccio simile è stato trovato durante gli incontri effettuati nel 2002 da un gruppo di esperti in crimini informatici che hanno redatto un modello legislativo per l'applicazione della Convenzione sul *Cybercrime* in tutti i Paesi aderenti al *Commonwealth*.

[236] I "dati di traffico" comprendono tuttavia anche gli indirizzi IP dell'utente e quindi ne consentono una sua localizzazione.

[237] In questo senso l'art. 14, comma 3 della Convenzione sul *Cybercrime* precisa in riferimento all'art. 20 che: «*Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20*».

dell'art. 248 c.p.p. e intercettazione telematica ai sensi dell'art. 266 *bis* c.p.p.), è pur vero che la Legge di ratifica della Convenzione sul *Cybercrime* ha perso un'importante occasione per poter effettuare alcune doverose precisazioni in materia. Ad esempio, l'obbligo per i *provider* di fornire un'interfaccia *software* alla Polizia Giudiziaria avrebbe potuto velocizzare l'attività d'indagine e garantire un minor rischio di alterabilità dei dati. Nella procedura attuale, infatti, i *provider* forniscono le informazioni relative ai *file* di *log* o all'indirizzo IP dell'indagato, estrapolando i dati richiesti senza nessun accorgimento previsto dalle *best practice* di *digital forensics* soprattutto nella trasmissione alla Polizia Giudiziaria che, alle volte, avviene con *email* non firmate digitalmente, né inviate tramite posta elettronica certificata. Oltre agli strumenti indicati, in molti Paesi europei sono al vaglio progetti di legge per garantire l'accesso remoto da parte della Polizia Giudiziaria sui *computer* degli indagati[238]. Negli Stati Uniti, il *Federal Bureau of Investigation* (FBI), invece, ha già sperimentato con successo l'utilizzo di un particolare tipo di *spyware CIPAV*[239] che ha la funzione di raccogliere informazioni riguardanti l'attività *online* dell'indagato e di ritrasmetterle in tempo reale agli investigatori[240].

Alla luce di quanto sopra esposto, emerge chiaramente come la possibilità di effettuare l'attività investigativa rimanendo davanti allo schermo di un *computer* e senza che l'indagato ne sia a conoscenza, rappresenti un indiscutibile vantaggio e una garanzia di successo per l'indagine.

Tuttavia, i vantaggi di questa metodologia investigativa così invasiva potrebbero arrecare notevole pregiudizio ad alcuni diritti fondamentali del soggetto sottoposto all'indagine. Occorre quindi prestare la massima attenzione alla tutela di tutti gli interessi in gioco, bilanciando attentamente le esigenze di prevenzione e di sicurezza con la tutela dei diritti fondamentali, come quello della *privacy* e delle garanzie dell'indagato. A questo proposito, la giurisprudenza di legittimità non si sia posta alcun problema circa la validità di decreto del Pubblico Ministero che, ai sensi dell'art. 234 c.p.p., ha disposto l'acquisizione in copia

---

[238] J. BLAU, *Debate rages over German government spyware plan*, 5 settembre 2007, in InfoWord, URL: *http://www.infoworld.com/article/2649377/security/debate-rages-over-german-government-spyware-plan.html*.

[239] CIPAV è l'acronimo di *Computer and Internet Protocol Address Verifier*.

[240] Per ulteriori informazioni sul progetto *CIPAV* suggerisce la lettura di questi due articoli apparsi sulla rivista Wired: K. POULSEN, *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats,* 18 luglio 2007, disponibile al seguente URL: http://www.wired.com/2007/07/fbi-spyware/; *Documents: FBI Spyware Has Been Snaring Extortionists, Hackers for Years*, 16 aprile 2009, disponibile al seguente URL: https://www.wired.com/2009/04/fbi-spyware-pro/#ixzz0vH9IUa6v.

attraverso l'installazione di un captatore informatico, della documentazione informatica memorizzata nel *personal computer* in uso all'imputato e installato presso un ufficio pubblico. La Suprema Corte ha, infatti, evidenziato come il provvedimento del Pubblico Ministero non avesse riguardato un flusso di comunicazioni, ma la semplice estrapolazione di dati già formati e contenuti nella memoria del "*personal computer*", ossia "un flusso unidirezionale di dati" confinati all'interno dei circuiti del *computer*[241]. La Corte ha, altresì, escluso che, nella specie, «dovesse essere osservata la disciplina prevista per gli accertamenti tecnici irripetibili, atteso che l'attività di riproduzione dei *file* memorizzati non aveva comportato l'alterazione, né la distruzione dell'archivio informatico, rimasto immutato, quindi consultabile ed accessibile nelle medesime condizioni, anche dopo l'intervento della polizia giudiziaria». Secondo i giudici della Corte di Cassazione si è trattato di un'attività sempre reiterabile, alla cui esecuzione non era necessaria la partecipazione del difensore, poiché la stessa sarebbe potuto essere compiuta una seconda volta, nel caso in cui si fosse giunti ad uno sviluppo dibattimentale del procedimento, cosa che poi non avvenne poiché fu preferito il "rito abbreviato".

La difesa, invece, aveva eccepito che il decreto del Pubblico Ministero, pur autorizzando una mera acquisizione in copia di atti, avrebbe costituito, di fatto, la premessa per condurre un'attività d'intercettazione di comunicazioni informatiche ai sensi dell'art. 266 *bis* c.p.p. Il decreto, infatti, aveva disposto la registrazione non solo dei *file* esistenti, ma anche dei dati che sarebbero stati inseriti in futuro nel *personal computer*, in modo da acquisirli periodicamente.

A dimostrazione di tale tesi, sono state evidenziate le concrete modalità esecutive del decreto, consistite nell'installazione, all'interno del sistema operativo del *personal computer*, di un captatore informatico *(ghost)* in grado di memorizzare i *file* già esistenti e di registrare in tempo reale tutti i *file* in via di elaborazione, in tal modo innescando un monitoraggio occulto e continuativo del *computer* dell'indagato (protrattosi per oltre otto mesi). In primo luogo, la Corte non sembra considerare come la presunta ripetibilità presupponga l'assenza di un intervento sul *personal computer* da parte del soggetto indagato in un momento successivo alla fase di captazione. In secondo luogo, la Corte, per escludere la disciplina delle intercettazioni telematiche, ha evidenziato come il flusso di comunicazioni acquisito non abbia riguardato una conversazione telematica tra

[241] Cass. Pen., Sez. V, 14 ottobre 2009, n. 16556.

due soggetti, ma solo un "flusso di comunicazioni unilaterale".

A tal proposito l'art. 266 *bis* non è affatto chiaro sul punto, poiché prevede che la captazione riguardi «un flusso di comunicazione relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi» e, rileva, come sia estremamente delicata la scelta di stabilire che un'operazione così invasiva come il monitoraggio occulto di un *computer* per un periodo prolungato di tempo possa essere autorizzato senza il vaglio del Giudice per le indagini preliminari.

4.2.5. *Intercettazioni telematiche: disciplina italiana e statunitense*.

Le intercettazioni telematiche avranno nel prossimo futuro un ruolo investigativo sempre più importante e decisivo, attraverso di esse è possibile controllare l'intero flusso di dati *(email* inviate e ricevute, siti *web* visitati, comunicazioni *VoIP* non criptate, *download* ed *upload* di *file*, conversazioni in *chat room)* del sistema informatico attenzionato. Le recenti statistiche dimostrano che, a livello europeo, l'Italia è il paese che fa più largo uso dell'intercettazione come mezzo di ricerca della prova nella fase delle indagini[242]. Negli ultimi anni, il Ministero di Giustizia italiano ha speso un miliardo e 800 milioni di dollari (1,3 miliardi di euro) per poter conseguire il seguente primato europeo: un cittadino ogni 500 abitanti è intercettato, nel 2013 sono state formulate oltre 605.000 richieste di intercettazioni.[243]

Va osservato tuttavia che questi dati riguardano principalmente le intercettazioni telefoniche e non quelle telematiche, in quanto in Italia, nonostante ogni giorno vengano scambiate oltre 940 milioni di *email*, non sono ancora sufficientemente note le enormi potenzialità di questo tipo di intercettazioni.

Negli Stati Uniti, le statistiche relative alle intercettazioni sono molto diverse, in quanto le richieste autorizzate di intercettazioni durante il 2014 sono state 3554 di cui 1279 da Giudici federali e le restanti 2275 a livello statale[244].

Una *email*, a differenza di una telefonata, può essere immediatamente

---

[242] J. LEYDEN, "*Italy tops global wiretap league. State of the surveillance nation*", del 7 marzo 2007, URL http://www.theregister.co.uk/2007/03/07/wiretap_trends_ss8/; per un approfondimento sui costi delle intercettazioni in Italia: S. Sansonetti del 2 luglio 2014, http://www.dagospia.com/rubrica-3/politica/girone-dantesco-intercettazioni-2009-2013-procura-80146.htm.

[243] Fonte Il Sole 24 ore. http://www.ilsole24ore.com/art/notizie/2014-06-06/intercettazioni-legali-telefonate-vodafone-italia-testa-oltre-600mila-richieste122934.shtml?uuid=AB0TQaOB&refresh_ce=1

[244] Per un approfondimento sulle intercettazioni negli U.S.A., Wiretap Report U.S.A. 2014, Fonte U.S. Courts: http://www.uscourts.gov/statistics-reports/wiretap-report-2014.

indicizzata con chiavi di ricerca determinate; inoltre, al suo interno, può trovarsi materiale potenzialmente utile alle indagini: si pensi, ad esempio, a della documentazione allegata, la cui lettura ed analisi può rendere più facile la comprensione del contesto del discorso.

Negli Stati Uniti le intercettazioni telematiche sono regolate, in particolare, dall'*Electronic Communications Privacy Act*, emanato nel 1986[245].

Con l'emanazione di tale atto legislativo, è stato chiarito che ogni intercettazione che non rispetti le condizioni previste dalla legge deve essere considerata illegale e, oltre a comportare l'inutilizzabilità delle informazioni così acquisite all'interno del processo, può determinare un'azione di risarcimento del danno rivolta nei confronti del responsabile. La normativa generale sulle captazioni del contenuto delle comunicazioni elettroniche e sui controlli agli accessi in Rete è invece ricompressa in tre atti normativi distinti: il primo, come appena visto, è dedicato specificamente alle intercettazioni delle comunicazioni telematiche *(Electronic Communications Privacy Act,* 18 U.S.C. § 2510), il secondo regola la possibilità di accedere ai contenuti memorizzati all'interno di un *computer* o di un *server (Stored Communications* Act, 18 U.S.C. § 2701) e il terzo riguarda la possibilità di monitorare gli accessi alla Rete da parte degli utenti, senza tuttavia poter conoscere il contenuto delle loro comunicazioni *(Pen Register Act,* 18 U.S.C. § 206). Teoricamente, tra questi tre atti, solo il primo riguarda specificamente le captazioni in tempo reale di informazioni digitali; tuttavia, ritengo opportuno effettuare una trattazione congiunta dei tre provvedimenti legislativi in quanto, come già detto per il caso della corrispondenza elettronica, è molto sottile la differenza tra l'intercettazione di una *email* attraverso un sistema di duplicazione della casella di posta elettronica, e un accesso alla casella di posta elettronica nella forma prevista dallo *Store Communications Act*. Per capire la sottile distinzione tra *Store Communications Act* e *Electronic Communications Privacy Act,* è utile citare il famoso caso "Scarfo". Per investigare il noto esponente della mafia russa Nicky Scarfo, il *Federal Bureau of Investigation* (FBI) installò un *keylogger* nel suo *computer* per intercettare le comunicazioni che il pregiudicato si scambiava con alcuni membri dell'organizzazione criminale. Tali comunicazioni, tuttavia, erano carpite solo quando il *computer* era *offline* in modo da non "intercettare comunicazioni in transito" e conseguentemente non rientrare

[245] *Electronic Communications Privacy Act,* 18 U.S.C. § 2510.

nella disciplina dell'*Electronic Communication Privacy Act*[246].

Sebbene in tutte e tre le ipotesi, il Pubblico Ministero debba ottenere un *warrant* da parte del Giudice competente (statale o federale in relazione al tipo di reato per cui si procede) prima che le forze di polizia o il *Federal Bureau of Investigation* possano procedere, quest'obbligo non è applicato rigidamente.

Infatti, nel caso delle informazioni memorizzate all'interno di un *computer* o di un *server (Stored Communication Act),* vi sono alcune specifiche eccezioni: nel caso in cui il *provider* si renda conto, per circostanze casuali, di un concreto e serio pericolo di vita di un soggetto; nel caso in cui debba tutelare i suoi diritti qualora fosse vittima di una frode[247]; ovvero nel caso in cui debba informare il *National Centre for Missing and Exploited Kids* per un'ipotesi di pedofilia *online,* può accedere ai contenuti memorizzati dal suo utente senza alcun mandato. Inoltre, è possibile che le sole informazioni relative all'identità di un determinato utente (e non quindi i contenuti delle sue comunicazioni) possano essere ottenute anche attraverso una diffida *(subpoena)* che, tuttavia, non può essere fatta da un privato, ma deve comunque essere richiesta dall'Autorità Giudiziaria.

Nel caso del monitoraggio, invece, il *Pen Register Act* a partire dal 2001 ha subito sensibili modifiche con il *Patriot Act* e con l'introduzione della *National Security Letter,* che hanno consentito una deroga notevole al principio generale. La *National Security Letter* è una forma di *subpoena* di natura amministrativa, utilizzata dal *Federal Bureau of Investigation,* in forza della quale viene concessa a tale organo investigativo la possibilità di richiedere il monitoraggio di alcune informazioni (nome dell'utente, indirizzo, registro delle transazioni, intestazioni delle *email),* senza sostanzialmente alcuna previa autorizzazione da parte del Giudice[248]. In Italia, la Legge n. 547 del 23 settembre 1993, oltre ad aver introdotto la disciplina relativa ai reati informatici, ha previsto anche uno specifico mezzo di ricerca della prova, vale a dire le intercettazioni del flusso di comunicazioni relativo a sistemi informatici o telematici[249].

---

[246] *United States vs. Scarfo, 180 F. Supp. 2d 572, 581-82 (D.N.]. 2001).*

[247] *Unitled States vs. Harvey, 540 F.2d 1345, 1350-52 (8th Cir. 1976).*

[248] La *National Security Letter* dava anche la facoltà al *Federal Bureau of Investigation* (FBI) di impedire che terzi avessero l'obbligo di mantenere segreta l'attività di monitoraggio che stavano svolgendo, ma anche l'esistenza stessa della lettera. Tale facoltà venne dichiarata incostituzionale con il caso *Ashcroft vs. ACLU, 542 U.S. 656, 665-66 (2004).*

[249] Tale legge, infatti, ha aggiunto al codice di procedura penale l'art. 266 *bis* ed il comma 3 *bis* dell'art. 268, accostando alle intercettazioni telefoniche ed ambientali, l'intercettazione telematica. Per un approfondimento: C. MAIOLI, R. CUGNASCO, *Profili normativi e tecnici delle intercettazioni. Dai sistemi analogici al voice over IP,* Gedit Edizioni, Bologna, 2008.

Preliminarmente, occorre chiarire cosa s'intende per sistema informatico e sistema telematico, in quanto ad oggi, a livello nazionale, come si è già detto in precedenza, non esiste alcuna definizione normativa. Al di là delle definizioni che la giurisprudenza di legittimità ha cercato di elaborare, con risultati non sempre soddisfacenti[250], possiamo dire che:

- per "*sistema informatico*", si intende ogni elaboratore elettronico che utilizzi un microprocessore per l'elaborazione di dati binari per l'esecuzione di una qualsiasi operazione in grado di esprimere un particolare significato per l'utente;
- per "*sistema telematico*", si intende l'insieme di più sistemi informatici collegati tra loro per lo scambio di informazioni, purché siano connessi in modo permanente e lo scambio di informazioni sia il mezzo necessario per conseguire i fini operativi del sistema.

La Convenzione sul *Cybercrime*, ratificata in Italia con la Legge n. 48/2008, non distingue invece tra sistema informatico e telematico, stabilendo che per sistema informatico si intende "qualsiasi apparecchiatura, dispositivo, gruppo di apparecchiature o dispositivi, interconnesse o collegate, una o più delle quali, in base ad un programma, esegue l'elaborazione automatica di dati"[251]. Partendo dal presupposto che, oggi, un *personal computer* è un oggetto privo di utilità se non connesso alla Rete, non si può non condividere tale definizione.

In Italia, l'intercettazione è disciplinata dal codice di procedura penale all'articolo *266 bis*, mentre l'accesso ai dati digitali, contenuti in un s*erver* o in un *computer*, avviene (o dovrebbe avvenire, vista la recente giurisprudenza citata al paragrafo precedente) attraverso il sequestro. Dal punto di vista procedurale, la disciplina non si differenzia in modo significativo da quella statunitense. Infatti, il Pubblico Ministero chiede al Giudice delle indagini preliminari (o al Giudice del dibattimento, ovvero ancora al Giudice di pace in caso di reati di sua competenza)

[250] Cass. Pen., Sez. II, 24 febbraio 2011, n. 9891 per la quale «deve ritenersi 'sistema informatico', [...] un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di 'codificazione' e 'decodificazione' - dalla 'registrazione' o 'memorizzazione', per mezzo di impulsi elettronici, su supporti adeguati, di 'dati', cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (*bit*), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare 'informazioni', costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente».

[251] Art. 1 Convenzione sul *Cybercrime*: «*Computer System means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*».

di emettere il decreto di autorizzazione allo svolgimento delle operazioni. Ove, invece, vi fossero ragioni di urgenza (art. 267 c.p.p.), sarebbe legittimo un provvedimento di autorizzazione del Pubblico Ministero: questi, tuttavia, deve tassativamente richiedere la convalida al Giudice competente entro 24 ore dal suo provvedimento e il Giudice deve autorizzare tale intercettazione entro 48 ore dalla richiesta. Una volta autorizzato, il Pubblico Ministero dispone l'intercettazione con decreto, indicando modalità e tempi di esecuzione delle operazioni (massimo quindici giorni, che diventano quaranta in caso di intercettazioni preventive). Proprio sui tempi di esecuzione potrebbe porsi un problema nell'applicazione dell'intercettazione telematica. Se, infatti, l'arco temporale in cui è ammissibile compiere delle intercettazioni è di quaranta giorni, può essere considerata legittima l'intercettazione di una *email* che contiene, al suo interno, una precedente *email* di due mesi prima? Come già anticipato sopra, nelle comunicazioni telematiche si è soliti, attraverso il comando "rispondi" o "rispondi a tutti", conservare le *email* precedentemente inviate. Se è indubbio che tale prassi favorisca gli investigatori, ne è meno certa la legittimità da un punto di vista procedurale. Nella scarsa giurisprudenza sul tema delle intercettazioni telematiche, un problema del genere non si è ancora posto, ma merita di non essere sottovalutato. Tornando alle intercettazioni telematiche *tout court*, l'articolo *266 bis* c.p.p. fa espressa menzione di due tipologie di reato che giustificano l'impiego di tale mezzo istruttorio: da un lato, vi sono gli illeciti previsti specificamente dall'articolo 266 c.p.p.[252] mentre, dall'altro, quelli commessi mediante l'impiego di tecnologie informatiche o telematiche.

Quanto al secondo gruppo, la dottrina ha fornito due interpretazioni: secondo alcuni la norma considera solo i *computer crime* (crimini introdotti dalla Legge n. 547/1993, in cui lo strumento informatico è elemento costitutivo della descrizione normativa); secondo altri si applica a tutti i *computer related crime*

[252] Quanto al primo gruppo, trattasi dei 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 c.p.p.;

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.p.p.;

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 di 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* del medesimo codice.

(crimini d'ogni sorta purché commessi mediante tecnologie informatiche)[253].

Secondo i sostenitori dell'interpretazione restrittiva[254], non vi sarebbe altra possibilità ermeneutica dal momento che il canone costituzionale delle intercettazioni, ossia l'art. 15 della Costituzione, impone un'interpretazione necessariamente restrittiva della disposizione in esame. Ne deriva che le intercettazioni non sono ammissibili se non nel rispetto di tre criteri fondamentali, conformemente all'art. 8 della Convenzione Europea per la tutela dei diritti dell'uomo e delle libertà fondamentali del 4 novembre 1950, e all'interpretazione di tale disposizione data dalla Corte europea dei diritti dell'uomo:

1. una normativa analitica, che precisi limiti e strumenti di applicazione;
2. l'esigenza del provvedimento dell'autorità giurisdizionale, che verifichi il rispetto di tale fondamento giuridico;
3. la conformità ad uno degli scopi legittimi, tra cui il fine di prevenire e reprimere i reati, indicati nella Convenzione.

Affermare che l'intercettazione informatica è esperibile con riferimento a qualsiasi reato, vorrebbe dire rilevare un preoccupante vuoto normativo in tale (necessaria) regolamentazione. Ad esempio, si dubita del rispetto, da parte delle norme in argomento, del principio di uguaglianza, stante il fatto che detta regolamentazione fa sì che, per certi reati commessi con lo strumento informatico, non ricompresi nell'elenco di cui all'art. 266 c.p.p. ma aventi pari gravità, l'Autorità Giudiziaria possa disporre intercettazioni telematiche e non intercettazioni telefoniche o ambientali.

Secondo l'interpretazione estensiva[255], invece, la lettera della norma non lascia spazio ad alcuna limitazione riguardo al titolo del reato, ma soltanto, come già ribadito, riguardo al mezzo attraverso cui l'illecito è commesso: sarebbe tale uso del mezzo telematico o informatico a giustificare una risposta investigativa di pari livello. Ne discenderebbe, come detto, la possibilità di disporre intercettazioni telematiche ed informatiche e non telefoniche o ambientali in relazione ad una pluralità di reati non catalogati ai sensi dell'art. 266 c.p.p. Tale disparità

[253]L. LUPARIA, G. ZICCARDI, *La disciplina processuale e le garanzie difensive*, in, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Giuffrè Editore, Milano, 2007.

[254] L. FILIPPI, *L'intercettazione di comunicazioni,* Giuffrè Editore, Milano, 1997.

[255] A. CAMON, *Le intercettazioni nel processo penale,* Giuffrè Editore, Milano, 1996.

troverebbe giustificazione proprio nell'uso, da parte del reo, dello strumento informatico, che qualificherebbe come particolarmente insidiosa la sua condotta. In sostanza, i sostenitori della tesi estensiva ritengono irragionevole, nel momento in cui detto strumento è utilizzato per offendere, non utilizzarlo anche per reprimere tale offesa. L'uso dello strumento informatico diviene allora di per sé solo portatore di uno specifico disvalore o, meglio, di una specifica offensività che giustifica particolari strumenti di indagine.

L'elenco dei reati in forza dei quali è possibile richiedere l'intercettazione telematica negli Stati Uniti è ampio (18 U.S.C. § 2516) e si divide tra:

- Reati di competenza federale (tra cui, a titolo meramente esemplificativo, è possibile citare il sabotaggio delle centrali nucleari, reati collegati alle armi biologiche, lo spionaggio, la rivelazione di segreti industriali, la corruzione di un funzionario e le associazioni a delinquere finalizzate allo spaccio di stupefacenti);
- Reati di competenza del singolo Stato (tra cui l'omicidio, il rapimento, il gioco d'azzardo, la rapina, la corruzione, l'estorsione, il traffico di stupefacenti, o altri crimini che possono cagionare danni fisici punibili con la reclusione superiore ad un anno).

Un discorso a parte merita il *Foreign Intelligence Surveillance Act* del 1978[256], che definisce le procedure per la sorveglianza elettronica e la raccolta di informazioni relative a cittadini americani, al fine di proteggere gli Stati Uniti contro attuali e potenziali attacchi, sabotaggi o possibili atti terroristici.

Questo tipo di attività di sorveglianza può includere, oltre ai dati di registrazione di un utente, anche l'accesso ai contenuti delle sue comunicazioni: esso può avvenire senza un ordine del Giudice, nel caso in cui sia richiesto dal Presidente degli Stati Uniti attraverso *l'Attorney General*[257]; oppure attraverso un ordine della *Foreign Intelligence Surveillance Court,* la quale dovrà valutare l'effettiva pertinenza (ossia se l'obiettivo della sorveglianza riguardi effettivamente una minaccia proveniente da uno Stato estero) e la legittimità di tale richiesta.

Da menzionare, infine, il *Communications Assistance for Law Enforcement Act* 47 U.S.C. § 1001-1021), che impone alle compagnie telefoniche di

[256] *Foreign Intelligence Surveillance Act* (50 U.S.C. § 1801-1885C).

[257] L'Attorney General negli Stati Uniti è il capo del Dipartimento di Giustizia ai sensi del Title 28 U.S.C. § 503.

implementare la propria infrastruttura tecnologica, al fine di poter favorire eventuali attività di sorveglianza elettronica da parte delle forze dell'ordine[258].

In estrema sintesi, la vera differenza tra la disciplina italiana delle intercettazioni e quella americana, non sta tanto nella procedura quanto nell'effettiva applicazione.

Negli Stati Uniti vi è una massiccia applicazione dei sistemi di monitoraggio preventivo, mentre in Italia vi è un ampio utilizzo delle intercettazioni per ora solo telefoniche, ma che diventeranno sicuramente telematiche nei prossimi anni.

Nonostante vi siano numerose similitudini nella procedura, esse non sono sufficienti per creare una forma di cooperazione, pertanto sono stati sottoscritti tra Italia e Stati Uniti in data 3 maggio 2006, dagli "Accordi sulla mutua assistenza giudiziaria tra gli Stati Uniti e l'Italia", che sostituiscono gli accordi del 1982, successivamente con Legge 16 marzo 2009, n. 25 è stata ratificata in Italia il trattato sottoscritto dagli Stati Uniti con l'Unione europea il *25* giugno 2003[259].

Il tema è particolarmente delicato, in quanto i principali "detentori" delle informazioni digitali del mondo sono Società come Google, Yahoo, Facebook e Microsoft, che hanno sede negli Stati Uniti.

Per un paese come l'Italia, affrontare un processo rogatoriale per ottenere tali informazioni potrebbe diventare molto complesso: ogni giorno, mediamente, in Italia vengono autorizzate 464 intercettazioni, mentre negli Stati Uniti ne vengono autorizzate 10. Sulla difficoltà di trovare una forma di cooperazione su questo tema, già il Consiglio d'Europa, nel 2001, in sede di ratifica della Convenzione sul *Cybercrime*, aveva evidenziato il problema nella sua relazione illustrativa all'articolo 32, che copre la materia dell'accesso transfrontaliero ai contenuti memorizzati all'interno di un *computer*. Il Consiglio affermava, laconicamente, che permettere ad uno Stato membro della Convenzione di accedere ai dati contenuti in un *computer* e memorizzati da un utente o da una società di un altro Stato membro, è «questione particolarmente complessa che non è possibile affrontare in carenza di esperienze consolidate in materia».

In questi anni, la crescita esponenziale dei sistemi di *cloud computing* e delle tecnologie *Voice Over IP* hanno reso questo problema ancora più attuale e, a

[258] Per una critica a tale normativa si veda il seguente URL:
http://www.eff.org/issues/calea?f=summary.html.

[259] Ratifica ed esecuzione degli Accordi di estradizione e sulla mutua assistenza giudiziaria tra Stati Uniti e U.E. del 25 giugno 2003. Ratificata in Italia con la Legge 16 marzo 2009, n. 25.
Il testo del trattato è disponibile al seguente URL:
https://www.giustizia.it/giustizia/it/mg_1_2_1.wp?facetNode_1=1_8%282008%29&facetNode_2=1_8%28200811%29&previsiousPage=mg_1_2&contentId=SAN47260.

livello Europeo, non mancano le soluzioni operative per trovare una soluzione a tale vuoto normativo[260]. Forse è giunto il momento di metterle in pratica.

4.2.6. *Intercettazioni telematiche*.

Le intercettazioni telematiche sono uno strumento, ad oggi, poco utilizzato in ambito investigativo per tre ragioni: la prima di natura tecnica, la seconda di natura giuridica e la terza di natura pratica.

Da un punto di vista tecnico, la possibilità di utilizzare tecniche di crittografia per nascondere le informazioni che transitano in Rete abbinate a sistemi *peer to peer* per la comunicazione vocale, rende estremamente difficile anche per i consulenti più esperti poter intercettare, e conseguentemente decifrare i pacchetti di informazioni che vengono scambiati tra gli utenti[261]. Dal punto di vista giuridico, la collocazione fisica fuori dal territorio nazionale dei *servers* dei principali gestori di servizi *VoIP (Skype, Gtalk, Windows Live Messenger)* e di posta elettronica *(@gmail.com, @yahoo.com, @live.com)* comporta per l'Autorità Giudiziaria la necessità di avviare un procedimento rogatoriale, che molto spesso non coincide con i tempi di un'indagine penale.

Da un punto di vista pratico, infine, la conseguente impossibilità di poter intercettare i dati direttamente presso il *provider*, obbliga la Polizia Giudiziaria ad utilizzare sistemi molto più elaborati, che comportano un notevole dispendio economico sia in termini di *hardware (sistemi embedded* da utilizzare come sonde)[262], che in termini di risorse umane (consulenti tecnici qualificati).

Le modalità operative sono condizionate dalle caratteristiche del sistema, dal tipo di comunicazioni e dall'oggetto delle stesse. I punti più vulnerabili di un'intercettazione sono i punti di gestione e di concentrazione del traffico di Rete come i *routers*[263], le *gateways*[264] o i *server* di rete[265].

---

[260] Per un approfondimento si veda JAN SPOENLE, *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?,* (*Council of Europe Project on Cybercrime*), disponibile al seguente URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df.

[261] T. BERSON, *Skype Security Evaluation. Anagram Laboratories 18 october 2005,* ricerca disponibile al seguente URL: http://www.anagram.com/berson/skyeval.pdf.

[262] Con il termine sistema *embedded* (generalmente tradotto in italiano con sistema incorporato) si identificano genericamente tutti quei sistemi elettronici a microprocessore progettati appositamente per una determinata applicazione (*special purpose*) ovvero non riprogrammabili dall'utente per altri scopi, spesso con una piattaforma *hardware ad hoc*, integrati nel sistema che controllano. Alcuni di questi modelli sono commercializzati dalla società Austriaca SILA Embedded Solutions, sito disponibile al seguente URL: http://www.embedded-solutions.at/en/.

[263] Il *Router* è un dispositivo responsabile dell'instradamento dei dati attraverso una Rete.

In generale, l'intercettazione telematica può avvenire:

- attraverso la collaborazione dei *provider* di servizi: qualora il gestore del servizio abbia una sede operativa in Italia, l'Autorità Giudiziaria, una volta emesso il decreto di intercettazione, consegna alla Polizia Giudiziaria l'eventuale delega e un documento ("griglia") contenente i dati tecnici. La Polizia Giudiziaria consegna la "griglia" al *provider,* il quale ha l'obbligo di mettere a disposizione un collegamento dedicato che porta i dati sul *server* della sala ascolto della Procura della Repubblica, in cui avvengono tecnicamente le intercettazioni. Un esempio di questa forma di collaborazione avviene nel caso dell'intercettazione di corrispondenza elettronica: il gestore del servizio, una volta ricevuta la "griglia", provvederà a duplicare la casella di posta elettronica dell'indagato e inoltrerà tutte le *email* direttamente sul *server* della Procura della Repubblica;
- presso i privati o presso i *provider* di servizi: questo tipo di intercettazione avviene nel caso in cui non vi sia la collaborazione del gestore del servizio di *hosting* in cui sono memorizzati i dati, o qualora sia necessario effettuare un'intercettazione dell'intero flusso di dati trasmesso dal soggetto indagato. In questo caso, viene svolto un filtraggio sull'indirizzo IP[266]. Qualora l'utente utilizzi linee fisse come ADSL, al posto dello *switch*[267] viene messa una sonda detta *Front End* collegata ad una porta denominata *span port*[268] che riceve in copia tutto il traffico scambiato (in entrambe le direzioni quindi) dall'apparato di accesso che gestisce la connessione finale dell'utente. La sonda filtra solo il traffico rilevante per il decreto d'intercettazione in base all'indirizzo IP

---

[264] Il *Gateway* (dall'inglese passaggio) è un dispositivo di rete il cui scopo principale è quello di effettuare una traduzione di protocollo tra due Reti.

[265] J.F. KOROSE, K.W. Ross, *La sicurezza nelle reti,* in *Reti di calcolatori e internet,* Pearson Addison Wesley, Milano, 2005.

[266] Nel caso in cui il *computer* da cui sono originate le conversazioni sia connesso ad una LAN, avrà un IP privato interno alla stessa, e un IP pubblico, ma in questo caso tutti i dati in transito dalla rete LAN utilizzeranno lo stesso IP pubblico e non sarà possibile, durante l'intercettazione, dividere il traffico dei vari terminali attivi. V.S. DESTITO, G. DEZZANI, C. SANTORIELLO, *Il diritto penale delle nuove tecnologie,* Cedam, Padova, 2007.

[267] Uno *switch* è un dispositivo di rete che inoltra selettivamente i frame ricevuti verso una porta di uscita.

[268] A. GHIRARDINI, G. FAGGIOLI, *op. cit.*, p. 72.

del soggetto indagato. Il flusso viene poi scaricato localmente su disco e trasferito tramite la linea RES ad alta velocità verso la postazione di decodifica *(Back End)*[269]. La postazione di decodifica ha un modulo che interpreta e ricostruisce i protocolli in modo che l'addetto alla postazione possa vedere, ad esempio, i messaggi di posta elettronica inviati e ricevuti, le pagine *web* visitate, la comunicazione *VoIP* nel caso in cui non sia captata[270];

- su dorsali di comunicazione *(backbone):* nel caso di intercettazioni parametriche su dorsali di comunicazione, si è più spesso interessati ad identificare sessioni di traffico generate da un punto imprecisato di un'area geografica, che contengono tipicamente parole o frasi chiave. Viene, quindi, impostato un filtro e tutti i pacchetti che compongono la comunicazione del canale vengono ispezionati. Data l'ampiezza di banda mediamente disponibile sugli attuali canali di comunicazione, la quantità di dati trasportata è considerevole e richiede sicuramente due attività: filtraggio (esclusione della maggioranza dei dati che ai fini delle indagini è generalmente inutile) ed eventuale correlazione dei dati acquisiti con l'utente intercettato.

Il sistema operativo utilizzato per effettuare un'intercettazione telematica è, generalmente, *Linux,* in quanto tale sistema ha subito una rapidissima evoluzione nel campo del *networking.* Molte delle funzioni necessarie ad effettuare una captazione di dati digitali, infatti, sono già incorporate nel sistema operativo[271].

L'applicativo più importante è invece l'analizzatore di rete *(sniffer).* Esso è un *software* adatto all'analisi dei dati (pacchetti) che transitano su una rete, in quanto fornisce una panoramica dettagliata di tutto ciò che accade nella rete locale ed è in grado di individuare i protocolli di rete utilizzati per i vari tipi di

[269] Qualora non si riesca ad avere accesso fisico allo *switch* è possibile procedere con un attacco c.d. "*man in the middle*": Se "X" e "Y" sono i due interlocutori "Z" che è *l'attacker* cercherà di deviare *il* flusso tra X e Y al fine di trovarvisi in mezzo per poterlo intercettare comodamente. Per attuare un attacco "*man in the middle*" è necessario utilizzare delle tecniche di *ARP spoofing*.
Per un approfondimento si veda D. D'AGOSTINI, Le indagini sulle *reti informatiche,* in *Diritto penale dell'informatica,* Experta Edizioni, Forlì, 2007.

[270] La Polizia Giudiziaria dispone anche di uno strumento *hardware* denominato "*tele-monitor*" che consente di intercettare l'utente nel caso egli decida di accedere alla Rete da diversi punti e con diverse tipologie di collegamento. Per un approfondimento sul tema si consiglia di consultare il sito dell'ufficiale dei Carabinieri Marco Mattiucci (Comandante della Sezione Telematica del RIS di Roma che svolge attività scientifico forense nello specifico settore dei crimini ad alta tecnologia) disponibile al seguente URL: www.marcomattiucci.it.

[271] A. GHIRARDINI, G. FAGGIOLI, *op. cit.*, p. 75.

comunicazione. Alcuni analizzatori di protocollo permettono di acquisire i *log* da altri programmi per i prodotti di libero accesso, e di applicare dei filtri per rendere selettiva la cattura del traffico.

Gli *sniffer* intercettano i singoli pacchetti, decodificano i dati contenuti, e rendono disponibili le informazioni sul mittente, il destinatario, il tipo di protocollo, l'applicazione e, soprattutto, il contenuto in forma di testo, audio e video[272]. Tra quelli più utilizzati si ricordano, Wireshark[273] e *Tcpdump*[274].

Vi sono, inoltre, programmi specifici che estraggono dal flusso di comunicazioni solo alcune informazioni, come *login, password e file* trasferiti[275].

Come già osservato[276], l'intercettazione dei sistemi *VoIP* criptati costituisce uno dei maggiori problemi sia da un punto di vista giuridico (i gestori del servizio non hanno sede nel territorio del soggetto intercetta to e, talvolta, non accettano di collaborare con le forze di polizia), sia da un punto di vista tecnico (i gestori del servizio non sono spesso in grado di fornire la chiave di cifratura o non hanno intenzione di creare una *back door* per consentire l'intercettazione da parte dell'Autorità Giudiziaria[277].

La soluzione potrebbe essere, quindi, quella di installare, nel *computer* del soggetto indagato, a sua insaputa, un *software* di *remote forensics* attraverso l'invio di un *trojan horse*[278]. Un *software* di *remote forensics*[279] potrebbe

---

[272] Uno dei sistemi più noti è il *software* DCS (*Digital Collection System*) 1000, meglio noto come "Carnivore", implementato dal *Federal Bureau of Investigation.* Per un approfondimento sul tema, O.S. KERR, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't,* in *Northwestern University Law Review*, Vol. 97, 2003, disponibile al seguente URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=317501.

[273] Ulteriori informazioni su *Wireshark* sono disponibili al seguente URL: https://www.wireshark.org/.

[274] Ulteriori informazioni su *TCPdump* sono disponibili al seguente URL: http://www.tcpdump.org.

[275] Due programmi che svolgono a tale funzione sono: *Chaos reader* disponibile al seguente URL: http://chaosreader.sourceforge.net e *Ettercap-ng,* disponibile al seguente URL: http://ettercap.github.io/ettercap/.

[276] Sul tema si veda ancora: D. BEM, F. FELD, E. HUEBNER, O. BEM, *Computer Forensics-Past, Present And Future,* in *The Journal of Information Science* & *Technology,* 2008. Presente all'URL: http://www.scopemed.org/?mno=170752.

M. BATES - T. MIN, *Problems With Wiretapping of VoIP Services,* disponibile al seguente URL: http://www.colorado.edu/policylab/Papers/Secure_Voip_writeup%20v3_2%20_2_.pdf.

[277] La società Skype, ad esempio, sostiene di non riuscire a fornire la chiave di decifratura a causa della complessità dell'algoritmo di criptazione la cui chiave, oltretutto, viene cambiata ad ogni sessione di comunicazione. Tutto ciò contrasta con quanto espresso dalla *Organisation for Economic Cooperation and Development* (OECD), nelle *Guidelines* sulla crittografia: «*National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible*». http://www.oecd.org/internet/ieconomy/guidelinesforcryptographypolicy.htm.

[278] Un *trojan horse* (dall'inglese: Cavallo di Troia), è un tipo di *malware.* Deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è dunque

permettere alla Polizia Giudiziaria di ricercare le informazioni sul *computer* del soggetto, registrare le conversazioni effettuate tramite i sistemi *VoIP*[280], recuperare le chiavi di decifratura utilizzate per criptare i *file*[281] e, addirittura, attivare le periferiche audio/video per identificare il sospettato e il luogo in cui si trova[282]. L'utilizzo di questi programmi, ovviamente, dovrebbe avvenire sotto il costante controllo dell'Autorità Giudiziaria, che avrebbe il preciso compito di delimitare il tipo di attività del sistema controllante, filtrando le informazioni utili alle indagini e quelle che invece non hanno alcuna attinenza con esse.

Se questa metodologia è in grado di superare il problema delle intercettazioni *VoIP*, è evidente che la stessa genera non poche perplessità dal punto di vista giuridico[283], in quanto si potrebbero ledere alcuni diritti fondamentali dei soggetti indagati, come verrà meglio discusso nel paragrafo seguente. Anticipando nuovamente un tema che verrà meglio approfondito nel prossimo capitolo, è necessario trovare un punto di equilibrio tra le esigenze di prevenzione dei reati e di tutela dell'ordine pubblico, con quelle di tutela dei dati personali e del rispetto del principio di sovranità[284].

---

l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice *trojan* nascosto.

[279] Oltre al già citato progetto *CIPAV*, sempre gli Stati Uniti nel 2001 avevano adottato un progetto simile in un'indagine chiamata "*magic lantern*" un *keylogger* per accedere all'interno dei *computer* degli indagati. Per un approfondimento si veda, Christopher Woo - Miranda So, *The Case For Magic Lantern: September 11 Highlights The Need For Increased Surveillance*, in *Harvard Journal of Law & Technology*, 2002, disponibile al seguente URL: http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf.

[280] Per ottenere questo risultato sarebbe sufficiente installare da remoto uno dei tanti *software* disponibili in rete, come ad esempio: MP3 Skype Recorder v.4.23 disponibile all'URL: http://voipcallrecording.com/.

[281] Per poter visualizzare ogni tipo di *password* inserita da un utente sarebbe possibile installare da remoto un *keylogger*. Tale *software* è in grado di intercettare tutto ciò che un utente digita sulla tastiera del proprio *computer*.

[282] M. GERCKE, *Secret Online Search*, in *Computer und Recht*, 2007.

[283] Di diversa opinione F. TESTA, *op. cit.*, p. 5, per il quale l'installazione di un *keylogger* all'interno del *computer* dell'indagato non costituisce intercettazione e sarebbe sufficiente un "decreto motivato del Pubblico Ministero" che autorizzi la Polizia Giudiziaria ad installare siffatto *software*.

[284] Sul principio di sovranità, basti pensare alle problematiche che potrebbero sorgere nel momento stesso in cui il proprietario del *computer* su cui è installato un *software* di *remote forensics*, decida di partire in un altro Stato portando con sé il *computer* "infetto". In questo caso, si potrebbe ipotizzare che la polizia giudiziaria stia svolgendo un'attività investigativa al di fuori del territorio nazionale.

CAPITOLO V

Informatica Forense e Standard ISO

5.1. Introduzione - 5.2. Lo Standard ISO/IEC 27037:2012 - 5.3. Postulati dello Standard ISO/IEC 27037:2012 - 5.3.1. La Verificabilità - 5.3.2. La Ripetibilità - 5.3.3. La Riproducibilità - 5.3.4. La Giustificabilità - 5.4.Standard ISO/IEC e fasi della informatica forense - 5.4.1. Identificazione della prova digitale - 5.4.2. Raccolta della prova digitale - 5.4.3. Operazioni da effettuare su *Personal Computer* in funzione - 5.4.4. Operazioni da effettuare su *Personal Computer* spento - 5.4.5. L'acquisizione della prova digitale - 5.4.6. Conservazione e trasporto - 5.4.7. *Chain of custody*, la catena di custodia - 5.4.8. Analisi dei reperti informatici - 5.4.9. Valutazione - 5.4.10. Presentazione.

5.1. *Introduzione*.

L'International Standard ISO/IEC 27037, stabilito dall'International Organization for Standardization, e l'International Electrotechnical Commission, rappresenta lo standard operativo fondamentale in materia di *Computer Forensic*.

L'International Organization for Standardization, è la più importante organizzazione a livello mondiale per la definizione delle norme tecniche, fondata il 23 febbraio 1947, ha sede a Ginevra. Membri dell'ISO sono gli organismi nazionali di standardizzazione di 164 Paesi del mondo. Pur non essendo una organizzazione non governativa, la sua capacità di stabilire standard che diventano leggi attraverso accordi e trattati internazionali la rendono molto importante ed influente. Le lingue ufficiali dell'organizzazione ISO sono l'inglese, il francese e il russo. L'International Electrotechnical Commission, è l'organizzazione internazionale per la definizione di nuovi standard in materia di elettricità, elettronica e tecnologie correlate, fondata nel 1906, aveva inizialmente sede a Londra, ma dal 1948 ha spostato la sua sede a Ginevra. Ad essa attualmente partecipano più di 60 Paesi. La IEC ha il compito di sviluppare e distribuire gli standard per le unità di misura, in particolare il *gauss*, l'*hertz* e il *weber*. Il compito principale della commissione tecnica congiunta è di redigere gli standard internazionali i cui progetti adottati, vengono fatti circolare fra gli organismi internazionali per il voto. La pubblicazione a livello di standard internazionale richiede l'approvazione di almeno il 75% degli enti nazionali esprimenti un voto. Tra i numerosi standard promossi dall'ISO, di recente sono stati presentati documenti che riguardano l'informatica forense che si pongono quali norme tecniche di riferimento riconosciute a livello internazionale:

- ISO/IEC 27037:2012, emesso in versione definitiva il 15 ottobre 2012 relativamente a linee guida per identificazione, raccolta, acquisizione e conservazioni delle prove digitali;
- ISO/IEC 27041:2015, emesso in versione definitiva il 15 giugno 2015 raccoglie le best practice e fornisce linee guida sulla garanzia di idoneità e adeguatezza dei metodi di investigazione;
- ISO/IEC 27042:2015, emesso in versione definitiva il 15 giugno 2015 relativamente a linee guida per l'analisi e l'interpretazione di prove digitali;
- ISO/IEC 27043:2015, pubblicato il 4 marzo 2015, relativamente a principi e processi per l'investigazione di incidenti informatici, accessi non autorizzati, *data corruption*.

5.2. *Lo Standard ISO/IEC 27037:2012*.

Le linee guida preesistenti alla pubblicazione di questo Standard erano per lo più prodotte da forze di polizia ed agenzie governative, anche se non sono mancate linee guida prodotte da organizzazioni sovranazionali (OCSE), ma non esistevano linee guida in materia prodotte da un organismo neutrale. Per questo motivo lo Standard internazionale ISO/IEC 27037:2012, la cui prima edizione risulta datata il 15 ottobre 2012, e che nella sua definizione richiama altri standard ISO/IEC[285] rappresenta una grande innovazione, contiene le linee guida per la definizione, l'identificazione, raccolta, acquisizione e conservazione delle *digital evidence*. Lo Standard ISO/IEC 27037, applicabile sia a contesti aziendali che processuali, non si riferisce a nessuna particolare nazione o giurisdizione, tuttavia uno dei suoi scopi principali è quello di facilitare l'interscambio di evidenze tra nazioni e giurisdizioni diverse.

Esso fornisce anzitutto la definizione di "evidenza digitale" (*digital evidence)*: Informazioni o dati memorizzati o trasmessi in forma binaria, su cui si può fare affidamento come evidenza, fornendo le linee guida per le attività specifiche inerenti la ricerca e la raccolta, acquisizione e conservazione delle stesse *digital evidence*.

[285] ISO/TR 15801 - Document management - Information stored electronically - Recommendations for trustworthiness and reliability.

ISOI/IEC 17020 - Conformity assessment - Requirements for the operation of various types of bodies performing inspection.

ISO/IEC 17025:2005 - General requirements for the competence of testing and calibration laboratories.

ISO/IEC 27000 - Information technology - Security techniques - Information security management systems - Overview and vocabulary.

Lo Standard in esame individua le seguenti figure:

- Il DEFR, *Digital Evidence First Responders*, soggetto qualificato ad intervenire per primo sulla scena di un reato informatico, o realizzato mediante l'utilizzo di un dispositivo informatico, al fine di individuare, raccogliere e acquisire le prove digitali;
- Il DES, *Digital Evidence Specialists*, soggetto che ha conoscenze specialistiche e svolge le mansioni a supporto del DEFR;

Il documento in esame prevede che i soggetti responsabili gestiscano le potenziali prove digitali con metodologie che risultino standardizzate su scala mondiale, con l'obiettivo di facilitare l'investigazione riguardo ai dispositivi e le prove digitali in maniera sistematica e imparziale, preservandone al contempo l'integrità e l'autenticità. Lo standard intende altresì offrire informazioni ai soggetti responsabili a livello decisionale che hanno necessità di determinare l'affidabilità delle prove digitali. È applicabile alle organizzazioni che hanno necessità di proteggere, analizzare e presentare le potenziali prove digitali, dove con questa dizione si intendono i dati che possono essere ricavati da diversi tipi di dispositivi digitali, dispositivi di rete, *database* e quant'altro purché siano già in formato digitale[286].

L'intrinseca fragilità delle prove digitali, rende necessario l'utilizzo di metodologie adeguata per assicurare l'integrità, l'autenticità delle prove digitali: lo standard non indirizza la metodologia dei processi legali, delle procedure disciplinari e delle altre azioni relative alla gestione delle potenziali prove digitali che siano estranee allo scopo di identificazione, raccolta, acquisizione e conservazione. L'applicazione dello standard richiede conformità alle leggi, alle regole e ai regolamenti nazionali, non dovrà sostituire gli specifici requisiti legali di una giurisdizione mentre può servire come una linea guida di tipo pratico per ogni DEFR o DES nelle investigazioni che riguardano le potenziali prove digitali. Non si estende all'analisi delle prove digitali e non sostituisce requisiti specificamente giurisdizionali che attengono ad istanze come l'ammissibilità, il valore persuasivo, la rilevanza ed altre limitazioni soggette al controllo giudiziale dell'uso delle potenziali prove digitali nelle aule di giustizia.

[286] Lo standard non si occupa di documenti analogici che vengono convertiti in formato digitale.

Lo standard può essere di aiuto nella semplificazione dello scambio fra giurisdizioni delle potenziali prove digitali. Allo scopo di mantenere l'integrità delle prove digitali, gli operatori sono tenuti ad adattare e correggere le procedure descritte in ottemperanza ai requisiti legali delle prove previsti dalla giurisdizione specifica.

Lo standard ISO/IEC 27037:2012 integra gli standard ISO/IEC 27001[287] ISO/IEC 27002[288], ed in particolare i requisiti di controllo riguardanti l'acquisizione delle potenziali prove digitali offrendo un ulteriore indirizzo applicativo, oltre a trovare applicazione in contesti indipendenti dai due standard citati.

5.3. *Postulati dello Standard ISO/IEC 27037:2012.*

I tre postulati fondamentali introdotti dallo Standard ISO/IEC27037:2012 sono descritti come segue:

- **Rilevanza**, dovrebbe essere sempre possibile dimostrare che il materiale informatico acquisito sia rilevante ai fini delle indagini in corso, ovvero che contenga informazioni di valore, importanti ai fini delle investigazioni, e che pertanto è necessario procedere alla loro acquisizione.
- **Affidabilità**, tutti i processi utilizzati nella gestione delle potenziali prove digitali dovrebbero essere verificabili e ripetibili. I risultati dell'applicazione di tali processi di acquisizione devono essere riproducibili.
- **Sufficienza**, il DEFR dovrà considerare quanto materiale informatico sarà necessario acquisire per permettere un'adeguata attività di indagine. Lo stesso dovrà essere in grado di fornire spiegazioni in merito a quanto materiale informatico o quantità di dati sono stati acquisiti, le procedure utilizzate per decidere quanto e quale materiale raccogliere o acquisire.

Vi sono quattro aspetti chiave nella gestione dell'evidenza digitale: verificabilità, giustificabilità e ripetibilità o riproducibilità a seconda delle circostanze, vediamole:

[287] ISO/IEC 27001:2013 - ISO/IEC 27001 - Information security management.

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

5.3.1. *La verificabilità*.

Dovrebbe essere possibile per un valutatore indipendente o di altre parti interessate autorizzate, valutare le attività svolte da un DEFR[289] o un DES[290]. Ciò sarà reso possibile documentando adeguatamente tutte le azioni intraprese dagli stessi.

Il DEFR ed il DES devono essere in grado di giustificare in ogni momento il processo decisionale nella scelta di una determinata linea di condotta. I processi eseguiti dagli stessi dovrebbero essere disponibili per una valutazione indipendente al fine di stabilire se un appropriato metodo scientifico o appropriate tecniche sono state seguite nello svolgimento delle attività loro deputate.

5.3.2. *La ripetibilità*.

La *ripetibilità* si realizza quando gli stessi risultati sono ottenuti, mediante le seguenti condizioni:

- Utilizzando le stesse procedure di misurazione e di metodo;
- Utilizzando gli stessi strumenti operativi e alle stesse condizioni;
- Il risultato identico può essere ottenuto in qualsiasi momento.

Un DEFR opportunamente qualificato ed esperto dovrebbe essere in grado di svolgere tutti i processi descritti nella documentazione allegata ed ottenere lo stesso identico risultato, senza necessità di guide o interpretazioni.

Il DEFR dovrebbe essere consapevole che potrebbero rappresentarsi circostanze in cui non risulti possibile ripetere il test o l'attività svolta in precedenza, ad esempio quando un *hard disk* originale dopo essere stato acquisito sia stato successivamente restituito e riutilizzato, o quando si tratta di un elemento contenuto in una memoria volatile. In questi casi il DEFR dovrà assicurarsi che il processo di acquisizione sia stato e sia sempre affidabile. Per rendere effettiva la ripetibilità delle attività svolte, è importante il controllo della qualità e della documentazione prodotta nell'ambito dell'attività stessa, che dovrebbe essere sempre presente e completa.

[289] DEFR, *Digital Evidence First Responders*.
[290] DES, *Digital Evidence Specialists*.

5.3.3. *La riproducibilità*.

Analogamente alla *ripetibilità* la *riproducibilità* viene stabilità quando gli stessi risultati sono prodotti sotto le seguenti condizioni:

- Utilizzando le stesse procedure di misurazione e di metodo;
- Utilizzando gli stessi strumenti operativi e alle stesse condizioni;
- Il risultato identico può essere ottenuto in qualsiasi momento.

Le esigenze di riprodurre i risultati variano in base alle giurisdizioni e alle circostanze, in modo che il DEFR, o comunque chi sta svolgendo tale attività, dovrà essere informato sulle condizioni applicabili.

5.3.4. *La giustificabilità*.

Il DEFR dovrebbe essere sempre in grado di giustificare e motivare le azioni ed i metodi adottati nella gestione delle potenziali prove digitali.

La giustificazione può essere ottenuta dimostrando che la decisione presa coincideva con la scelta migliore per ottenere tutte le potenziali prove digitali. Un altro DEFR o DES, potrebbe anche dimostrare riproducendo con successo le azioni ed i metodi adottati in precedenza.

E' nell'assoluto interesse dell'ente o dell'organizzazione che svolge l'attività forense di avvalersi di incaricati DEFR o DES in possesso delle competenze e conoscenze necessarie così come descritte nell'allegato A del presente Standard Internazionale. Questo assicurerà che le corrette procedure verranno utilizzate durante la manipolazione delle prove digitali al fine di assicurare l'eventuale corretta conservazione delle stesse che possono avere valore probatorio. Questo assicurerà inoltre che le varie organizzazioni possano validamente utilizzare queste prove digitali, ad esempio, nelle loro procedure disciplinari o agevolarne lo scambio tra giurisdizioni differenti.

5.4. *Standard ISO/IEC e fasi della informatica forense.*

Basandoci sull'analisi delle varie linee guida che definiscono le c.d. "*best practice*", e su quanto correttamente definito ed illustrato all'interno degli standard ISO/IEC in materia, il processo dell'informatica forense si può correttamente dividere in sei distinte fasi secondo il seguente schema: identificazione; conservazione; acquisizione; valutazione; analisi; presentazione.

5.4.1. *Identificazione della prova digitale.*

La prova digitale si presenta come entità immateriale, ciò non significa che non abbiano una loro fisicità, trattandosi concettualmente di "impulsi elettrici che rispondono ad una sequenza numerica prestabilita e che, convogliati in un supporto informatico dotato di una memoria, originano informazioni intellegibili"[291], è pertanto una fisicità che in assenza di un supporto idoneo, non può essere percepita. E' il caso ad esempio dei supporti magnetici o la rappresentazione del dato informatico in *pit* e *land* nei supporti ottici.

Ciò spiega in parte come in passato si tendesse a confondere le prove digitali con gli oggetti nei quali le stesse erano contenute. Una traccia di questa fuorviante concezione emerge in modo chiaro dal previgente art. 491 *bis* c.p.[292], il quale identificava il «documento informatico» con qualunque «supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli». Se le cose stessero in questi termini non sorgerebbero particolari questioni in tema di raccolta delle prove digitali: sarebbe sufficiente applicare le disposizioni in materia di acquisizione delle prove documentali. I supporti materiali contenenti informazioni digitali reperiti nel corso delle indagini potrebbero essere prodotti in giudizio ed inseriti nel fascicolo per il dibattimento ai sensi degli Artt. 495 comma 3 e 515 c.p.p.

---

[291] M. DANIELE, La prova digitale nel processo penale, Rivista di diritto processuale Anno LXVI (seconda serie) – N.2, Cedam, Bologna, 2011.

[292] Introdotto dalla Legge 23 dicembre 1993 n. 547, ed ora abrogato dalla Legge n. 48 del 2008.

L'unico spazio per il contraddittorio si aprirebbe in sede di discussione finale, e riguarderebbe il valore conoscitivo delle informazioni. Oggi nessuno dubita più del fatto che le prove digitali esistano indipendentemente dai supporti in cui si trovano, i quali sono solo involucri esterni di per sé processualmente irrilevanti6. Spesso vi è, anzi, un'assoluta sproporzione tra le prove digitali ed i loro recipienti: un supporto di piccole dimensioni è in grado di contenere una massa enorme di informazioni digitali. L'identificazione è il processo di ricerca, individuazione e documentazione delle prove in formato digitale all'interno dell'enorme quantità di informazioni presenti all'interno di un *computer*, di un *server*, o di altri dispositivi di memorizzazione che possono essere rilevanti ai fini dell'indagine in corso[293], individuando dove possibile anche i dati che si possono trovare all'esterno o in spazi virtuali come ad esempio *server cloud*.

5.4.2. *Raccolta della prova digitale*.

La raccolta è l'attività ove la fonte di prova può essere maggiormente esposta al rischio di alterazione, dispersione o cancellazione[294]. Dopo aver individuato i dispositivi informatici che potrebbero contenere dati digitali rilevanti per l'indagine, l'informatico forense (o meglio il DEFR secondo le indicazioni dello standard ISO/IEC 27037:2012) deve decidere se procedere immediatamente all'acquisizione oppure se procedere alle operazioni di raccolta del supporto che verranno seguite solo successivamente dalle operazioni di acquisizione.

Questa è la fase del trattamento di dati digitali in cui i dispositivi che possono contenere potenziale prove digitali (ad esempio degli *hard disk*) vengono rimossi dalla loro posizione originale per essere trasportate in un laboratorio o comunque in un altro ambiente controllato per l'acquisizione e la successiva analisi. Ogni reperto va etichettato riportando il numero del caso, una descrizione, la data e l'ora di raccolta e il nome del soggetto che lo ha rilevato.

La distinzione che a questo punto occorre fare è sullo stato "acceso" oppure "spento" del sistema informatico rinvenuto, in quanto anche la semplice accensione del *computer* determina un'automatica alterazione del *file* di registro del sistema operativo, con conseguente perdita o alterazione di informazioni che potrebbero essere rilevanti ai fini dell'indagine.

---

[293] L. MARAFIOTI, "*Digital evidence* e processo penale" in Rivista Giuridica DeJure Giuffrè.

[294] J. VACCA, *Computer forensics. Computer Crime Scene Investigation.* Charles River Media, Boston, 2005.

Spesso la raccolta, quando possibile, è l'attività più opportuna da svolgere in ambito operativo forense, soprattutto se l'attività forense viene posta in essere dalla Polizia Giudiziaria nell'ambito di una perquisizione, per i seguenti motivi:

- semplicità: la raccolta del supporto fisico non richiede le particolari conoscenze tecniche necessarie per l'acquisizione, sebbene la stessa rimozione di supporti di memorizzazione digitale richieda comunque una certa competenza; inoltre il rinvio dell'operazione di acquisizione contribuisce ad allentare la tensione nei momenti critici di un'attività di sequestro, evitando errori;
- rapidità: la raccolta richiede semplicemente l'indicazione degli estremi identificativi del supporto all'interno di un verbale, oltre al carico di lavoro necessario per il trasporto, mentre l'acquisizione del supporto sul posto richiederebbe molte ore;
- inidoneità dei luoghi e insufficienza dei dispositivi *hardware* e/o di *storage* presenti sul posto ove la perquisizione o gli accertamenti si stanno svolgendo.

Tuttavia, in alcune particolari circostanze la raccolta fisica non è possibile:

- sistemi informatici che non possono essere spenti: si tratta di sistemi che erogano servizi critici in modalità 24/7; ad esempio, sistemi di controllo degli scambi dei binari ferroviari;
- sistemi informatici che erogano servizi anche a terzi: si tratta di sistemi che tipicamente risiedono in *datacenter* e forniscono risorse, sia computazionali che di spazio di memorizzazione, a vari utenti consentendo loro di ridurre i costi centralizzando l'investimento di *hardware* e *software*, nonché i costi per l'attività sistemistica; ad esempio, sistemi di fornitori di servizi di *hosting* che ospitano siti *web*;
- sistemi virtuali: si tratta di sistemi che simulano una macchina reale la cui consistenza fisica è quella del sistema sul quale viene eseguita l'attività.

5.4.3. *Operazioni da effettuare su personal computer in funzione*.

Il *Personal Computer* in funzione è un patrimonio di informazioni al quale un DEFR ed in particolare un operatore di Polizia Giudiziaria non può assolutamente rinunciare per completezza delle indagini relative al reato per cui si procede. Il riferimento riguarda l'eventuale applicazione della misura precautelare dell'arresto. Talvolta, infatti, i reati per cui la perquisizione viene eseguita, prevedono la possibilità, in via facoltativa od obbligatoria, di procedere all'esecuzione dell'arresto in flagranza. Analizzando le fattispecie per le quali viene predisposta la perquisizione finalizzata al sequestro di supporti informatici, si può immediatamente notare che le figure per cui l'arresto è previsto ma, soprattutto, per cui se ne può rilevare la flagranza tramite l'utilizzo dell'elaboratore elettronico sono quelle enucleate negli Artt. 600 *bis*, 1comma (prostituzione minorile), 600 *ter*, 1, 2 e 3 comma c.p. (pornografia minorile) e 600 *quinquies* c.p. (iniziative turistiche volte allo sfruttamento della prostituzione minorile) oltre a tutte le altre fattispecie di reato da cui si può dedurre in via mediata la flagranza per mezzo del sopra descritto utilizzo (ad es.: il reato di ricettazione ove l'indagato venga colto nell'atto di concordare l'acquisto di beni di chiara provenienza illecita tramite connessione alla rete Internet).

In presenza di evenienze di questo tipo, le metodologie operative da mettere in pratica sono poche ma efficaci:

- Occorre innanzitutto agire affinché l'intervento svolto sia il meno invasivo possibile; ogni operazione effettuata, infatti, andrà a modificare lo stato della fonte di prova. Non si deve confondere il compimento di tali operazioni con un'approfondita ricerca degli elementi utili ai fini della prosecuzione delle indagini;
- Si dovrà ove possibile inserire un supporto vergine di tipo ottico all'interno del masterizzatore collegato al *personal computer* ove salvare gli elementi utili reperiti (tale operazione sarebbe quella ideale; in realtà molte volte gli operatori di Polizia Giudiziaria hanno a che fare con PC sprovvisti anche della porta Usb o di qualsiasi masterizzatore; in tali casi sarà sufficiente creare una cartella sul *desktop* ove immagazzinare gli elementi reperiti);

- Il passo successivo è l'analisi, ovviamente non invasiva, dei processi in esecuzione; si dovrà porre in essere un'analisi della Ram e se possibile acquisirne il contenuto;
- Una volta verificata la presenza di connessioni attive, bisognerà porle sotto specifica analisi tramite adeguati *tool* (esempio classico il "*netstat*" del sistema operativo *Ms-Dos*);
- Se si è in presenza di connessioni attive e queste riconducono alla presenza di programmi per il "*filesharing*" anch'essi attivi, bisognerà analizzarne l'attività tramite la verifica del tipo di *file* che si sta "*scaricando*" oppure condividendo, senza tralasciare le informazioni relative agli utenti connessi all'elaboratore dell'indagato e che compiono a loro volta operazioni di "*download*" da questi;
- Si provvederà a redigere un verbale riepilogando dettagliatamente con riferimenti spazio/temporali le operazioni svolte ed ove possibile si allegheranno degli *screenshots* che provvederanno a documentare ulteriormente le operazioni compiute;
- Prima di concludere le attività di analisi sommaria del *personal computer* in oggetto sarà opportuno verificare l'esatta corrispondenza della data e dell'ora indicata dal sistema operativo, annotando le eventuali differenze con l'ora e/o la data effettiva.
- Si procederà, dunque, allo spegnimento del *Personal Computer* semplicemente staccando la spina dalla presa dell'alimentazione elettrica; bisognerà, però prestare attenzione al Sistema Operativo presente ed attivo nel PC in quanto un tale genere di spegnimento potrà provocare un malfunzionamento del disco rigido, pregiudicandone l'integrità. Per alcuni sistemi operativi, quali ad esempio *Macintosh* o *Linux*, sarà appropriato compiere le tipiche operazioni di "*shutdown*" prima di privare la macchina dell'alimentazione elettrica;
- Dette operazioni andrebbero documentate tramite riprese video o fotografiche, almeno per ciò che concerne le fasi essenziali di esse.

La serie di operazioni descritte in precedenza, trovano giustificazione nella norma enunciata all'art. 55 del codice di rito. Tale norma, al primo comma, infatti, impone alla Polizia Giudiziaria di "*compiere gli atti necessari per assicurare le fonti di prova e raccogliere quant'altro possa servire per l'applicazione della*

legge penale". A rafforzare tale assunto, infine, provvede l'art. 348 c.p.p. che al primo capoverso cita: "*Anche successivamente alla comunicazione della notizia di reato, la Polizia Giudiziaria continua a svolgere le funzioni indicate nell'art. 55 raccogliendo in specie ogni elemento utile alla ricostruzione del fatto e all'individuazione del colpevole*" ed ancora, in occasione di problematiche tecniche di difficile risoluzione, al 3° comma: "*La Polizia Giudiziaria quando[…] compie atti od operazioni che richiedono specifiche competenze tecniche, può avvalersi di persone idonee le quali non possono rifiutare la propria opera*".

5.4.4. *Operazioni da effettuare su personal computer spento.*

La Legge n. 38 del 6 febbraio 2006 recante "*Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet*" modifica l'art. 381 del codice di rito (Arresto facoltativo in flagranza) enucleandovi la nuova lettera 1 *bis,* volta a consentire la possibilità "*di procedere, nel caso in cui la misura sia giustificata dalla gravità del fatto ovvero dalla pericolosità del soggetto desunta dalla sua personalità o dalle circostanze del fatto medesimo, all'arresto facoltativo in flagranza*"[295] dell'autore del reato di cui all'art. 600 *quater* del Codice Penale (Detenzione di materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori degli anni 18).

Detta novella, prevedendo quanto sopra citato, pone una serie di facoltà in capo all'operatore di Polizia Giudiziaria chiamato ad effettuare una perquisizione per il reato di cui all'art. 600 *quater* C.P. Dovendo, infatti, stabilire i termini della gravità e delle circostanze del fatto-reato, l'operatore di cui sopra potrà compiere una serie di atti che si sostanziano in una vera e propria analisi dei supporti informatici posseduti dall'indagato. Per determinare la metodologia e le tecniche tramite le quali effettuare tali operazioni, viene, ancora una volta in soccorso la Legge di ratifica della Convenzione di Budapest che introduce il comma 1 *bis* all'art. 354 del codice di rito che cita testualmente: "*Nella flagranza del reato[…] gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino*

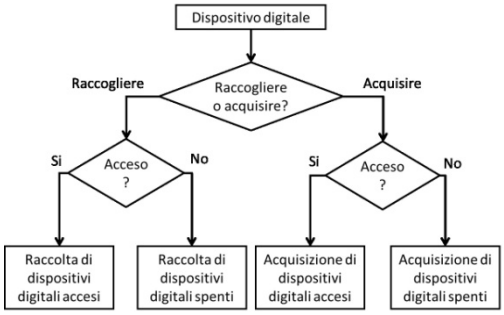
[295] Disegno di Legge n. 4599 recante "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet" presentato il 13 gennaio 2004.

occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi".

Sia per ciò che concerne il concetto di perquisizione di sistemi informatici che per quanto riguarda le misure di sicurezza atte a garantire la genuinità della fonte di prova si veda quanto già esplicato in precedenza.

Ciò che comporta il combinato delle norme di cui sopra è assai intuitivo: si dovranno analizzare i supporti informatici reperiti nella disponibilità dell'indagato e nel caso di *Personal Computer*, si dovranno estrarre i dischi rigidi e, in tale occasione senza il bisogno di effettuare copie, utilizzare sistemi di blocco di scrittura *hardware* che impediscano in maniera fisica la modificazione del disco, tipo *Write Blocker*[296]. A questo punto si provvederà nell'immediatezza ad una sommaria analisi c.d. *preview*, anteprima, dei contenuti presenti all'interno del supporto informatico in oggetto. Come già evidenziato nei paragrafi precedenti, da un punto di vista giuridico, la raccolta è la fase che trova riscontro nel sequestro probatorio[297], il mezzo di ricerca della prova con il quale l'autorità giudiziaria acquisisce il corpo del reato o le cose pertinenti che siano necessarie per l'accertamento dei fatti. Il seguente schema, tratto dallo standard ISO/IEC 27037:2012, evidenzia il processo di valutazione da parte del DEFR riguardo alla possibilità di operare una raccolta o un'acquisizione. Sulla base della scelta effettuata, lo stesso standard fornisce delle dettagliate procedure da seguire.

Figura 1 – Criterio decisionale circa l'opportunità di raccogliere o acquisire una potenziale evidenza digitale[298].



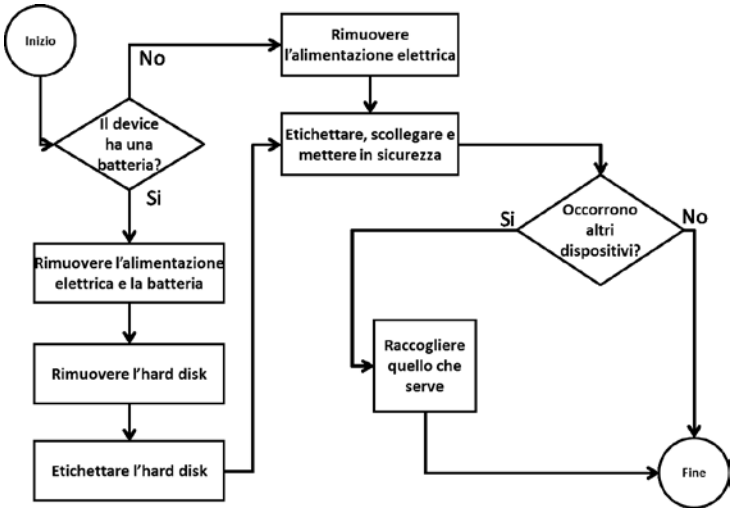
[296] Un *write blocker hardware* è un dispositivo fisico che viene interposto tra l'*hard disk* e la macchina di acquisizione forense (per questo motivo è anche detto "*forensic bridge*"), che inibisce a livello fisico la scrittura sul supporto sorgente.

[297] Articoli 253 e seguenti c.p.p.

[298] Traduzione della figura 1 riportata nello standard ISO/IEC 27037:2012.

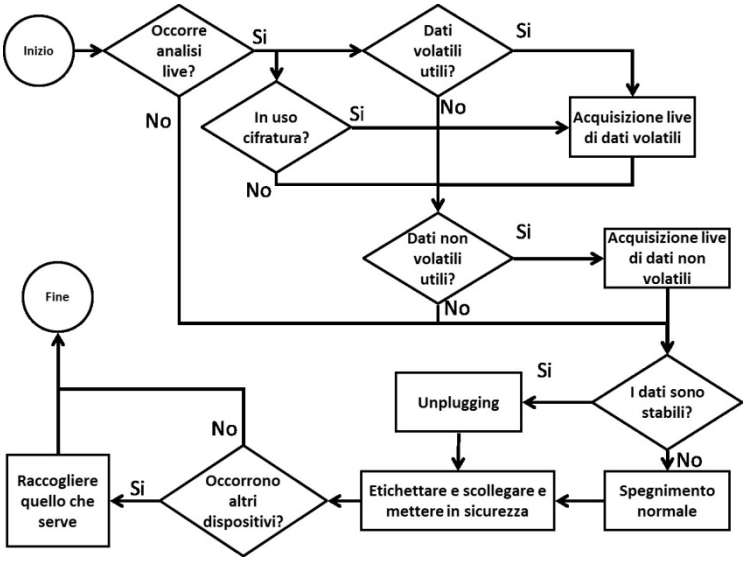
Qualora si dovesse propendere per la raccolta, in caso di dispositivi spenti lo schema da seguire è il seguente.

Figura 2 - Linee guida per la raccolta di dispositivi digitali spenti[299].



Entrando in contatto con un dispositivo acceso, lo schema è più complesso perché richiede la valutazione di alcuni elementi che andrebbero persi definitivamente dopo lo spegnimento del sistema.

Figura 3 – Linee guida per la raccolta e acquisizione di dispositivi digitali accesi[300].



[299] Traduzione della figura 3 riportata nello standard ISO/IEC 27037:2012.

[300] Traduzione e delle figure 2 e 3 riportate nello standard ISO/IEC 27037:2012.

5.4.5 *L'Acquisizione della prova digitale*.

L'acquisizione è il processo di produzione di una copia forense (o *bit-stream image*, o immagine *bit* a *bit*), ovvero una copia identica al supporto informatico originale, completa del supporto compresi spazio non allocati e *slack space*[301].

Il processo di acquisizione deve essere il meno invasivo possibile, ovvero deve comportare l'alterazione del minor numero possibile di *bit*, possibilmente mirando all'inalterabilità del supporto sorgente, allo scopo di produrre una sequenza di *bit* che rappresenti la sequenza originaria. Il prodotto finale di un'acquisizione può dunque essere un clone, ossia un dispositivo che contiene l'esatta e identica sequenza del dispositivo sorgente, oppure un *file* immagine (o una serie di *file* frammentati) che rappresentano l'esatta e identica sequenza del dispositivo sorgente; nel secondo caso è possibile applicare algoritmi di compressione come nel caso del formato Expert Witness[302]. L'identicità tra sorgente e destinazione può essere facilmente provata mediante algoritmi di *hash*[303], funzioni matematiche che consentono di sintetizzare la rappresentazione di milioni di *bit* in stringhe esadecimali di poche decine di *bit*: infatti, l'applicazione di una stessa funzione di *hash* a due sequenze di *bit* produce sempre lo stesso risultato (*digest*) se e solo se le due sequenze in *input* sono identiche. È doveroso precisare che in alcune circostanze, quali ad esempio l'acquisizione di un sistema in funzione, c.d. acquisizione *live*[304], questa verifica

---

[301] Lo *slack space* è un insieme di dati digitali generati dalla modalità con cui i dati stessi sono organizzati in un supporto di memorizzazione. A prescindere dalle dimensioni del *file*, il supporto è strutturato in blocchi (settori) di dimensione fissa. Qualsiasi spazio inutilizzato all'interno del blocco conterrà i dati che esistevano fino al momento della cancellazione e continuerà a contenerli finché lo spazio non verrà sovrascritto in seguito a operazioni di *wiping* o ad allocazione di nuovi *file*. Gli *slack space* possono essere di vario tipo: *volume slack*, cioè lo spazio alla fine disco; *partition slack*, ossia spazio alla fine della partizione; *sector slack*, cioè lo spazio alla fine del settore non utilizzato dal *file* allocato.

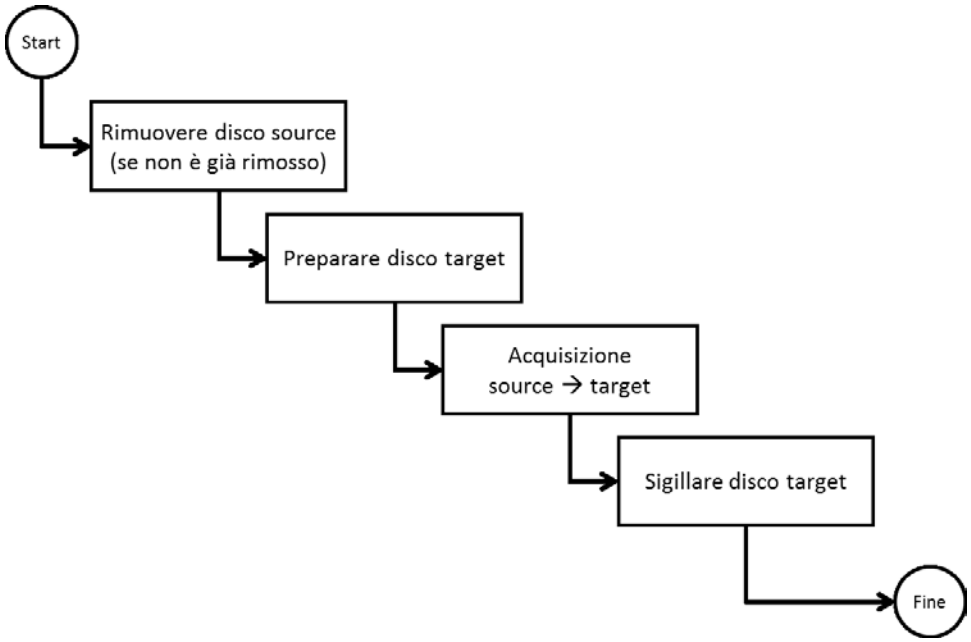
[302] EWF è un formato proprietario di dati utilizzato per copie forensi realizzato dalla Guidance Software, sviluppatrice del programma forense EnCase ma ormai supportato dalla gran parte di *software* per l'informatica forense.

[303] L'*hash*, come si è già detto, è una funzione matematica che prende in *input* una sequenza di *bit* di qualsiasi lunghezza e produce in *output* una stringa di *bit* di dimensione fissa (la cui lunghezza dipende dall'algoritmo prescelto), solitamente espresso in formato più leggibile come stringa di caratteri esadecimali (0123456789ABCDEF). Quando l'*output* della stringa di *hash* applicata al reperto originario o a copie forensi è sempre lo stesso si ha la garanzia di integrità dei dati. MD5, SHA-1, RIPEMD-160 sono alcuni degli algoritmi più comuni che possono essere utilizzati per la creazione dell'impronta.

[304] Con il termine *live forensics* si indica una metodologia di acquisizione di informazioni da un sistema informatico attuata mentre questo è operativo, al fine di catturare quei dati,

non è possibile, sarà quindi necessario fornire un'approfondita documentazione del processo di acquisizione, anche mediante l'utilizzo di immagini fotografiche e filmati video.

Figura 4 – Linee guida per l'acquisizione di dispositivi digitali spenti.[305].



transitanti o memorizzati in esso, che non sarebbero acquisibili dopo lo spegnimento dell'apparato o comunque di svolgere un monitoraggio delle attività in corso mentre queste stanno avvenendo. Gli obiettivi principali sono la cattura e la conservazione in forma statica di tutte le informazioni di rilievo che hanno natura volatile o che sarebbero troppo complesse da ricostruire a posteriori, preservando al massimo il sistema oggetto d'esame da possibili alterazioni. Sul punto, D. GABRINI, P. PERRI, G. SPECCHIO Live forensics. *In:* A. ATTANASIO, G. COSTABILE, eds. *IISFA Memberbook 2011*, Experta Edizioni, Forlì, 2011.

[305] Traduzione della figura 4 riportata nello standard ISO/IEC 27037:2012.

Si intuisce come l'attività di acquisizione da un *computer* acceso debba essere considerato un atto di natura "irripetibile" da compiere nel contraddittorio delle parti (e cioè alla presenza del difensore dell'indagato). Per svolgere un'acquisizione nel modo appropriato, sarebbe necessario svolgere un resoconto cronologico e documentati che tenesse in considerazione: l'attività svolta dal consulente *step by step*, il sistema operativo utilizzato, il contesto (ovvero la descrizione dell'ambiente e degli elementi circostanti), i programmi e versioni utilizzati dal consulente nello svolgimento delle operazioni, le cautele adottate per garantire l'integrità del dato[306].

L'attività del perito sarà quanto più credibile ed affidabile, se svolge le operazioni in modo asettico e scientifico.

I *files* sono "documenti ed informazioni modificabili e per natura stessa volatili. Nel momento in cui si accede al *file* si pone in essere un'operazione che ne consente la visualizzazione o lettura ma che contestualmente ne determina una modifica, anche involontaria"[307].

L'acquisizione, ad esempio nel caso di un *hard disk*, è caratterizzata da una copia "*master*" del *database* che dovrà essere oggetto di successiva analisi.

Non è possibile analizzare il reperto senza effettuare la copia *master*, in quanto si potrebbe verificare la rottura, la distruzione o la cancellazione dello stesso con il conseguente rischio di perdita della fonte di prova.

Dalla copia è possibile ricavare le ulteriori copie, che potranno essere consegnate alla difesa ed alla polizia giudiziaria, per consentire ad entrambe un proprio resoconto di analisi.

Si eseguirà una copia integrale *bit per bit* dell'*hard disk* del sistema oggetto del sequestro, ovvero la cosiddetta "*bit-stream image*", che consente di operare su una copia tecnicamente identica all'originale senza correre il rischio di alterare la fonte. La copia così ottenuta dovrà essere necessariamente validata, ovvero confrontata con l'originale per verificarne la sua esatta corrispondenza, allo scopo viene effettuato mediante appositi *tools* forensi il calcolo computazionale dell'*hash* del disco originale e della copia per ottenerne un confronto e garantire

---

[306] D. D'AGOSTINI, Diritto penale dell'informatica, *dai computer crimes alla digital forensic*, Experta Edizioni, Forlì, 2007.

[307] S. PESCI, Consiglio Superiore della Magistratura, Incontro di formazione decentrata Ufficio Referente distrettuale formazione magistrati Bologna "Criminalità Informatica: profili sostanziali e di ricerca e formazione della prova" Bologna 27.11.2006, L'ingresso nel processo della prova informatica.

che tra gli stessi non sia intervenuta alcuna modifica o alterazione. Il calcolo dell'*hash* è una funzione univoca atta alla trasformazione di un testo di lunghezza arbitraria in una stringa di lunghezza fissa, relativamente limitata. Tale stringa rappresenta una sorta di "impronta digitale" del testo in chiaro, e viene detta valore di *hash*[308]. Di conseguenza, due documenti che differiscono anche di un solo *bit*, producono codici di *hash* completamente differenti[309]. E' importante che i metodi utilizzati operino sulle copie, proprio per evitare un intervento diretto sulle informazioni che potrebbero alterarsi.

Al momento gli algoritmi più utilizzati per la validazione delle evidenze digitali sono MD5 e SHA-1. Entrambi questi algoritmi sono stati oggetti negli ultimi anni di attacchi matematici atti a creare *collision ad hoc*, per cui non sono più da considerare affidabili per la validazione a meno di non essere usati assieme.

A questo punto diventa molto più conveniente passare a sistemi di *hash* più sofisticati e, per ora, immuni da attacchi. Risulta evidente come, con il crescere della potenza di calcolo fornita dai moderni *computer*, sia sempre più semplice riuscire a trovare dei sistemi per generare collisioni e sia sempre più complesso riuscire a sviluppare algoritmi che possano fornire una validazione per lungo tempo. Gli algoritmi MD5 e SHA-1 non sono comunque gli unici disponibili al momento, come indicato nella Tabella seguente.

Algoritmo	Grandezza del dato finale computato	Trovati modi di generare collisioni
HAVAL	256/224/192/160/128	Sì
MD2	128	Sì
MD4	128	Sì
MD5	128	Sì
PANAMA	256	Sì
RIPEMD	128	Sì
RIPEMD-128/256	128/256	No
RIPEMD-160/320	160/320	No
SHA-0	160	Sì
SHA-1	160	Sì
SHA-256/224	256/224	No
SHA-512/384	512/384	No
Tiger (2)-192/160/128	192/160/128	No
VEST-4/8 (hash mode)	160/256	No
VEST-16/32 (hash mode)	320/512	No
WHIRLPOOL	512	No

[308] Una funzione di *hash* è una funzione matematica non invertibile in grado di processare un dato arbitrariamente grande e di calcolare, da questo, un valore di grandezza fissa. È implicito in questa definizione che qualunque funzione di *hash* al mondo ha un problema evidente: essendo il numero di dati possibili infinito ed essendo, nel contempo, il numero risultante di grandezza fissa (quindi invariabilmente un numero finito di valori), esiste la probabilità che più dati diversi generino uno stesso valore di *hash*. Tale problema è noto come collisione.

[309] A. GHIRARDINI, G. FAGGIOLI, *Computer Forensics*, Apogeo, Milano, 2010.

5.4.6. *Conservazione e trasporto*.

Le fasi di conservazione e trasporto richiedono l'adozione delle stesse precauzioni. Dopo aver prelevato i reperti bisogna osservare precise modalità di conservazione dei supporti al fine di garantire l'integrità dei dati in essi contenuti, prevenire alterazioni ed evitare danneggiamenti o rotture e, di conseguenza, l'accettabilità e la validità in giudizio dei medesimi.

Lo standard ISO/IEC 27037:2012 prescrive dei requisiti per la conservazione quali il mantenimento della catena di custodia, l'uso di imballo idoneo che dipende dalle caratteristiche del reperto da trattare e il controllo dell'ambiente in cui il reperto viene conservato (minacce ambientali, umidità, temperatura); per quanto concerne il trasporto lo standard richiede che siano messe in sicurezza le parti mobili e che il tutto sia opportunamente imballato.

5.4.7. *Chain of custody, la catena di custodia*.

Profilo fondamentale dell'idonea acquisizione e successiva conservazione e analisi delle prove informatiche è costituita inoltre dalla "catena di custodia" o "*chain of custody*" che consiste nella corretta e puntuale documentazione di tutte le attività poste in essere nel corso delle attività di *Digital Forensics*.

Le migliori pratiche di *digital forensics* evidenziano e rimarcano l'importanza di una buona gestione della prova dal primo momento in cui questa viene individuata al fine di poter concretamente conoscere, istante per istante, dove si trovi il reperto acquisito e quali attività siano state effettuate su quel reperto. I primi documenti legati ad una corretta gestione della catena di custodia di un reperto, così come espressamente prescritto dalla normativa vigente, sono i verbali. In particolare il codice di rito contempla l'obbligo di verbalizzare sia le attività del sopralluogo che quelle di sequestro[310].

La gestione della prova tuttavia non si esaurisce nella mera redazione di documentazione tecnico giuridica ma deve prevedere una serie di procedure da attuare al fine di comprovare che tutti i supporti informatici sequestrati ed i dati ivi contenuti, sottoposti ad analisi, siano stati preservati ed adeguatamente protetti

[310] Il Titolo IV del Libro V (Artt. 347 e ss. c.p.p.) del codice di procedura penale individua le attività della Polizia Giudiziaria, prescrivendo oltre all'obbligo di riferire la notizia di reato, anche le modalità di assicurazione della fonte di prova, indicando altresì gli strumenti atti all'individuazione, alla ricerca e alla repertazione della stessa.

da danneggiamenti o da possibili alterazioni durante tutta l'attività investigativa.

La sola documentazione dunque non è sufficiente, occorre mettere in atto procedure che ne garantiscano una corretta gestione, utilizzando ad esempio appositi contenitori o buste antistatiche per i reperti digitali, depositando i corpi di reato digitali presso archivi che garantiscano condizioni di temperatura ed umidità costanti, privi di luce naturale ed adeguatamente schermati dal punto di vista elettromagnetico[311]. Archivi appositamente realizzati che dovrebbero altresì prevedere sistemi di protezione fisici ad accesso condizionato, con registrazione di ogni singola apertura.

Il personale che interagisce con i reperti dovrà indossare appositi dispositivi antistatici, utilizzando strumentazione idonea nel momento in cui il reperto dovrà essere aperto per un successivo esame[312].

La normativa vigente si limita a prescrivere i casi e i modi entro cui si potrà acquisire o repertare un'evidenza, documentandone la storia e prevedendo la redazione di verbali ogni qualvolta il reperto sia consegnato all'Ufficio Corpi di Reato del Tribunale, a un perito a un C.T., ovvero ad altro organo competente per le indagini tecnico-informatiche.

Il nostro ordinamento però non detta adeguate prescrizioni al fine di evitare ogni possibile alterazione, ovvero non entra nello specifico fornendo delle procedure da adottare nel momento in cui si debba gestire un'evidenza digitale.

Negli Stati Uniti, o comunque in quasi tutti i paesi ove vige l'ordinamento di *common law*, la catena di custodia è uno *standard de facto*, messo in atto e rispettato dalle *law enforcement* come dalle agenzie federali di sicurezza. In questi casi il rispetto delle procedure e l'agire secondo una metodologia comprovata sono alla base per una corretta gestione della prova e per il suo utilizzo in un procedimento. Non seguire le procedure comunemente riconosciute pregiudica, infatti, quel reperto come elemento probatorio, inficiandone dunque la sua utilizzabilità. La catena di custodia garantisce una continuità probatoria attraverso la possibilità di tenere traccia delle fasi di individuazione, acquisizione ed analisi,

---

[311] E' notorio come le cariche elettrostatiche o forti campi elettromagnetici possano interagire con i dati contenuti all'interno di tutti quei dispositivi di memorizzazione di tipo *read-write*, come ad esempio *Hard disk*, *floppy disk*, *pen drive*, memorie allo stato solido, memorie ad accesso casuale (RAM, ROM) etc. I soli dispositivi apparentemente non influenzabili da campi elettromagnetici sono i dispositivi ottici quali CD-ROM o DVD-ROM, etc., che comunque possono essere soggetti a degrado in particolare se vengono a contatto con sostanze solventi o composti solforosi.

[312] L'uso di bracciali antistatici è opportuno ogni qual volta si viene a contatto con dispositivi elettronici. Tali dispositivi permettono di scaricare eventuali cariche elettrostatiche dell'operatore, al fine di evitare ogni possibile danneggiamento dell'*hardware* sottoposto ad analisi.

mediante la produzione di adeguata reportistica con differenti livelli di dettaglio.

Viene dunque garantita la protezione delle prove, indicando tutti i soggetti che vi hanno accesso e le ragioni per cui tali soggetti hanno in qualsiasi misura interagito con il reperto.

Il *Computer Security Resource Center* del NIST[313] individua nella catena di custodia quel processo che tiene traccia dei movimenti delle fonti di prova durante le fasi di repertamento ed analisi ed altresì ne garantisce la salvaguardia attraverso una dettagliata documentazione che riporti, tra le altre informazioni, l'identità di ogni persona che ha trattato il supporto, la data e l'ora del repertamento o del trasferimento delle *digital evidence*s, con annessa motivazione.

Le procedure da adottare per una corretta gestione della catena di custodia devono essere estremamente semplici e devono contemplare sia la documentazione da redigere, sia le necessarie procedure da adottare per una corretta gestione della prova al fine di non danneggiarla. Questo non solo assicura l'integrità della prova, ma ne rende difficile anche la contestazione dinanzi ad un giudice in sede dibattimentale.

Un documento base da redigere per una corretta gestione della catena di custodia dovrebbe rispondere a determinati quesiti e conservare informazioni sull'identità degli operatori preposti al sequestro, su cosa è stato repertato e come è stato sottoposto a sequestro, dove erano posizionati i supporti/sistemi informatici, come vengono conservate e protette le evidenze e fornire informazioni anche sul personale tecnico che può disporre dei supporti per sottoporli alle analisi del caso.

Tutta la documentazione dovrebbe inoltre essere conservata e posta al sicuro anche per eventuali verifiche *in itinere*, al fine di ricostruire la storia dell'indagine: chi ha preso in carico i supporti, dove e quando, come sono stati trasportati e dove sono conservati, chi vi ha avuto accesso e che cosa ne ha fatto. La presenza di un'imprecisione o una mancanza di informazioni anche in una sola delle numerose attività svolte potrebbe vanificare l'intero lavoro.

[313] http://csrc.nist.gov/index.html.

L’immagine seguente mostra un esempio di catena di custodia che contiene tutti i dati previsti dallo standard ISO/IEC 27037:2012.

Dettagli reperto informatico e catena di custodia			
Caso:		ID reperto:	
Informazioni sulle evidenze			
Dettagli macchina originaria			
Produttore:			
Modello:			
Serial number:			
Part number:			
Note aggiuntive (adesivi, etichette, username, psw…):			
Dettagli reperto			
Produttore:			
Modello:		Dim. (GB):	
Serial number:			
Part number:			
HASH:	MD5:		
	SHA1:		
Note aggiuntive:			
Reperto informatico originario presentato da			
Nome e cognome:			
Data e ora:			
Luogo:			
Note aggiuntive:			
Catena di custodia			
Data e ora	In carico a		Descrizione
	Nome	Firma	
	Nome	Firma	
	Nome	Firma	
	Nome	Firma	
	Nome	Firma	

5.4.8. *Analisi dei reperti informatici*.

L'analisi è quella parte dell'attività finalizzata a visionare, leggere, esaminare ed estrapolare un significato tecnico al materiale acquisito. Quanto più completa è l'analisi, tanto più saranno gli elementi che potranno essere utilizzati per sconfessare una tesi investigativa o un costrutto accusatorio[314].

L'analisi dovrà essere eseguita non solo all'interno dei *file* ma anche nei settori del supporto magnetico sui quali gli stessi sono conservati, settori a volte lasciati liberi, come gli *slack space*, le aree non allocate, le aree di *swap* del sistema in questione, parti che contengono comunque dati registrati e cancellati in precedenza e che potrebbero rivelarsi utili.

L'operatore tecnico, per svolgere un'analisi completa deve svolgere le seguenti attività[315]:

- Verificare le condizioni "fisiche" di ogni supporto magnetico oggetto del sequestro;
- Ricercare elementi utili anche tra i quaderni, gli appunti fondi di tastiera e *monitor* per individuare eventuali *password* (attività classica svolta durante la perquisizione dei luoghi);
- Individuare la presenza di *virus* o altro *software* malevolo o cosiddetti *Trojan Horse* al fine di saggiare l'effettivo totale ed esclusivo controllo del *computer* in questione o del dispositivo oggetto dell'analisi da parte dell'indagato;
- Ricostruire per quanto sia possibile, la successione cronologica delle attività svolte sul *computer* oggetto di analisi o sui *file* in esso contenuti o sui *log* del *server*, cercando in questo caso di astenersi da commenti interpretativi nella fase della ricostruzione e mirando soltanto alla raccolta del dato oggettivo (l'interpretazione dello stesso dovrà essere fatta nella coralità degli elementi raccolti);
- Confrontare, in caso di collegamento alla rete, gli indirizzi IP delle connessioni e la compatibilità degli orari delle connessioni e dell'effettiva portata, ad esempio, del *download* rispetto ai tempi di esecuzione dello stesso;
- Individuare il ruolo che assume il sistema oggetto dell'indagine rispetto ad altri eventuali *computer* ad esso collegati (*server* aziendali etc.);
- Considerare il ruolo delle persone che utilizzano il sistema per individuare eventuali soggetti informati dei fatti o comunque in grado di conoscere le *password*.

---

[314] L. LUPARIA, G. ZICCARDI, Investigazione penale e tecnologia informatica, Giuffrè Editore, 2007.

[315] D. D'AGOSTINI, Diritto penale dell'informatica, *dai computer crimes alla digital forensic*, Experta Edizioni, Forlì, 2007.

La fase di analisi presuppone necessariamente la conoscenza della struttura informatica degli elaboratori e dei sistemi operativi in gioco, ed in generale dei sistemi delle reti telematiche, e dei protocolli di comunicazione.

In molti casi alcuni dati possono risultare apparentemente nascosti. Si specifica "apparentemente" poiché ha una rilevanza penalmente differente il fatto che un documento sia volutamente nascosto dall'utente oppure se sia il sistema operativo stesso, per la sua natura, a consentire di recuperare successivamente quei documenti che sono stati cancellati dall'utente, ma soltanto apparentemente, ed in realtà si trovano "nascosti dal sistema" senza che ciò comporti un'effettiva disposizione della volontà del titolare dello stesso di "nascondere".

Questa differenza, dal punto di vista della responsabilità e del possesso, appare fondamentale in quanto una cosa è cancellare un *file* perché ritenuto di non interesse, una cosa diversa è nasconderlo. Questa puntualizzazione è importante perché in realtà, quando un *file* viene cancellato, continua a risiedere sul disco fisso. L'operazione di cancellazione non fa altro che modificare un *bit* che discrimina se il *file* deve essere visualizzato o no dall'utilizzatore del *computer*, cancellandolo parzialmente o interamente solo nel momento in cui il settore dell'*hard disk* su cui era collocata quella informazione, verrà scritto nuovamente per registrare un altro *file*[316]. Tecniche utilizzate per nascondere i dati consistono nella modifica dell'estensione del *file* per "ingannare" il sistema operativo ed impedirgli l'apertura con l'apposita applicazione; oppure utilizzare programmi di criptazione che attraverso un algoritmo di codifica e decodifica, alterino il messaggio originale così da non renderlo intelligibile ad altri, ma soltanto a coloro che conoscono la chiave di decodifica dell'informazione.

Un'ulteriore zona di interesse del disco fisso, è rappresentata dal *file di swap*, che viene utilizzato dal sistema per gestire la memoria virtuale ed ospitare i contenuti in eccesso della memoria RAM[317]. Questo *file* può essere configurato dal sistema operativo come *file* temporaneo, e di conseguenza assume un comportamento simile a quello della memoria RAM. La sua utilità si riscontra in caso di perquisizione e sequestro di un *computer* che viene rinvenuto acceso e quindi sarebbe opportuno analizzarlo immediatamente per evitare la perdita di preziose informazioni sull'attività in essere dell'indagato.

---

[316] D. D'AGOSTINI, Diritto penale dell'informatica, *dai computer crimes alla digital forensic*, Experta Edizioni, Forlì, 2007.

[317] O. SIGNORILE, *Computer Forensic Guidelines: un approccio metodico – procedurale per l'acquisizione e analisi delle digital evidence*, in Ciberspazio e Diritto, Enrico Mucchi Editore, Modena, 2009.

La fase di analisi invece presuppone approfondite nozioni di architettura degli elaboratori e di sistemi operativi, ma anche di reti, di protocolli di comunicazione, di amministrazione di sistemi e anche un certo talento da parte dell'esaminatore che deve scovare il materiale rilevante ai fini dell'indagine.

L'attività di analisi consiste nel recuperare quei dati che possono risultare utili ai fini di un'indagine forense che quindi con tutta probabilità sono nascosti, volontariamente o no, alla vista di un comune utilizzatore: quando un *file* viene cancellato in realtà viene solo nascosto all'utente in quanto continua a risiedere sul disco. L'operazione di cancellazione non distrugge l'intero *file* ma modifica un *bit* che discrimina se il *file* è da visualizzare o no dall'utente: con questo comportamento è possibile avere velocità dell'operazione e tempo di vita del supporto di memorizzazione decisamente superiori. Le tracce del *file* cancellato si perdono solo nel momento in cui quel settore viene riscritto per ospitare un altro *file* e per questo motivo quando bisogna analizzare un disco è necessario effettuarne una copia *bit-stream* che preserva anche quei dati sembrerebbero inesistenti. Altre tecniche comunemente usate per celare i dati consistono nella modifica dell'estensione del *file* per "ingannare" il sistema operativo ed impedirgli di aprire il *file* con l'applicazione di default oppure nascondere dati scritti cifrandoli all'interno di altri documenti con la tecnica della steganografia[318].

L'investigatore deve prestare molta attenzione allo spazio non visibile all'utente comune in quanto e in quelle zone che spesso risiedono i dati più utili ai fini forensi. Alcuni di essi sono:

- *email*: la posta elettronica è una delle fonti più importanti perché mantiene un numero molto alto di informazioni;
- *file* di *peer-to-peer*: sono i *file* condivisi da applicazioni di *file-sharing* (fondamentali per risalire al *download* di copie pirata di *software* o di brani musicali o alla condivisione di materiale pedopornografico);
- *file* temporanei di internet: i *browser* impiegati per la navigazione salvano in una cartella temporanea del disco i *file* scaricati dai vari siti per poi mostrarli effettivamente a video;

[318] Il termine steganografia è composto dalle parole greche *steganòs* (nascosto) e *gràfein* (scrivere) e indica una tecnica risalente all'antica Grecia che si prefigge di nascondere la comunicazione tra due interlocutori. In informatica, due utenti possono utilizzare la steganografia digitale per inviarsi messaggi nascosti all'interno di *file* di "copertura" (filigrana elettronica), come immagini o altri *file* multimediali: ad esempio, nelle immagini a colori e di grandi dimensioni l'inserimento di messaggi richiederebbe una percentuale minima di *bit* rispetto alla totalità del *file*, non provocando alterazioni evidenti del contenuto dell'immagine.

- *file* temporanei di applicazioni: alcune applicazioni durante l'esecuzione si avvalgono di *file* di supporto per tenere traccia per eventuali *backup* (ad esempio un *word processor* salva periodicamente i cambiamenti che l'utente effettua sul documento) che verranno poi cancellati alla terminazione dell'applicazione;
- *file* di installazione: durante i processi di installazione vengono copiati o generati diversi *file* temporanei che permettono di determinare quali *software* sono stati installati sulla macchina e in che data;
- *file* di stampa: i processi di stampa vengono messi in coda e le informazioni salvate dal sistema operativo in un *file* che poi verrà cancellato nel momento in cui il processo sarà completato;
- *file* parziali: la copia di *file* da un dispositivo di memorizzazione di massa ad un altro talvolta potrebbe non andare a buon fine a causa dell'interruzione da parte dell'utente o per spazio insufficiente nel drive di destinazione durante un'operazione di generazione di *file*[319]; in tal caso sul dispositivo destinazione saranno comunque presenti i dati copiati fino al punto in cui era disponibile spazio, ma saranno trattati come un *file* cancellato parzialmente sovrascritto.

In fase di indagine può rivelarsi necessario analizzare eventuali danneggiamenti (o tentativi) nei confronti di un *computer* connesso in rete: in tal caso l'indagine si propone sia di tracciare le intrusioni nel sistema informatico (questa operazione consiste nella verifica della presenza di eventuali *backdoor*[320] o tramite l'analisi di *file* di *log*) che a scovare ed analizzare eventuale codice maligno presente nella macchina.

5.4.9. *Valutazione*.

Riguardo alla valutazione della prova informatica, occorre tenere conto di alcuni limiti all'efficacia probatoria dell'indagine tecnico-scientifica che possono influire sulla decisione giudiziale in quanto in relazione ad essi sarà articolata l'attività argomentativa delle parti.

Infatti, le argomentazioni che le parti proporranno al giudice riguardo alla

[319] Ad esempio, la decompressione di *file* di tipo "*.zip*" su un supporto con insufficiente spazio libero porta all'interruzione dell'operazione e alla visualizzazione di un messaggio che avverte dell'arresto del processo.

[320] Le *backdoor* sono porte di servizio che consentono di superare le procedure di sicurezza attivate in un sistema informatico: possono essere intenzionalmente create dai gestori del sistema informatico per permettere una più agevole opera di manutenzione dell'infrastruttura informatica o da *cracker* intenzionati a manomettere il sistema. Possono anche essere installate autonomamente da alcuni *malware* (come *virus*, *worm* o *trojan*) in modo da consentire ad un utente esterno di prendere il controllo remoto della macchina senza l'autorizzazione del proprietario.

valutazione delle risultanze probatorie influiranno necessariamente sul convincimento giudiziale. Verranno pertanto poste in sede dibattimentale osservazioni sulle tecniche di acquisizione, conservazione ed analisi dei reperti digitali, sarà quindi indispensabile che tutte le attività svolte per portare la prova digitale in giudizio siano state compiute in maniera rigorosa e scientifica e nel pieno rispetto delle prescrizioni tecniche e normative, garantendo in ogni caso la ripetibilità delle operazioni compiute per la sua estrazione. Un ulteriore aspetto significativo riguarda la determinazione delle circostanze in cui un reato è commesso e le modalità dello stesso; anche se la vittima può essere nota, ricostruire i dettagli è essenziale per far piena luce su ciò che e accaduto. La fase di valutazione della prova informatica deriva dal fatto che la prova digitale è di per se neutra, un *bit* vale 1 o 0, potendo il reperto informatico subire alterazioni, inquinamenti, occorre accertare se questi fatti si siano verificati o se erano potenzialmente verificabili. Dovranno quindi essere formulati giudizi in merito all'attendibilità del reperto informatico, nel senso della sua integrità ed autenticità, ma anche rispetto alla sua idoneità ad individuare compiutamente ed eventualmente a dimostrare la responsabilità penale dell'autore del reato o dei reati contestati.

5.4.10. *Presentazione*.

L'ultima fase dell'esame forense consiste nella presentazione di tutte le prove rinvenute dall'investigatore o dal consulente in una relazione dettagliata che sarà presa in esame durante il dibattimento. All'interno della relazione tecnica dovrà essere inserita tutta la documentazione acquisita o prodotta generata durante l'analisi. In maniera esaustiva si dovrà indicare la metodologia usata per analizzare i dati, gli strumenti utilizzati, le risultanze ottenute, fornendo una spiegazione di cosa è stato fatto, perché, da chi e in quanto tempo ogni operazione è stata eseguita. Lo scopo della presentazione è trasmettere a tutte le parti del processo i fatti accertati secondo tecniche e metodologie scientifiche di cui si dovrà illustrare le fasi percorse, evidenziando anche il pieno rispetto dei protocolli operativi a garanzia dell'autenticità delle evidenze acquisite e la piena ripetibilità delle operazioni svolte.

CAPITOLO VI

Informatica e Privacy

6.1. Introduzione - 6.2. La tutela della *privacy* in Italia - 6.3. *Privacy* e *Web* - 6.4. Il trattamento dei dati per finalità investigative - 6.5. La Legge n. 675/1996 e l'attività investigativa - 6.6. Il Codice della *Privacy*: D.Lgs. n. 196/2003 - 6.7. Il nuovo regolamento europeo sulla Privacy - 6.8. Le principali novità introdotte dal Nuovo Regolamento *Privacy* - 6.9. Considerazioni finali.

6.1. *Introduzione*.

Privacy è un termine inglese che evoca significati a volte mutevoli, sinonimo dei concetti di "riservatezza", "privatezza". Nella realtà contemporanea, con il concetto di Privacy non si intende soltanto il diritto di essere lasciati in pace o di proteggere la propria sfera privata, ma soprattutto il diritto di controllare l'uso e la circolazione dei propri dati personali che costituiscono il bene primario della società dell'informazione nella quale noi tutti viviamo. Il diritto alla *Privacy* e, in particolare, alla protezione dei dati personali costituisce un diritto fondamentale delle persone, direttamente collegato alla tutela della dignità umana, come sancito anche dalla Carta dei diritti fondamentali dell'Unione Europea[321].

La tutela della Privacy è un diritto fondamentale della persona.

La tradizionale nozione di privacy, definita come il diritto ad essere lasciati indisturbati è fondata sul criterio dell'esclusione degli altri dalla propria sfera privata, si è evoluta nel diritto di controllare come gli altri trattino i propri dati. Complice il progresso tecnologico, che consente di vivere ogni momento della propria vita *online*, perennemente connessi alla rete - sottolinea S. Rodotà - *«la tutela della privacy si è sempre più strutturata come diritto di ogni persona al mantenimento del controllo sui propri dati, ovunque essi si trovino, così riflettendo la nuova situazione nella quale ogni persona cede continuamente, e nelle forme più diverse, dati che la riguardano»*[322]. La nozione stessa di "sfera privata" si è trasformata per effetto della rivoluzione elettronica *«in un luogo di* scambi, *di condivisione di dati personali, di informazioni la cui circolazione non riguarda più soltanto quelle in uscita di cui altri possono appropriarsi o venire a conoscenza, ma interessa anche quelle in entrata, con le quali altri invadono quella sfera in forme sempre più massicce e indesiderate e così la modificano continuamente»*. Il profondo mutamento delle modalità di invasione nella sfera

[321] Glossario, sito *web* Garante.

[322] S. RODOTA', Il mondo nella rete. Quali i diritti, quali i vincoli, Laterza, Roma – Bari, 2014.

privata generano continue interferenze. *«Cediamo informazioni, lasciamo tracce quando ci vengono forniti beni o* servizi *quando cerchiamo informazioni, quando ci muoviamo nello spazio reale o virtuale»*.

Il mondo virtuale, nel quale quotidianamente ci troviamo ad operare (*internet*, *social network*, *chat*, ecc.), ha assunto il ruolo di un vero e proprio ambiente dove si esplica la propria personalità, con il risultato che *«non si ha più una persona virtuale contrapposta alla persona reale, ma un intreccio che restituisce la persona reale come connotata dal digitale»*.

Il diritto dell'interessato a controllare come vengono trattati i propri dati significa richiedere e pretendere da chi ha raccolto i dati (Titolare del trattamento) livelli di sicurezza commisurati alla loro natura e alle finalità della raccolta.

Da questa semplice ma fondamentale, considerazione deriva la disciplina della "*data protection*" prevista dal Testo Unico in materia di protezione dei dati personali (D.Lgs. n. 196/2003).

Risk assessment e modelli di gestione *privacy*, pensati e strutturati in funzione delle diverse tipologia di dati e di trattamenti, consentono la riduzione dei rischi con conseguente abbassamento della responsabilità giuridica in capo al titolare del trattamento degli stessi.

Parlare oggi di *privacy*[323] non è affatto semplice in quanto, come evidenziato da autorevole dottrina, il diritto alla *privacy* ha tanti significati ed ambiti applicativi; ed è proprio la difficoltà a ricondurre ad unità il concetto stesso di privacy è alla base della scelta del Legislatore italiano di non tradurre il termine "*privacy*". La traduzione in lingua italiana nel termine "*riservatezza*" serve indubbiamente a rendere l'idea della *privacy* come diritto connesso all'identità personale, ma non ne esaurisce tutte le possibili sfaccettature in quanto diritto connesso all'autodeterminazione individuale[324].

L'avvento di nuove e sofisticate tecnologie alla portata di tutti, la semplicità delle comunicazioni connessa con la rapidità dello scambio di informazioni ed il mondo sempre più reale di internet hanno finito per renderci tracciabili in ogni momento. Non solo i servizi di geolocalizzazione consentono di individuare fisicamente un soggetto, ma anche le tracce digitali che lasciamo ogni qualvolta

[323] Storicamente, la dottrina fa risalire la prima formulazione del concetto di diritto alla *privacy* al saggio di Samuel D. Warren (1852-1910) – Luisi D. Brandeis (1856-1941). *The Right to Privacy*, 1890, mentre il concetto di *privacy* aveva visto la luce due anni prima, nel trattato del giudice Thomas M. Cooley, A Treatise on the Law of Torts, Chicago, 1888.

[324] Si pensi al diritto all'identità personale. Esso tutela l'immagine pubblica della persona e cioè l'immagine di se, che la stessa intende proiettare nella società, mentre il diritto alla riservatezza tutela la sfera più intima e privata dell'individuo.

scriviamo su un forum, o partecipiamo ad una *chat*, acquistiamo beni o servizi *online* o semplicemente navighiamo nel *web*, generiamo un'enorme quantità di dati che circolano nella Rete indipendentemente dalla nostra volontà.

Negli ultimi anni si è scoperto di non avere infrastrutture informatiche mirate per proteggere la *privacy*, bensì architetture tecnologiche pensate per facilitare la sorveglianza[325].

Ciò è ancora più evidente se si pensa alle note rivelazioni di Edward Snowden[326], che hanno contribuito a farci riflettere sul concetto di *privacy* e a domandarci se ha ancora senso parlare di *privacy* e riservatezza in un mondo globalizzato e sempre più sorvegliato.

Nell'ultima relazione annuale al Parlamento, il Garante per la protezione dei dati personali ha sottolineato come *«il diritto alla riservatezza, tradizionalmente inteso come diritto a tutelare la vita intima dalle diverse ingerenze, ha assunto, nel mondo nuovo pervaso e condizionato dalle tecnologie, un profilo sempre più connesso alla dignità della persona, quale sintesi delle libertà che ci appartengono: libertà di scegliere, di non essere omologati, di non essere controllati, di esprimere spontaneamente la nostra creatività»*[327].

In un mondo sempre più digitalmente connesso, la protezione dei dati presuppone necessariamente la protezione dei sistemi che li conservano.

Non a caso, il nostro Codice Privacy è denominato Codice in materia di protezione dei dati personali, volendo proprio porre l'accento sull'importanza, in termini di responsabilità giuridica, del livello di adeguatezza delle misure di sicurezza adottate dal titolare del trattamento a protezione del sistema informativo.

Come precisato dal Garante nel corso dell'ultima relazione annuale, in un mondo segnato dall'incontenibile affidamento alla tecnologia di parti essenziali della nostra esistenza, proteggere i nostri dati significa proteggere la nostra vita e la nostra libertà.

6.2. *La tutela della privacy in Italia*.

---

[325] G. ZICCARDI, *Internet, controllo e libertà*, Raffaello Cortina Editore, Milano, 2015.

[326] Edward Joseph Snowden, nato il 21 giugno 1983 negli USA è un tecnico informatico, *ex contractor* della CIA (*Central lntelligence Agency*) e collaboratore della società Booz Allen Hamilton, azienda informatica di assistenza tecnica della NSA (*National Security Agency*). Nel giugno del 2013 Snowden ha rivelato al giornale The Guardian un programma segreto della NSA finalizzato a raccogliere metadati riferiti alle comunicazioni domestiche negli USA. Immediatamente dopo rese noto anche il programma "prisma" (sempre della NSA) finalizzato ad accedere al traffico internet (*email*, siti ecc.) a fini di sorveglianza. Snowden è incriminato per attività di spionaggio per aver divulgato informazioni segrete e classificate.

[327] Relazione 2013 - Discorso del Presidente Antonello Soro - Roma, 10 giugno 2014.

A partire dal 1996, anno in cui è stata introdotta nel nostro ordinamento la prima legge di carattere generale in materia di tutela delle persone rispetto al trattamento dei dati personali, ad oggi sono state emanate numerose disposizioni in materia di tutela della riservatezza della persona. La Legge 31 dicembre 1996, n. 675, relativa alla *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali* ha dato attuazione a vari provvedimenti europei ed internazionali quali la Direttiva 95/46/CE, relativa alla *Tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati* e l'Accordo di Schengen ratificato in Italia con la Legge n. 388/1993, *Relativo all'eliminazione graduale dei controlli alle frontiere comuni*.

Il 27 giugno 2003 è stato approvato dal Consiglio dei Ministri il Testo Unico in Materia di Protezione dei Dati Personali, comunemente denominato «Codice della *Privacy*». In particolare, il nuovo «Codice della *privacy*» ha dato attuazione alla Direttiva n. 2002/58/CE del 12 luglio 2002, relativa al *Trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche* che integrano e precisano le disposizioni contenute nella Direttiva 95/46/CE. Procedendo ad analizzare il Codice sulla *privacy*, è possibile distinguere tre parti principali del testo: una prima parte, relativa alle disposizioni generali, sancisce i principi cardine su cui si basa tutta la disciplina, ovvero il diritto alla protezione dei dati personali, il quale si rivolge al singolo individuo e non a categorie determinate di soggetti, garantendo così uno dei diritti fondamentali sanciti a livello comunitario in materia di *privacy*, e il principio di necessità del trattamento dei dati, volto a ridurre al minimo l'utilizzazione dei dati personali, prevedendo che i sistemi informatici ed i *software* siano configurati solo per il perseguimento delle finalità consentite, escludendo così il trattamento ogni qualvolta sia possibile perseguire dette finalità attraverso l'utilizzo di dati anonimi o di modalità tali da consentire l'identificazione solo nel momento di necessità. Le finalità espresse nel Codice sono volte alla garanzia e alla tutela dei dati, nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'individuo con particolare riferimento al diritto alla riservatezza, all'identità personale e al nuovo diritto alla protezione dei dati personali[328].

Per quanto attiene alle definizioni, sono state raggruppate in un unico

[328] Vedasi art. 2, Codice *Privacy*.

articolo (art. 4), pur provenendo da fonti diverse, per meglio facilitare la comprensione dell'intero testo. Interventi di carattere innovativo si sono avuti, in particolare, nella definizione di "*trattamento*", in cui è stata introdotta la "*consultazione*", in ottemperanza a quanto già previsto a livello comunitario, e nell'inserimento di tutta una nuova serie di definizioni relative alle misure minime di sicurezza, di cui al Titolo V e al Disciplinare Tecnico (allegato B del Codice sulla *privacy).* Dopo aver individuato i diritti dell'interessato e aver esposto le modalità per il loro esercizio, il Codice sancisce in modo sistematico le regole generali per il trattamento dei dati, specificando quali siano gli adempimenti da eseguire, a seconda che il trattamento sia effettuato da soggetti pubblici o privati e a seconda del tipo di dato che ci si trova a dover trattare (se dato personale o dato sensibile). Sempre nella prima parte del Codice sono riportate le norme relative alla sicurezza dei dati e dei sistemi, le quali introducono grandi novità soprattutto per quanto attiene l'adozione delle misure di sicurezza. Una delle peculiarità del nuovo testo legislativo riguarda l'innovazione della procedura di *notificazione* al Garante della *Privacy*, ovvero la segnalazione fatta allo stesso, ad opera del titolare, del tipo di trattamento dei dati che intende effettuare, che risulta essere notevolmente semplificata. Se prima era imposto a tutti i titolari del trattamento l'obbligo di notificare, eccetto i casi per cui si era esentati, con il nuovo Codice l'impianto normativo viene ribaltato, in quanto l'obbligatorietà della notificazione riguarda solo pochi casi specificamente individuati[329], mentre per tutti gli altri non è più necessario questo adempimento.

Anche le modalità da seguire sono state rivoluzionate: è valida la notificazione trasmessa *solo per via telematica,* utilizzando il modello predisposto dal Garante e seguendo le procedure dallo stesso indicate[330].

Circa il consenso dell'interessato, secondo la nuova disciplina esso deve «essere espresso liberamente e specificatamente in riferimento ad un trattamento chiaramente individuato», non risultando più sufficiente la formulazione «reso in

---

[329] L'art. 37 individua in positivo i casi specifici per cui è richiesta la notificazione al Garante. In sintesi occorre la notificazione quando il trattamento riguarda: dati genetici, biometrici, dati sull'ubicazione di persone o di oggetti, da chiunque effettuati; dati sensibili relativi allo stato di salute e la vita sessuale, raccolti per trattamenti sanitari; dati sensibili rilevanti lo stato psichico o la vita sessuale trattati da strutture senza scopo di lucro; dati raccolti con strumenti elettronici volti alla definizione della personalità dell'interessato, analizzare abitudini o scelte di consumo o monitorare l'utilizzo di servizi di comunicazione elettronica, ad esclusione dei trattamenti necessari per la fornitura dei servizi stessi; dati sensibili registrati in banche dati relativi a procedure di selezione del personale e ricerche di *marketing;* dati inseriti in banche dati elettroniche relative allo stato di solvibilità economica (cosiddette *centrali rischi).*

[330] Vedasi art. 38 Codice *Privacy*.

forma specifica», contenuta nella Legge n. 675/96, in ottemperanza a quanto stabilito dalla Direttiva Europea n. 95/46/CE. Inoltre viene ribadita la necessità dell'informativa all'interessato da prestarsi prima che si dia inizio al trattamento dei dati. La seconda parte del Codice è dedicata alla regolamentazione di specifici settori. Per quanto riguarda i trattamenti in ambito giudiziario, i trattamenti da parte di forze di Polizia e da parte di organismi addetti alla Difesa e sicurezza dello Stato, il Codice introduce *ex novo* la loro disciplina poiché precedentemente non erano mai stati regolamentati in forma specifica; inoltre, per i trattamenti in ambito pubblico, viene ribadita la compatibilità tra le norme in materia di accesso ai documenti amministrativi e quelle in materia di diritto di accesso ai dati personali da parte dei soggetti pubblici[331]. In campo sanitario sono state introdotte modalità semplificate circa il rilascio dell'informativa e la prestazione del consenso dell'interessato[332] nonché tutta una serie di accorgimenti volti alla garanzia dei diritti alla riservatezza del paziente, che, però, hanno suscitato già molte polemiche tra gli operatori sanitari in quanto, a livello pratico, potrebbero creare dei problemi al regolare svolgimento delle loro attività (si pensi, ad esempio, alla possibilità di non rendere immediatamente identificabili in farmacia gli intestatari delle ricette mediche). In materia di lavoro, si conferma la necessità dell'elaborazione di un codice di deontologia, soprattutto in relazione al trattamento dei dati finalizzati alla selezione del personale e alla ricezione dei *curricula.* Inoltre viene riaffermato il divieto di controllo a distanza dei lavoratori (videosorveglianza), già espresso nelle disposizioni dell'articolo 4 della Legge 25 maggio 1970 n. 300 (Statuto dei Lavoratori). Infine, in materia di telelavoro e di lavoro domestico, il Codice sancisce il dovere in capo al lavoratore «*di mantenere la necessaria riservatezza per tutto quanto si riferisce alla vita familiare*»[333].

Per quanto riguarda il settore delle telecomunicazioni, il Codice ha dato attuazione a numerose norme contenute nella Direttiva 2002/58/CE del 12 luglio

---

[331] Il riferimento è all'articolo 43 della Legge 31 dicembre 1996 n. 675 e all'articolo 16 del D.Lgs. 11 maggio 1999 n. 135, con i quali, rispettivamente, viene fatta salva l'applicazione della Legge 7 agosto 1990, n. 241, e successive modifiche, e viene confermato come le attività finalizzate all'applicazione della disciplina in materia di accesso ai documenti amministrativi siano di rilevante interesse pubblico.

[332] Le modalità di semplificazione si caratterizzano sotto tre profili: (1) Ambito oggettivo di applicazione: è possibile che l'informativa del medico e il consenso dell'interessato vengano forniti con un unico atto, valido per la pluralità di trattamenti svolti a fini sanitari; (2) Ambito soggettivo: l'informativa può essere rilasciata sia dal medico di famiglia sia da un qualsiasi altro professionista; (3) Modalità con cui vengono rilasciati sia l'informativa che il consenso: il codice richiede preferibilmente la forma scritta, pur prevedendo altre forme alternative (ad esempio carte tascabili).

[333] Vedasi art. 115 Codice *Privacy*.

2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, la quale ha sostituito la precedente Direttiva 97/66/CE del 15 dicembre 1997, in Italia recepita con il D.Lgs. 13 maggio 1998 n. 171, in materia di tutela dei dati personali nel settore delle telecomunicazioni. Pertanto in questa sezione del Codice sono ripresi gli articoli del precedente D.Lgs. n. 171/98. Le novità di particolare interesse riguardano sopratutto la conservazione dei dati relativi al traffico telefonico, che per fini civilistici non può essere superiore a sei mesi, mentre per fini di accertamento e repressione dei reati può giungere a trenta mesi (di gran lunga inferiore rispetto al precedente termine di cinque anni) con modalità di conservazione stabilite «con decreto del Ministro della Giustizia, di concerto con i Ministri dell'interno e delle Comunicazioni e su conforme parere del Garante»[334].

Infine la terza, ed ultima, parte del Codice è dedicata alla tutela dell'interessato, che può essere sia di natura amministrativa che giurisdizionale.

Vengono individuate tre forme di tutela esperibili innanzi al Garante:

- il reclamo circostanziato, con cui si denuncia una violazione della «disciplina rilevante»[335] in materia di trattamento dei dati personali;
- la segnalazione, con la quale, nel caso non sia possibile presentare un reclamo, s'intende ugualmente sollecitare un controllo da parte del Garante;
- il ricorso, con il quale si fanno valere gli specifici diritti dell'interessato[336].

In riferimento al *regime sanzionatorio,* le sanzioni amministrative risultano maggiorate nel loro importo, in modo da divenire un più efficace deterrente; mentre le disposizioni sugli illeciti penali hanno subìto una modifica, prevedendo la punizione del trattamento illecito di dati solo se dal fatto derivi nocumento, a differenza della precedente disciplina nella quale il nocumento costituiva un'aggravante.

6.3. *Privacy e Web*.

[334] Vedasi art. 132 Codice *Privacy*.

[335] Per «disciplina rilevante» s'intende l'insieme di norme contenute nel testo del Codice sulla *privacy*, negli Allegati al Codice e nei codici deontologici di settore di cui si è stata prescritta l'adozione.

[336] Vedasi art. 141 Codice *Privacy*.

La diffusione di Internet e del suo utilizzo ha mutato, si è visto, il volto dell'informatica moderna, ma ha anche sollevato nuovi problemi con riferimento alla *privacy*, soprattutto a causa dell'enorme potenziale di diffusività dell'informazione insita in questo mezzo. Oggi tutte le aziende, piccole o grandi che siano, hanno un sito *web*; molte commerciano *online*; altre sono presenti su Facebook, tutte in un modo o nell'altro permettono all'utente di interagire sfruttando le potenzialità della Rete. Connessioni veloci e *computer* potenti offrono possibilità di interazione, un tempo inimmaginabili.

Internet[337] è ormai parte integrante della società e della vita quotidiana di tutti noi. Una recente ricerca ha rilevato che in Italia, a fronte di una popolazione di circa 60 milioni di abitanti, esistono 35 milioni di utenti quotidianamente connessi al *web*, 26 milioni di utenti Facebook attivi e addirittura 97 milioni di abbonamenti di telefonia mobile. Analogamente, anche negli ambienti lavorativi è cresciuto l'utilizzo di internet e della posta elettronica, o il sempre più diffuso fenomeno del BYOD (*Bring Your Own Device*), ovvero l'utilizzo in ambito lavorativo dei propri dispositivi *smartphone* o *tablet*, che richiede l'adozione da parte del datore di lavoro di misure di sicurezza adeguate e policy aziendali aggiornate ed efficienti. In un quadro operativo così dinamico, l'obiettivo di tutte le Autorità Garanti, è quello di valutare il progresso tecnologico esaminando non solo la fattibilità tecnica dell'innovazione ma anche e sopratutto l'accettabilità giuridica sotto il profilo della tutela dei diritti. Verosimilmente in futuro si assisterà all'incorporazione dei diritti nelle tecnologie attraverso un'opera di responsabilizzazione dei titolari del trattamento dei dati. Nozioni quali, *privacy by design*, *privacy by default*, *privacy impact assessment*, *data breach*, diventeranno anche alla luce della nuova Direttiva Privacy che si approfondirà in seguito, il terreno sul quale si dovranno confrontare le aziende che intendano sfruttare le opportunità di mercato offerte dal *web*.

Proprio in considerazione di questo rapido e pervasivo sviluppo di comunicazioni digitali che già a partire dal 1999 il Garante si è occupato di valutare il delicato rapporto tra dati presenti in Internet e diritto alla privacy[338].

In primis, il Garante ha notato come la Legge sulla *privacy* regoli la diffusione dei dati personali in maniera uniforme, a prescindere dal mezzo utilizzato, e preveda una analoga disciplina sia per la diffusione di un elenco di dati personali attraverso una pubblicazione, sia per la messa a disposizione

[337] Il 29 luglio 2015 è stato presentato il testo della Dichiarazione dei diritti in Internet.

[338] Vedasi la *Newsletter* del Garante per la Protezione dei Dati Personali, 14-20 giugno 1999.

dell'elenco su Internet mediante una pagina *web* consultabile da chiunque si colleghi in rete. Le norme sulla tutela dei dati personali si applicano, infatti, a tutte le operazioni di trattamento effettuate, con o senza ausilio di mezzi elettronici.

La questione era stata sollevata da un quesito posto dalla Federazione nazionale delle imprese di spedizione che aveva domandato all'Autorità se la diffusione via Internet dell'annuario dei propri associati, prima divulgato attraverso la pubblicazione di un apposito volume, fosse contraria ai princìpi della allora vigente Legge n. 675 del 1996. Il Garante ha sottolineato che, ai fini dell'applicazione della Legge sulla *privacy*, non è rilevante la modalità attraverso cui le informazioni vengono diffuse (pubblicazione cartacea o informatica), ma il rispetto degli specifici requisiti che rendono possibile tale diffusione. In particolare, per diffondere i dati personali, anche per via telematica occorre acquisire il preventivo consenso degli interessati oppure verificare che ricorra uno dei presupposti che permetta di farne a meno: ad esempio, quando si tratta di adempiere ad un obbligo di legge o di regolamento, oppure i dati provengono da pubblici registri, elenchi o atti conoscibili da chiunque o riguardano lo svolgimento di attività economiche. Nel caso in questione, l'Autorità ha stabilito che la pubblicazione su Internet dell'elenco degli spedizionieri associati non pone particolari problemi perché le informazioni contenute nell'annuario riguardano dati relativi allo svolgimento di attività economiche che possono, quindi, essere divulgati a terzi senza il consenso delle imprese interessate (come era previsto dall'art. 20 della Legge n. 675 del 1996). Un argomento simile è venuto in considerazione in un intervento del Garante nel 2000[339] avente ad oggetto i verbali e deliberazioni della Pubblica Amministrazione immessi in rete. Nota il Garante come le pubbliche amministrazioni possano pubblicare via Internet i verbali, le deliberazioni ed altri atti ufficiali riguardanti la propria attività. Per i provvedimenti che contengono dati personali relativi a terzi, serve tuttavia una norma, anche di regolamento, che definisca l'ambito di diffusione dei dati nel rispetto del diritto alla riservatezza, come avviene, ad esempio, in alcune disposizioni che disciplinano, anche su un piano generale, la pubblicità di determinati atti (es., pubblicazione di atti nell'albo pretorio).

L'Autorità ha, innanzitutto, rilevato che, perché le deliberazioni e gli atti ufficiali contenenti dati personali possano essere consultati via Internet, vanno osservate le generali disposizioni che disciplinano il regime di pubblicità degli atti

[339] Vedasi la *Newsletter* del Garante per la Protezione dei Dati Personali, 24-30 aprile 2000.

e dei documenti delle amministrazioni pubbliche nel rispetto delle norme che tutelano la *privacy*. Tali norme prevedono particolari cautele per i dati cosiddetti «sensibili» e, anzi, pongono anche un divieto assoluto per la diffusione di quelli idonei a rivelare lo stato di salute (si potrà procedere quindi eventualmente ad «oscurare» alcuni riferimenti a dati del genere). Nel 2006[340] il Garante ha disposto il blocco di una sezione di un sito Internet, gestito presso un'associazione culturale informatica triestina, nella quale erano consultabili i dati anagrafici di centinaia di persone con l'indicazione di diagnosi e risultati di analisi cliniche. I dati erano contenuti all'interno di un foglio elettronico presente in un'area consultabile da chiunque tramite un determinato indirizzo *web*. Ad accorgersi della grave violazione della *privacy* e dell'illecita diffusione di dati sulla salute è stata la figlia di una delle persone interessate che, effettuando una ricerca mediante un motore di ricerca, aveva scoperto per caso che, insieme a molti altri nominativi, erano visibili anche il nome e il cognome del padre con l'indicazione di importanti dati sul suo stato di salute. La donna ha segnalato la circostanza al Garante, il quale ha disposto tempestivamente il blocco del trattamento dei dati. Il Codice sulla *privacy* vieta, infatti, la diffusione, in qualunque forma, dei dati sulla salute (cosiddetti dati sensibili). Il provvedimento di blocco si è reso necessario considerato l'elevato numero di soggetti interessati dall'illecita diffusione dei dati idonei a rivelare il loro stato di salute e il concreto rischio di un grave pregiudizio nei loro confronti. Il sito ha dovuto rimuovere immediatamente le pagine «incriminate» dopo la notifica del provvedimento tramite la Guardia di finanza.

Un fatto increscioso è occorso nel 2007 in Puglia[341], e ha comportato un intervento deciso del Garante, che ha bloccato i nomi di migliaia di disabili pubblicati sul sito della Regione. Il Garante ha vietato alla regione Puglia la diffusione dei dati sullo stato di salute di circa 4.500 disabili, reperibili sul sito della Regione. In base al provvedimento la Regione ha disposto la rimozione della pagina. L'intervento del Garante è stato deciso a seguito di una nota in cui si segnalava che, *online,* sul Bollettino regionale erano riportate le graduatorie dei disabili beneficiari di un contributo per l'acquisto di un *personal computer*.

Sul sito erano consultabili gli elenchi di tutte le domande presentate per avere il contributo, accolte o respinte con l'indicazione dei motivi del rifiuto. Nel corso degli accertamenti il Garante ha rilevato che tali graduatorie riportavano

---

[340] Vedasi la *Newsletter* del Garante per la Protezione dei Dati Personali, n. 272 del 7 marzo 2006.

[341] Vedasi la *Newsletter* del Garante per la Protezione dei Dati Personali, n. 286 del 26 febbraio 2007.

nomi e cognomi dei richiedenti, immediatamente visibili in rete e associati alle diverse patologie: disabili dell'udito e del linguaggio, disabili della vista, disabili motori. Inoltre, i dati relativi al codice fiscale, comune di residenza e data di nascita erano integralmente visibili mediante la semplice trasposizione del documento dal formato "PDF" al formato «Word». Nel provvedimento il Garante ha riconosciuto che tale pubblicazione rappresenta una diffusione di dati illecita perché consente di far conoscere ad estranei, informazioni sullo stato di salute di un elevato numero di persone arrecando loro un grave pregiudizio. L'Autorità ha ordinato, inoltre, alla Regione che nel predisporre atti in cui si riconoscono benefici a particolari categorie siano adottanti opportuni accorgimenti in grado di garantire la riservatezza e la dignità dei beneficiari.

Simile, anche se con riferimento a dati personali, un fatto accaduto presso Palau, in Sardegna[342]: su segnalazione del Comune di Palau, l'Autorità ha bloccato il trattamento dei dati personali relativi ad una lista contenente i nomi degli alunni delle scuole medie inferiori, secondarie e superiori che hanno ottenuto un contributo per l'acquisto dei libri di testo apparsa sul sito *web* del capogruppo consiliare di minoranza.

Tante le informazioni personali pubblicate: i dati identificativi di alunni e genitori, l'ammontare del contributo economico erogato e, in alcuni casi, perfino le coordinate del conto corrente bancario. Il Comune, che aveva segnalato all'Autorità la diffusione dei dati, aveva precisato di non averne dato pubblicità per evitare che i dati personali di natura economica divenissero facilmente di dominio pubblico. Gli elenchi, infatti, non erano stati affissi né all'albo pretorio, né pubblicati sul sito istituzionale perché, secondo l'amministrazione comunale, la loro diffusione poteva creare imbarazzo o disagio agli interessati, appartenenti a fasce deboli della popolazione, ed esporli a conseguenze indesiderate. Le informazioni erano comunque accessibili su richiesta. Una copia degli elenchi era stata consegnata anche al capogruppo di minoranza in ragione del suo mandato politico, il quale decise invece di pubblicarla sul suo sito. Il trattamento dei dati contenuti negli atti dell'amministrazione comunale - ha ricordato l'Autorità - può essere effettuato dai consiglieri in ragione del loro mandato, ma sempre nel rispetto del diritto alla riservatezza degli interessati. La pubblicazione su Internet di queste informazioni personali, rese in tal modo immediatamente accessibili a tutti attraverso una semplice ricerca per nome, è risultata invece illecita, in

[342] Vedasi la *Newsletter* del Garante per la Protezione dei Dati Personali, n. 305 del 22 aprile 2008.

particolare perché eccessiva rispetto alle finalità per le quali le informazioni erano state raccolte. Il Garante ha, pertanto, disposto in via d'urgenza il blocco dei dati diffusi dal sito in attesa di ulteriori accertamenti. Il consigliere, nel frattempo, avrebbe dovuto limitarsi a conservare i dati senza poter compiere nessun'altra operazione di trattamento.

6.4. *Il trattamento dei dati per finalità investigative*.

Quello del diritto alla riservatezza è un problema strettamente connesso e contrapposto con le attività in generale dell'investigatore privato. Le indagini, infatti, incidono sotto due profili con la tutela del diritto alla riservatezza: da un lato le investigazioni trovano limiti interni, dovendo svolgersi in modo da garantire la riservatezza dei dati raccolti, dall'altro le investigazioni incontrano il limite esterno degli ostacoli che sono frapposti dai soggetti privati a tutela della propria riservatezza[343].

La *ratio* della normativa è quella di tutelare il diritto alla prova da un lato, mentre dall'altro di tutelare la *privacy*, soprattutto per quanto attiene alla riservatezza, all'identità personale ed al diritto alla protezione dei dati personali nel compimento delle investigazioni[344]. Al centro del sistema normativo vigente sono posti i concetti di riservatezza e identità personale. Si tratta di beni personali suscettibili di peculiari forme di tutela volte a sanzionare i comportamenti che costituiscono "indebite intrusioni" nella sfera della riservatezza, caratterizzata dal diritto di mettere determinate informazioni a disposizione unicamente di specifici destinatari prescelti. Nel 1995 la Direttiva europea n. 46 obbligò gli stati membri ad adottare norme per garantire la sicurezza dei dati personali.

In particolare nel disegno di legge n. 1901 *ter*, approvato alla Camera il 6 dicembre 1995, veniva totalmente ignorata la problematica degli investigatori privati. Di conseguenza l'investigatore privato che avesse voluto indagare sui dati attinenti alla vita privata di altri soggetti (quindi sempre) avrebbe dovuto avvisare l'interessato dello scopo per cui raccoglieva tali dati e chiedergli il consenso. Inoltre l'interessato poteva addirittura chiedere all'investigatore privato di conoscere i dati che aveva raccolto[345]. Sono limiti che evidentemente impedivano, rendendola totalmente inutile, lo svolgimento dell'attività investigativa. A seguito

[343] P. TONINI, Manuale *di procedura penale*, Giuffrè Editore, Milano. 2001.

[344] V. SALVADORI, *L'investigatore* privato autorizzato *e il segreto professionale*, 2005, in http://www.altalex.com/index.php ?idnot=9407.

[345] P. TONINI. *Manuale di procedura* penale, Giuffrè Editore, Milano, 2001.

di questa lacuna ci fu una mobilitazione generale da parte della Federpol (Federazione Italiana degli Istituti Privati per le Investigazioni le Informazioni e la Sicurezza), di avvocati e di docenti universitari che portò alla previsione di alcune deroghe in favore dell'attività di indagine. Nacque così la Legge n. 675/1996, intitolata *«Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali»*.

6.5. *La Legge n. 675/1996 e l'attività investigativa*.

Per comprendere bene la normativa sulla *privacy* è necessario distinguere diverse tipologie di dati: i dati personali non sensibili *(c.d.* comuni) e i dati sensibili, con particolare attenzione a quelli riguardanti la salute e la vita sessuale.

In particolare, l'art. 1, comma 2, lett. c), della Legge n. 675/1996 stabilisce che *«ai fini della presente Legge si intende: […] c) per "**dato personale**" qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili" anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale»*. L'art. 22, comma 1, invece, definisce i **"dati sensibili"** come quei *«dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati idonei a rivelare lo stato di salute e la vita sessuale»*.

a) Dati personali non sensibili.

Per quanto riguarda i dati personali non sensibili l'art. 12, lett. h), prevede che *«il consenso non è richiesto quando il trattamento: [...] è necessario ai fini dello svolgimento delle investigazioni di cui all'art. 38 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale [...], o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento»*. Inoltre, a norma dell'art. 10, comma 4, non deve neanche essere data la comune informativa perché la persona non ha il diritto di opporsi; infatti, l'art. 14, lett. e), stabilisce che *«i diritti di cui all'art. 13, comma 1, lettere*

c) e d)[346]*, non possono essere esercitati nei confronti dei trattamenti di dati personali raccolti: [...] ai sensi dell'art. 12, comma 1, lettera h), limitatamente al periodo durante il quale potrebbe derivarne pregiudizio per lo svolgimento delle investigazioni o per l'esercizio del diritto di cui alla medesima lettera h)».*

Le condizioni che autorizzano la deroga, quindi, riguardano esclusivamente:

- lo svolgimento delle investigazioni di cui all'art. 38 delle norme di attuazione, di coordinamento e transitorie del Codice di procedura penale;
- il far valere o difendere un diritto in sede giudiziaria. Con l'ulteriore limite temporale;
- per il periodo strettamente necessario al loro perseguimento. Se tali condizioni non sussistono vige la regola generale e quindi, in caso di inosservanza, anche le relative sanzioni previste dalla Legge n. 675/1996.

Nel caso in cui si raccolgano le informazioni personali presso un soggetto (non necessariamente la persona a cui si riferiscono i dati), l'art.10, comma 1, stabilisce che: *«l'interessato o la persona presso la quale sono raccolti i dati personali devono essere preventivamente informati per iscritto circa:*

a) le finalità e le modalità del trattamento cui sono destinati i dati;

b) la natura obbligatoria o facoltativa del conferimento dei dati;

c) le conseguenze di un eventuale rifiuto di rispondere;

d) i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;

e) i diritti di cui all'art. 13;

f) il nome, la denominazione o la ragione sociale e il domicilio, la residenza o la sede del titolare e, se designato, del responsabile».

---

[346] L'art. 13, lett. c) e d) stabiliva che: *«In relazione al trattamento di dati personali l'interessato ha diritto*:*[...] c) di ottenere.* a *cura del titolare* o *del responsabile, senza ritardo:*

1) la *conferma dell'esistenza* o *meno di dati personali che lo riguardano. anche se* non anc*ora registrati. e la comunicazione in forma intellegibile dei medesimi dati e della loro origine. Nonché della logica e delle finalità su cui si* basa *il trattamento; la richiesta può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore* di *novanta giorni;*

2) la cancellazione, la trasformazione in forma anonima o *il blocco dei dati trattati in violazione* di *legge, compresi quelli di cui non è necessaria lo conservazione in relazione agli scopi per* i *quali i dati sono stati raccolti* o *successivamente trottati;*

3) l'aggiornamento, la rettificazione ovvero, qualora vi abbia *interesse, l'integrazione dei dati;*

4) l'attestazione che le operazioni di cui ai numeri 2) e 3) sono state portate o *conoscenza, anche per quanto riguarda il loro contenuto,* a *coloro ai quali i dati sono stati comunicati* o *diffusi, eccettuato il* coso *in* cui *tale adempimento si riveli impossibile* o *comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato;*

d) di opporsi, in tutto o *in parte. per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta».*

Si possono agevolmente notare alcune similitudini tra gli elementi dell'informativa di cui alla Legge n. 675/1996 e gli avvertimenti previsti dall'art. 391 *bis*, comma 3, lett. a), c.p.p., tanto che, in alcuni casi, l'informativa e l'avvertimento possono essere fusi tra loro, naturalmente con gli opportuni adattamenti[347].

b) Dati sensibili in particolare quelli attinenti alla salute e vita sessuale.

L'elemento di maggiore impatto riguarda il trattamento dei dati contemplati al capo IV della Legge ed in particolare dei dati sensibili e di quelli inerenti alla salute[348]. A tal proposito la Legge n. 675/1996 prevede una limitazione riguardo ai dati personali "sensibili" che possono essere oggetto di indagine.

L'art. 22, comma 4, stabilisce che *«i dati personali idonei a rivelare lo stato di salute e la vita sessuale possono essere oggetto di trattamento previa autorizzazione del Garante, qualora il trattamento sia necessario ai fini dello svolgimento delle investigazioni di cui all'art. 38 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale [...], o, comunque, per far valere o difendere in sede giudiziaria un diritto di rango pari a quello dell'interessato, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Il Garante prescrive le misure e gli accorgimenti di cui al comma 2 e promuove la sottoscrizione di un apposito codice di deontologia e di buona condotta secondo le modalità di cui all'art. 31, comma 1, lettera h). Resta fermo quanto previsto dall'art. 43, comma* 2». Infine, in relazione ai dati idonei a rivelare lo stato di salute, l'art. 23, comma 4, ne vieta la diffusione, *«Salvo nel caso in cui sia necessaria per finalità di prevenzione, accertamento o repressione dei reati con l'osservanza delle norme che regolano la materia»*.

Il Garante, successivamente all'entrata in vigore della Legge n. 675/1996, ha emesso una serie di autorizzazioni di carattere generale, annualmente rinnovate, valevoli per alcune tipologie di dati. Per quanto riguarda il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale deve essere effettuato anche nel rispetto dell'Autorizzazione generale del Garante n. 2.

La specifica attività svolta dall'investigatore privato è regolamentata

[347] P. TONINI. *Manuale di* procedura *penale.* Giuffrè Editore, Milano. 2001.

[348] G. LOCATELLI, G. SARNO, *Gli atti di investigazione difensiva nel procedimento penale,* CEDAM, Padova, 2006.

nell'Autorizzazione generale del Garante n. 6, secondo la quale *«il trattamento può essere effettuato unicamente per l'espletamento dell'incarico ricevuto»* dal cliente *e in particolare:*

a) per permettere a chi conferisce uno specifico incarico di far valere o difendere in sede giudiziaria un proprio diritto che, quando i dati siano idonei a rivelare lo stato di salute e la vita sessuale dell'interessato, deve essere di rango pari a quello del soggetto al quale si riferiscono i dati, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile;
b) su incarico di un difensore in riferimento ad un procedimento penale, per ricercare e individuare elementi a favore del relativo assistito da utilizzare ai soli fini dell'esercizio del dritto alla prova».

Il trattamento può riguardare i dati sensibili per eseguire *«specifici incarichi conferiti per scopi determinati e legittimi»;* inoltre i *«dati devono essere pertinenti e non eccedenti rispetto agli incarichi conferiti».*

L'Autorizzazione generale del Garante n. 6 stabilisce anche che *«gli investigatori privati non possono intraprendere di propria iniziativa investigazioni, ricerche o altre forme di raccolta di dati»,* ma solo sulla base di un apposito incarico conferito per iscritto.

L'Autorizzazione generale del Garante n. 6 fissa inoltre che *«i dati sensibili possono essere conservati per un periodo non superiore a quello strettamente necessario per eseguire l'incarico ricevuta»* e *«una volta conclusa la specifica attività investigativa, il trattamento deve cessare in ogni sua forma, fatta eccezione per l'immediata comunicazione al difensore o al soggetto che ha conferito l'incarica».* Infine afferma che *«la mera pendenza del procedimento al quale l'investigazione è collegata, ovvero il passaggio ad altre fasi di giudizio in attesa della formazione del giudicato, non costituiscono, di per se stessi una giustificazione valida per la conservazione dei dati da parte dell'investigatore privato».* Tuttavia, l'investigatore può essere chiamato a testimoniare su quanto da lui effettuato e la conservazione dei documenti da questi redatti può essere fondamentale, soprattutto se è passato del tempo da quando ha svolto le attività su cui verte la testimonianza. La conservazione di tale documentazione (non eccedendo le tempistiche processuali) può essere scriminata, *ex* art. 51 c.p. (adempimento di un dovere), dall'adempiere il dovere di testimoniare secondo

verità, restante però l'obbligo del segreto professionale[349].

Per quanto riguarda la comunicazione, l'Autorizzazione generale del Garante n. 6 stabilisce che *«i dati possono essere comunicati unicamente al soggetto che ha conferito l'incarico»*. Inoltre *«non possono essere comunicati ad un altro investigatore privato, salvo che questi sia stato indicato nominativamente nell'atto di incarico e la comunicazione sia necessaria per lo svolgimento dei compiti affidati»*.

6.6. *Il Codice della Privacy: D.Lgs. n. 196/2003.*

Il Codice della Privacy ripropone in buona parte la normativa della Legge n. 675/1996. L'art. 24, comma 1, lett. f), stabilisce che il consenso per il trattamento dei dati non è richiesto quando, *«con esclusione della diffusione, è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla Legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale»*.

Quindi, per garantire lo svolgimento delle indagini difensive, il Codice della Privacy esclude qualsiasi autorizzazione preventiva da parte dell'interessato al professionista che acquisisca dati personali anche di natura sensibile.

Naturalmente l'autorizzazione generalizzata al trattamento dei dati sensibili è limitata all'espletamento dell'incarico professionale secondo i limiti del proprio ordinamento.

Secondo il contenuto dell'autorizzazione del Garante, i dati sensibili possono, inoltre, essere comunicati e ove necessario diffusi, a soggetti pubblici o privati, nei limiti strettamente pertinenti all'espletamento dell'incarico conferito e nel rispetto, in ogni caso, del segreto professionale. Con tale provvedimento viene riconosciuto all'avvocato che intenda svolgere le investigazioni difensive ampio potere, eliminando tutti gli oneri specifici previsti dalla legge, tra cui la necessità delle attività di notificazione o comunicazione. Rimane il dovere dell'avvocato di informare il soggetto che renda dichiarazioni nel corso dello svolgimento di investigazioni difensive della circostanza che le notizie fornite saranno utilizzate in ossequio alle forme e ai limiti stabiliti dalle norme sulla tutela della riservatezza. L'avvocato è tenuto alla custodia dei dati personali oggetto di

[349] P. TONINI, Manuale *di procedura penale*, Giuffrè Editore. Milano, 2001.

trattamento, in modo da ridurre al minimo i rischi di distruzione o perdita dei dati ovvero di accesso non autorizzato o di trattamento non consentito. Il professionista è quindi obbligato ad adottare preventive misure di sicurezza idonee ad assicurare la correttezza della custodia dei dati.

Dalla disciplina della Legge n. 675/1996 e successivamente da quella del Codice della *privacy* emerge, in conclusione, che la rilevanza delle investigazioni difensive esce certamente rafforzata, in quanto queste ultime sono citate espressamente come ipotesi di generalizzata deroga alla previsione delle regole sulla riservatezza e specificamente differenziate rispetto agli altri diritti attinenti alla difesa in giudizio. In particolare la chiarezza del riferimento esclude qualsiasi possibile lettura interpretativa riduttiva dei diritti del difensore nell'attività di ricerca della prova a discarico.

6.7. *Il nuovo regolamento europeo sulla Privacy.*

Il 4 maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il nuovo Regolamento sulla protezione dei dati personali e la libera circolazione dei dati personali, che si applicherà a decorrere dal 25 maggio 2018. Il nuovo regolamento, denominato "Nuovo Pacchetto Protezione Dati", risulta essere composto da 99 articoli, suddivisi in 14 capitoli. Il nuovo Regolamento abroga la Direttiva 95/46/CE, attuata in Italia prima con la Legge n. 675/96 e successivamente con il Codice Privacy del 2003, analizzate nei paragrafi precedenti, e si applicherà direttamente in tutti gli Stati Membri senza necessità di un intervento legislativo dei medesimi a tal fine. Lo strumento del regolamento è stato utilizzato proprio per far fronte alle critiche che sono sempre state mosse alla Direttiva Privacy, che invece, in quanto direttiva, è stata attuata con sostanziali differenze nei vari Stati Membri. Questo ha, di fatto, determinato una scarsa armonizzazione tra le normative dei vari Stati Membri e per tanto il 25 gennaio del 2012 la Commissione Europea ha proposto una sua bozza di regolamento, che è stata oggetto di analisi e discussione tra le Istituzioni europee negli ultimi sei anni, fino alla sua definitiva approvazione il 6 aprile 2016.

La Direttiva Privacy fu adottata quando Internet non era ancora diffuso, i *social network,* le *App* o *l'Internet of Things* (cioè la possibilità per oggetti comuni di essere connessi a Internet e raccogliere enormi quantità di dati relativi ai comportamenti delle persone) non esistevano. Le tecnologie che si sono diffuse negli ultimi anni e l'internazionalizzazione dei flussi di dati hanno

significativamente aumentato il rischio per gli individui di diminuire o perdere il controllo sui propri dati. Il nuovo Regolamento è stato introdotto proprio per fornire delle risposte e degli strumenti operativi a queste sfide. Nel gennaio 2012 la Commissione europea presentava ufficialmente il cosiddetto "*pacchetto protezione dati*" con lo scopo di garantire un quadro coerente ed un sistema complessivamente armonizzato in materia nell'UE.

Il Parlamento Europeo[350], in data 14 Aprile u.s., ha approvato definitivamente, dopo un *iter* legislativo durato oltre quattro anni, il c.d. "*Pacchetto protezione dati*", che si compone di due diversi strumenti:

- un nuovo Regolamento concernente la "tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati", volto a disciplinare i trattamenti di dati personali, sia nel settore privato, sia nel settore pubblico, e destinato ad abrogare la Direttiva 95/46/CE[351]("Direttiva 95/46") che ha portato in Italia, all'adozione del vigente D.Lgs. 30 giugno 2003 n. 196 ("Codice *Privacy*");
- una nuova Direttiva indirizzata alla "regolamentazione dei settori di prevenzione, contrasto e repressione dei crimini, nonché all'esecuzione delle sanzioni penali", che sostituirà (e integrerà) la decisione quadro 977/2008/CE sulla protezione dei dati personali scambiati dalle autorità di polizia e giustizia (che l'Italia, peraltro, non ha ancora attuato).

La pubblicazione del *Nuovo Pacchetto Protezione Dati* sulla Gazzetta UE è avvenuta in data 4 maggio 2016; a partire dal ventesimo giorno dalla pubblicazione, gli Stati membri avranno due anni di tempo per allineare la normativa nazionale alle prescrizioni introdotte dal Nuovo Regolamento, che diventerà definitivamente applicabile in tutto il territorio UE a partire dal 25 maggio 2018. Per quel che concerne la Nuova Direttiva, gli Stati membri avranno due anni per recepire con apposite norme le sue disposizioni all'interno dell'ordinamento nazionale.

---

[350] Ai sensi dell'articolo 16 del TFUE, il Parlamento e il Consiglio stabiliscono le norme relative alla protezione delle persone fisiche in merito al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e delle agenzie dell'Unione, nonché da parte degli Stati membri nell'esercizio delle attività che rientrano nel campo di applicazione del diritto dell'Unione.

[351] Adottata nel 1995, ha costituito, fino ad oggi, la pietra angolare nell'impianto della vigente normativa dell'UE in materia di protezione dei dati personali ed ha due obiettivi: salvaguardare il diritto fondamentale alla protezione dei dati e garantire la libera circolazione dei dati personali tra gli Stati membri.

Il nuovo "pacchetto protezione dati" mira ad adeguare la *data protection* rispetto all'evoluzione tecnologica che ha determinato un aumento dei flussi transfrontalieri e, quindi, dei dati scambiati tra attori pubblici e privati, rendendo così necessari: da un lato, una più libera circolazione di dati all'interno dell'UE ma, dall'altro, un più elevato livello di protezione. Merita altresì porre in rilievo la forte volontà del Legislatore europeo di eliminare la frammentazione applicativa della normativa in materia di protezione dei dati personali nel territorio dell'UE, dovuta alle diverse leggi di recepimento della Direttiva 95/46.

6.8. *Le principali novità introdotte dal Nuovo Regolamento Privacy*.

1 ***Ambito di applicazione territoriale*****.**

1.1 *Le norme attuali*.

L'attuale Direttiva 95/46 prevede che la disciplina in materia di tutela di dati personali trovi applicazione, per il tramite delle legislazioni nazionali, quando il trattamento di dati personali è effettuato "nel contesto delle attività svolte dal titolare situato nell'UE".

Sulla base di tale principio, il vigente Codice Privacy (art. 5) prevede che le sue norme s'applichino:

1. al "trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato [italiano] o in luogo comunque soggetto alla sovranità dello Stato [italiano]";
2. "anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato [italiano] anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea".

1.2 *Le nuove norme*.

Una delle maggiori caratteristiche del Nuovo Regolamento è senz'altro il suo ambito di applicazione, che si pone in maniera innovativa sotto due profili:

1. modifica la concezione tradizionale del principio di stabilimento;
2. estende l'ambito di applicazione anche a titolari e responsabili di trattamento ("Titolari" e "Responsabili") non residenti nell'UE.

Il Nuovo Regolamento, infatti, rovescia il tradizionale principio di stabilimento, sancendo l'applicabilità della disciplina da questo dettata "indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione" e stabilisce l'applicazione delle sue regole anche a Titolari e Responsabili non stabiliti nell'UE[352] che:

1. trattino dati personali di persone fisiche che si trovano nell'UE quando il trattamento è in relazione a offerte di beni e servizi, indipendentemente dal fatto che sia richiesto o meno un pagamento;
2. effettuino attività di monitoraggio sul comportamento di persone fisiche che si trovano nell'UE nella misura in cui tale comportamento avvenga nell'UE.

2 ***Nuovi obblighi e responsabilità.***

Il Nuovo Regolamento ridefinisce le figure di Titolare e Responsabile attribuendo loro obblighi ulteriori rispetto a quanto previsto dall'attuale Direttiva 95/46 e dal Codice Privacy. La non concretezza e l'inefficienza delle *policies* sotto esposte costituisce per il Titolare fonte di responsabilità (principio di rendicontazione o di "*accountability*", Artt. 24 e 32). Con il Nuovo Regolamento il Titolare ha un ruolo più proattivo e obblighi più pregnanti, finalizzati non soltanto al formalistico rispetto delle regole, ma anche all'adozione di tutti gli accorgimenti tecnici e organizzativi necessari a garantire la *compliance* effettiva dei trattamenti, anche sotto il profilo della sicurezza.

[352] Il Legislatore europeo dimostra così di aver preso in considerazione gli orientamenti delineatisi nella giurisprudenza della Corte di giustizia europea (soprattutto a partire dalla sentenza Google Spain) volti ad estendere la normativa europea in materia di tutela dei dati personali anche a casi in cui i Titolari sono soggetti non europei e i dati sono trattati principalmente fuori dall'Europa.

2.1 *Accresciuti obblighi di trasparenza* (Artt. 5 e 12).

Il Legislatore europeo dedica una sezione del Nuovo Regolamento alla "Trasparenza" (Sezione 1 del Capo III) e, con riferimento alle modalità di trattamento dei dati, richiede che le informazioni all'interessato:

1. siano rese con un linguaggio semplice e chiaro, soprattutto nel caso di minori;
2. abbiano sempre forma scritta[353], l'informativa in forma orale essendo ammessa solo quando ciò è richiesto dall'interessato e l'identità di questi possa essere provata con altri mezzi;
3. prevedano, tra l'altro, il periodo di conservazione dei dati personali, il diritto di proporre reclamo ad un'autorità di controllo, l'intenzione del titolare di trasferire dati personali a un paese terzo.

2.2 *Privacy by design e by default* (art. 25)[354].

1. La *privacy by design* richiede che Il Titolare adotti e attui misure tecniche e organizzative sin dal momento della progettazione oltre che nell'esecuzione del trattamento, che tutelino i principi di protezione dei dati;
2. La *privacy by default* presuppone invece, nella modalità operativa del trattamento, misure e tecniche che, per impostazione predefinita, garantiscano l'utilizzo dei soli dati personali necessari per ciascuna specifica finalità di trattamento.

[353] Ferma la possibilità di utilizzare apposite modalità elettroniche.

[354] I principi di *privacy by design* e *by default* si possono comunque dedurre anche dal Codice *Privacy*, attraverso il combinato disposto degli Artt. 3 e 11 lett. 3, che richiamano, infatti, i principi di minimizzazione e di necessità e che trovano, attraverso il Nuovo Regolamento, enunciazione espressa al fine di una tutela più intensa dei diritti dell'interessato a fronte di un costante sviluppo di nuove tecnologie.

2.3 *Data breach* (Artt. 33 e 34).

Attualmente prevede che solo i "fornitori di servizi di comunicazione elettronica accessibili al pubblico" hanno l'obbligo di comunicare l'avvenuta violazione di dati personali:

1. al Garante per la protezione dei dati personali ("Garante");
2. in determinati casi, anche al contraente/cliente.

Il Nuovo Regolamento estende tale obbligo di comunicazione a tutti i Titolari e Responsabili, quali che siano i trattamenti posti in essere. Nello specifico, il Responsabile deve informare il Titolare senza ingiustificato ritardo della violazione e quest'ultimo deve notificare la violazione, a sua volta senza ingiustificato ritardo, all'autorità di controllo (i.e., al Garante) e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la suesposta violazione presenti un rischio per i diritti e le libertà delle persone[355]. È previsto inoltre un obbligo di comunicazione anche all'interessato, se la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche[356]. La finalità della norma in questione, è palesemente quella di consentire all'autorità di controllo di attivarsi senza ritardo in modo da valutare quale sia la gravità della violazione e quali misure imporre al Titolare. Da notare, che mentre per la notifica all'autorità di controllo si richiede "un rischio per i diritti e le libertà degli individui", per la notifica all'interessato è necessario che il rischio sia "elevato": dunque, in quest'ultimo caso, è richiesta una soglia di pericolo maggiore anche per evitare inutili allarmismi degli interessati a fronte di violazioni di dati meramente potenziali.

[355] Qualora la notifica non sia effettuata entro 72 ore, deve essere corredata da una giustificazione motivata. La notifica deve contenere almeno, a titolo esemplificativo e non esaustivo: (1) la descrizione della natura della violazione e, ove possibile, il numero degli interessati, (2) il contatto del responsabile della protezione dati o di altro punto di contatto per ottenere più informazioni, (3) la descrizione delle misure adottate o che si intende adottare per porre rimedio alla violazione dei dati.

[356] Limitati casi di esclusione dall'obbligo di notifica all'interessato sono i seguenti: (1) se il Titolare ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, (2) se il Titolare ha successivamente adottato misure atte a scoraggiare il sopraggiungere di un elevato rischio per i diritti degli interessati; (3) se detta comunicazione richiederebbe sforzi sproporzionati (in tal caso si procede con una comunicazione pubblica tramite la quale gli interessati sono informati con analoga efficacia).

2.4 *Valutazione d'impatto sulla protezione dei dati* (art. 35).

Quando un determinato trattamento - tenuto conto dell'uso di nuove tecnologie e della sua natura, del contesto e delle finalità - può presentare un rischio elevato per i diritti e libertà delle persone fisiche, il Titolare deve effettuare una valutazione d'impatto dello stesso sulla protezione dei dati ("Valutazione d'Impatto"). L'autorità di controllo (ad esempio, il Garante) redige e rende pubblico un elenco delle tipologie di trattamenti che sono soggetti a Valutazione d'Impatto e di quelli che invece non vi sono soggetti, comunicandoli al Comitato europeo per la protezione dei dati. La Valutazione d'Impatto deve contenere:

1. una descrizione dei trattamenti previsti e delle finalità del trattamento;
2. una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
3. una valutazione riguardo i rischi per i diritti e le libertà degli interessati e le misure previste per affrontare i rischi.

La Valutazione d'Impatto è richiesta in particolare nei seguenti casi:

1. valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, sulla quale si fondano decisioni che hanno effetti giuridici o incidono su dette persone fisiche;
2. trattamento su larga scala di dati sensibili e giudiziari;
3. sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

È previsto che il Titolare riveda costantemente la Valutazione d'Impatto.

2.5 *Registri delle attività di trattamento* (art. 30).

Il Responsabile e il Titolare devono tenere un registro delle attività di trattamento in forma scritta, anche in formato elettronico, contenente gli elementi di cui all'art. 30 del Nuovo Regolamento. L'obbligo di tenuta dei suesposti registri non s'applica tuttavia in linea di principio alle imprese o organizzazioni con meno di 250 dipendenti (con limitate eccezioni).

3 ***Nuove figure soggettive*****.**

Il Nuovo Regolamento individua, come destinatari delle sue disposizioni, ulteriori figure rispetto al Codice Privacy.

3.1 *Responsabile della protezione dati ("RDP")* (art. 37).

Il Titolare o il Responsabile devono designare un RDP qualora:

1. il trattamento sia effettuato da un'autorità pubblica o da un organismo pubblico;
2. le attività principali del Titolare o del Responsabile consistano in trattamenti che, per loro natura, campo di applicazione e/o finalità richiedano il controllo regolare e sistematico degli interessati su larga scala;
3. il Titolare o il Responsabile trattino dati sensibili o giudiziari.

L'RDP deve essere designato in base alla sua professionalità e, in particolare, alla sua conoscenza della legislazione di protezione dei dati ed è tenuto, tra le altre cose a:

1. informare e consigliare il Titolare o il Responsabile in merito agli obblighi derivanti dal Nuovo Regolamento e da altre disposizioni dell'UE;
2. sorvegliare che il Nuovo Regolamento sia osservato;
3. fornire, se richiesto, un parere in merito alla Valutazione d'Impatto;
4. cooperare con l'autorità di controllo.

3.2 *Comitato europeo per la protezione dei dati* (art. 68).

E' un organismo dell'UE ed è dotato di personalità giuridica. E' composto dal responsabile di un'autorità di controllo di ciascuno Stato membro e dal Garante europeo della protezione dei dati, o dai rispettivi rappresentanti. Il Comitato, a titolo esemplificativo e non esaustivo, è tenuto a consigliare la Commissione europea in merito a qualsiasi questione relativa alla protezione dei dati personali dell'UE, comprese eventuali proposte di modifica del Nuovo Regolamento europeo, e pubblicare: linee guida, raccomandazioni e *best practices* al fine di promuovere l'applicazione coerente del Nuovo Regolamento.

4 *Diritti dell'interessato*.

4.1 *Diritto all'oblio* (art. 17).

Fino a oggi questo diritto era un prodotto dell'elaborazione giurisprudenziale, dalla quale era definito come il diritto dell'individuo ad essere "dimenticato" dalle banche dati, dai mezzi di informazione, o dai motori di ricerca. Il Nuovo Regolamento attua il riconoscimento su base legislativa del diritto all'oblio. In particolare, l'interessato ha diritto di chiedere che siano cancellati e non più sottoposti a trattamento i suoi dati personali:

1. che non siano più necessari per le finalità per le quali sono stati raccolti;
2. quando abbia ritirato il consenso o si sia opposto al trattamento o il trattamento dei dati personali non sia altrimenti conforme al Nuovo Regolamento.

La norma in oggetto, menziona tuttavia anche alcuni casi in cui il diritto all'oblio non sussiste; ad esempio, i casi in cui il trattamento sia necessario per l'esercizio del diritto alla libertà di espressione e di informazione o per l'adempimento di un obbligo legale.

4.2 *Portabilità dei dati* (art. 20).

L'interessato ha il diritto di:

1. ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati che lo riguardano forniti al Titolare;
2. trasmettere i propri dati (ad esempio, quelli relativi al proprio "profilo utente") da un Titolare (ad esempio un *social network*) ad un altro Titolare, senza impedimenti da parte di colui al quale sono stati forniti in precedenza.

5 *Armonizzazione.*

5.1 *One-stop-shop*.

Il Legislatore europeo si è posto il problema dell'ipotesi in cui un medesimo trattamento di dati sia operato dallo stesso Titolare in più di un paese dell'UE, coinvolgendo cittadini europei di Stati diversi. La scelta fatta attraverso il Nuovo Regolamento, al fine di perseguire un'uniformità non solo formale ma anche sostanziale, è stata quella di individuare un'unica autorità di controllo ("*Lead Authority*") identificata con riferimento al luogo dello stabilimento principale e/o unico del Titolare o del Responsabile, nel caso in cui questi ultimi effettuino trattamenti transfrontalieri. In questo modo, è possibile evitare che violazioni delle medesime norme del Nuovo Regolamento possano essere oggetto di ricorsi decisi diversamente a seconda dell'autorità di controllo di ciascun Paese. In ogni caso, il Nuovo Regolamento, al fine di non escludere le altre autorità di controllo eventualmente coinvolte, prevede una serie di norme volte a garantire cooperazione e assistenza reciproca, tenendo conto che la decisione della *Lead Authority* sarà vincolante anche per i trattamenti effettuati dal Titolare in altri Stati e utilizzando dati di cittadini di altri paesi dell'UE.

5.2 *Legislatore nazionale*.

Il Nuovo Regolamento (considerando 10 e 19) consente agli Stati membri di mantenere o introdurre disposizioni più specifiche per adattare le disposizioni del Nuovo Regolamento, soprattutto con riferimento al trattamento di dati sensibili. Nello specifico, a titolo esemplificativo e non esaustivo, gli Stati membri possono prevedere delle deroghe rispetto a quanto stabilito dal Regolamento europeo con riferimento ai trattamenti per scopi giornalistici, all'accesso del pubblico ai documenti ufficiali, al trattamento dei dati nell'ambito del rapporto di lavoro.

6 *Sanzioni.*

La nuova Direttiva Privacy ha provveduto inoltre ad uniformare ed inasprire il trattamento sanzionatorio in tutti gli Stati membri UE.

6.1 *Sanzioni amministrative* (art. 83).

Il Nuovo Regolamento prevede che l'autorità di controllo abbia il potere di imporre sanzioni amministrative per un importo pecuniario massimo predeterminato, tenendo conto, nella determinazione del quantum, di determinati indici, quali ad esempio: la natura, la gravità e la durata della violazione, il carattere doloso o colposo della stessa, le misure adottate dal Titolare. Le sanzioni variano a seconda del trasgressore, se si tratta di persona fisica o impresa.

6.2 *Altre sanzioni* (art. 84).

Il Nuovo Regolamento prevede che saranno gli Stati membri a stabilire le norme relative alle altre sanzioni assicurandone la proporzionalità e l'efficacia dissuasiva. Con riferimento all'Italia, non è da escludere il mantenimento dell'attuale quadro sanzionatorio per gli illeciti penali delineato dal Codice Privacy, con le necessarie modifiche in funzione de nuovo quadro di obblighi e requisiti previsti dal Nuovo Regolamento.

6.9. *Considerazioni finali*.

Non v'è dubbio che il Nuovo Regolamento, così come è formulato, ponga obblighi di *compliance* particolarmente stringenti nei confronti degli operatori che trattano dati personali. D'altro canto però non può non rilevarsi come, l'adozione di uno strumento normativo, quale, il Regolamento, comportante l'applicazione di un'unica disciplina in tutta l'UE, agevoli non poco l'esercizio del *business* di un'impresa che non si troverà più a dover fronteggiare quell'incertezza giuridica derivante da normative diverse per ogni Stato e i costi e la burocrazia ad esse connesse. Anche la particolare attenzione che viene data alle piccole e medie imprese, esonerandole da alcuni obblighi, deve essere guardata con nota di merito in quanto faciliterà notevolmente il loro ingresso e affermazione sul mercato.

CAPITOLO VII

Il Progetto ForensicStorage

7.1. Introduzione al progetto - 7.2. *ForensicStorage* – Custodia, gestione e analisi dei reperti informatici - 7.3. Obiettivi del progetto e quadro normativo - 7.4. Descrizione del servizio - 7.4.1. Consegna e accettazione dei supporti - 7.4.2. Copia, clonazione ed archiviazione delle copie - 7.4.3. Indicizzazione ed organizzazione dei contenuti - 7.4.4. Disponibilità dei contenuti via rete e/o supporto rimovibile - 7.4.5. Eventuale analisi dei contenuti con produzione esiti - 7.4.6. Cancellazione delle copie e distruzione/restituzione dei supporti originali al termine dell'*iter* processuale - 7.5. *ForensicBox – Hardware* per copia e clonazione forense - 7.6. Descrizione dei sistemi di autenticazione, di cifratura e delle procedure di consultazione e di accesso, sia fisico che logico, al materiale informatico conservato - 7.6.1. Premessa - 7.6.2. Strumenti di autenticazione e firma - 7.6.3. Descrizione delle procedure di accesso remoto - 7.6.4. Autenticazione e segretezza della comunicazione - 7.6.5. Copia dei supporti sequestrati: considerazioni tecniche - 7.6.6. Cifratura dei supporti acquisiti e loro consultazione - 7.7. Descrizione del sistema di erogazione delle macchine virtuali - 7.8. Strutture ed infrastrutture necessarie - 7.8.1. Costi ipotetici per infrastrutture, locali, risorse *hardware* e *software* - 7.9. Un modello economico sostenibile - 7.9.1. Ipotetici risultati economici attesi - 7.9.2. Ipotesi di listino servizi - 7.9.3. Ipotesi strategiche.

7.1. *Introduzione al progetto.*

La società contemporanea è sempre più dipendente dall'informazione in senso lato e dall'efficienza dei mezzi di comunicazione. Anche l'economia è ormai fortemente condizionata dalle nuove tecnologie informatiche e di telecomunicazione e la manipolazione della conoscenza diventa una risorsa strategica. L'evoluzione secondo queste direttrici è inevitabile ed inarrestabile, Tecnologie un tempo riservate agli addetti ai lavori sono oggi disponibili a chiunque ed anche necessarie da assimilare per essere accettati nel dinamico contesto sociale e lavorativo. Oggi non solo *computer*, *tablet*, *smartphone* sono connessi al *web*, ma anche automobili, giocattoli, elettrodomestici, perfino alcuni tipi di collari per animali domestici, si procede così sempre più spediti verso il c.d. "*Internet of Things*", si stima che già nel 2013 20 miliardi di dispositivi elettronici fossero connessi alla Rete, e che entro il 2020 saranno quasi raddoppiati, stimandone la crescita fino a 32 miliardi di dispositivi connessi.

Non vi è dubbio che siamo ancora agli albori di questa nuova epoca che ci vedrà sempre più connessi e forse anche sempre meno indipendenti. In questo quadro sempre più complesso, dunque, si presentano ovviamente grandi opportunità, ed importanti problematiche. Le distanze si annullano; le possibilità di collaborare, incontrare, lavorare e apprendere a distanza si moltiplicano; le informazioni diventano immediatamente fruibili da milioni di utenti in pochi istanti a costi contenuti. Per contro, emergono nuove criticità dovute all'enorme

mole di dati da gestire. Le analisi globali di *market intelligence* stimano una crescita annua del traffico Internet compresa fra il 50 e il 100%. Su un totale di 4,4 trilioni di GB dell'attuale universo digitale, si stima che il cosiddetto *digital footprint*[357] di ogni individuo sia quantificabile in svariate centinaia di GB[358] (fig. 1). La metà dei quali generata volontariamente e coscientemente tramite la quotidiana attività dell'utente, mentre l'altra metà - la cosiddetta *digital shadow*[359] - generata in maniera del tutto autonoma ed inconsapevole nell'*environment* tecnologico dato dall'insieme dei segnali della videosorveglianza, transazioni bancarie, tabulati telefonici, navigazione in Internet, interrogazioni dei motori di ricerca, ecc. Le ultime stime valutano l'ombra digitale di un individuo come superiore all'informazione digitale generata attivamente dallo stesso. Si parla quindi di una quantità di dati enorme se rapportata ai supporti comunemente a disposizione della maggior parte degli utenti appena pochi anni fa.

Fig. 1 - Stima della *digital footprint* di un utente medio, secondo il simulatore fornito dall'*International Data Corporation* (http://www.idc.com/), ammontante a oltre 320GB di dati digitali prodotti attivamente e involontariamente in tre mesi di normale attività.

Anche nel mondo digitale, come nel mondo reale, si rispecchiano luci e ombre. Di conseguenza vi è la necessità di un continuo aggiornamento ed affinamento delle tecniche investigative a sostegno della legalità e in contrasto al *cybercrime*[360]. Nasce quindi l'opportunità di organizzare e gestire la mole di informazioni in modo più funzionale ed efficiente possibile.

La caratteristica peculiare del *cybercrime* è quella di non conoscere confini, come abbiamo già avuto modo di vedere nei capitoli precedenti le ratifiche della Convenzione di Budapest, della Convenzione di Lanzarote e di numerose altre direttive europee introducendo nuove norme giuridiche nei singoli paesi, hanno

[357] *Digital Footprint*, "impronta digitale", l'insieme delle tracce di attività attiva e passiva lasciate dall'utente nell'universo digitale.

[358] Secondo il rapporto "*The Diverse and Exploding Digital Universe*" della International Data Corporation, https://www.emc.com/collateral/analyst-reports/idc-digital-universe-2014.pdf.

[359] *Digital Shadow*, "ombra digitale", l'insieme dei dati lasciati involontariamente dall'utente nel corso delle sue attività telematiche.

[360] L'attività criminale che utilizza il *computer* o la Rete, sia come strumento, sia come bersaglio.

permesso una progressiva omogeneizzazione delle normative degli Stati membri, ma molto risulta ancora da fare. In particolare tra le novità più importanti introdotte nel nostro ordinamento giuridico dal trattato di Budapest del 2001 ratificato con la Legge 18 marzo 2008 n. 48[361], vi sono una serie di misure finalizzate all'acquisizione e alla conservazione dei dati informatici, nonché alla loro preservazione da alterazioni. La dimensione in costante aumento dei dati da gestire e la loro eterogeneità di formati diventano fattori di criticità, rendendo fondamentale la realizzazione di infrastrutture adeguate capaci di trattare i dati secondo gli opportuni protocolli di sicurezza nel rispetto delle normative vigenti, e di interfacciarsi efficientemente alle banche dati esistenti.

7.2. *ForensicStorage – Custodia, gestione ed analisi dei reperti informatici*.

Gli strumenti informatici sono oggi presenti in ogni tipo di attività, professionale o ludica, privata o pubblica, a partire dalle comunicazioni telefoniche e dalla trasmissione di dati, fino alla sostituzione dei supporti che prima erano cartacei o analogici. La *dematerializzazione* delle informazioni, imposta anche da norme di legge[362], favorirà sempre più la diffusione - e la crescita – di sistemi e supporti informatici.

L'avvento della Rete Internet ha condizionato e rivoluzionato le modalità di comunicazione e scambio di informazioni tra milioni di persone e nella vita quotidiana la tecnologia ha portato alla crescita esponenziale dei dispositivi di memorizzazione delle informazioni digitali.

Come conseguenza di questa evoluzione, l'attività investigativa dovrà affrontare sempre più spesso il problema di *mettere in sicurezza, conservare ed analizzare supporti informatici*. La ricerca di prove o indizi sarà rivolta ad analizzare *computer*, *tablet*, video/fotocamere digitali, *smartphone* e tutti gli altri dispositivi che la tecnologia digitale ha reso disponibili, dispositivi connessi che *aumenteranno sempre più in termini di capacità e complessità*[363].

---

[361]Legge 18 marzo 2008 n. 48. Vedasi URL: http://www.camera.it/parlam/leggi/08048l.htm.

[362] Il processo mediante il quale gli atti riguardanti la formazione di documenti rilevanti sotto il profilo giuridico si realizzano senza altro supporto che quello informatico e/o telematico per l'acquisizione degli elementi costitutivi, l'elaborazione, l'archiviazione, il trasporto e la conservazione, con pieno valore tra le parti e verso i terzi. Per approfondimenti - anche normativi - si rimanda al sito *web* dell'Agenzia per l'Italia Digitale. URL: http://www.agid.gov.it/.

[363] Dai 10 MB di capacità di un comune disco rigido nel 1981 si è passati nel 2000 a 10 GB e, attualmente, a 1000 GB.

Com'è noto, tutti i dispositivi sopra citati possono contenere informazioni e dati fondamentali per ricostruire fatti e comportamenti di rilevanza giuridica. Si impone quindi l'esigenza di non disperdere questi dati, di garantirne l'integrità e renderne agevole la fruizione ai soggetti legittimati, nonché l'esigenza di custodire adeguatamente l'*hardware* posto sotto vincolo di sequestro anche per lunghi periodi di tempo.

Attualmente gli uffici pubblici preposti allo svolgimento di queste attività non sono attrezzati al fine di seguire una evoluzione così rapida. Infatti, nella maggior parte dei casi, non dispongono di strutture adeguate a gestire il nuovo trend, già a partire dagli spazi di custodia dei supporti di memorizzazione[364].

Al fine di evitare che l'acquisizione di indizi e prove preziose possa essere pregiudicata, ogni ufficio provinciale si troverebbe quindi costretto ad investire in maggiori spazi, in strumentazioni adeguate e in formazione del personale sulle nuove tecnologie, incorrendo però nel rischio di replicazione degli investimenti per ciascuna realtà operativa. In alternativa, potrebbe affidare la custodia e le eventuali analisi a soggetti terzi, rischiando però di avvalersi di realtà non adeguate con il rischio che vengano utilizzate procedure non rigorose. Entrambe le soluzioni appena descritte risulterebbero onerose, dispersive e potenzialmente poco adeguate.

Per garantire l'abbattimento dei costi, il rispetto di procedure rigorose e un servizio duraturo per la conservazione delle memorie di massa poste sotto sequestro, è necessario che il progetto venga posto in essere e sviluppato in partnership con un *DataCenter* di adeguate capacità strutturali e gestionali e di grande affidabilità, in grado di costruire al proprio interno una struttura specializzata capace di offrire, con protocolli aderenti agli attuali standard internazionali[365] ISO/IEC e normativi, ampie garanzie sia dal punto di vista tecnico, sia da quello procedurale e documentale, come ad esempio il consorzio CINECA[366].

---

[364] Ad esempio, nell'anno 2008 i settori della Polizia Postale di Bologna che operano a contrasto della pedopornografia e delle intrusioni informatiche hanno controllato supporti informatici (DVD, CD-ROM, floppy disk, *hard disk*) e *hardware* (*server*, pc, portatili) per oltre 20 TB.

[365] Standard ISO/IEC27037:2012, "linee guida per identificazione, raccolta, acquisizione e conservazioni delle prove digitali", ISO/IEC 27041:2015 "linee guida sulla garanzia di idoneità e adeguatezza dei metodi di investigazione", ISO/IEC 27042:2015 "linee guida per l'analisi e l'interpretazione di prove digitali" .

[366] CINECA è un Consorzio Interuniversitario senza scopo di lucro formato da 70 università italiane, 5 Enti di Ricerca Nazionali e il MIUR**.** Costituito nel 1969 (come Consorzio Interuniversitario per il Calcolo Automatico dell'Italia Nord Orientale), oggi CINECA è il

I vantaggi concreti di una soluzione come quella proposta tra gli altri sarebbero i seguenti:

1. l'accentramento delle risorse e delle tecnologie;
2. la costruzione di un protocollo metodologico secondo i più elevati standard qualitativi e di sicurezza;
3. la messa a disposizione degli investigatori delle copie delle memorie di massa originali in modalità remota;
4. la disponibilità di un sistema informatico di attribuzione delle autorizzazioni;
5. la possibilità di usufruire di una elevata capacità di elaborazione e di memorizzazione;
6. la verbalizzazione e documentazione rigorosa di tutte le attività svolte;
7. la possibilità di disporre nelle fasi dibattimentali di un comodo strumento di ricerca e di estrazione di materiale probatorio.

L'accentramento delle risorse e delle tecnologie porterebbe ovvi benefici economici e consentirebbe la standardizzazione di linee guida definite per ogni processo. Tutti i processi di copia, conservazione, autenticazione e verifica degli accessi aderirebbero agli standard di sicurezza internazionali utilizzando strumenti *software* ed *hardware* specificamente ingegnerizzati per garantire la sicurezza delle operazioni e l'ottimizzazione delle risorse e delle prestazioni. La cosiddetta *catena di custodia*[367], "*chain of custody*", potrebbe così essere progettata e mantenuta in modo controllato e rigoroso. In tal modo si assicurerebbero al meglio le garanzie previste dall'art. 55 c.p.p. riguardo alle funzioni della Polizia Giudiziaria, in particolare quelle di «*compiere gli atti necessari per assicurare le fonti di prova*» e procedere alla conservazione delle tracce pertinenti al reato. La metodologia scelta nella fase di conservazione rappresenta un punto cruciale, tanto più se riferita all'*iter* processuale, in cui si assiste ad un generalizzato e

maggiore centro di calcolo in Italia, uno dei più importanti a livello mondiale.

[367] *Chain of Custody*, cioè le procedure relative al sequestro, alla messa in sicurezza, al trasferimento, all'analisi e alla manipolazione degli elementi di prova fino alla conclusione dell'*iter* processuale. Le procedure devono essere documentate scrupolosamente e in ordine cronologico tramite strumenti di firma digitale e verbali, a garanzia che non siano state prodotte alterazioni ai dati e al fine di evitare accuse di manomissione o colpa.
Per approfondimenti: http://www.dm.unibo.it/~maioli/docs/fti_informatica_3009.doc e http://en.wikipedia.org/wiki/Chain_of_custody.

consistente aumento della durata media di tutte le fasi (indagini preliminari, udienza preliminare, giudizio di primo grado in tribunale e di quello di appello), che può anche superare i 1500 giorni. La realizzazione di un sistema automatico per la gestione e l'attribuzione degli incarichi per le perizie rigorosa e documentata e l'indicazione del periodo nel quale i dati saranno disponibili, comporterebbe indubbiamente grandi benefici in termini di risparmio economico e di tempo.

L'analisi da remoto delle memorie di massa consentirà di evitare i rischi legati al trasporto, alla conservazione e all'utilizzo di strumenti non idonei. Inoltre, la possibilità di accesso simultaneo ai medesimi dati per le analisi distribuite eviterà la replicazione dei supporti con conseguente ulteriore riduzione di tempo, di spazio e impegno economico. Un ulteriore importante vantaggio offerto dalla consultazione remota è dato dall'indisponibilità di una copia locale dei dati da parte dell'investigatore, che ha come conseguenza la riduzione dei rischi di fuoriuscita e divulgazione di informazioni riservate.

Disponendo di una rete a larga banda distribuita sul territorio si potrebbe consentire la consultazione - e in alcuni casi anche l'acquisizione - delle memorie di massa direttamente dalle sedi periferiche verso il centro di elaborazione presso il *DataCenter*.

I soggetti legittimati nell'ambito delle Procure della regione potranno così usufruire di collegamenti sicuri per accedere ai dati da remoto e, proprio nel caso particolare della Regione Emilia Romagna, disporre della rete a larga banda Lepida[368] (fig. 2), che potrebbe essere utilizzata per veicolare i dati in modo veloce e sicuro. Il punto di interscambio fra le diverse sottoreti di Lepida, collocato a Bologna, vede inoltre l'interconnessione fra Lepida ed il Sistema Pubblico di Connettività (SPC)[369].

[368] Rete a banda larga delle Pubbliche Amministrazioni dell'Emilia-Romagna, avviata secondo i Piani Telematici regionali e così chiamata in onore del console romano Marco Emilio Lepido. Lepida collega oggi fra loro la Regione, i 341 Comuni, le 9 Province, le 18 Comunità montane, Università, 160 Aziende sanitarie e ospedali, 378 scuole, per un totale di 90 mila dipendenti. Per ulteriori informazioni: http://www.lepida.it/.

[369] "l'insieme di infrastrutture tecnologiche e di regole tecniche per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione" Decreto Legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale).
Per informazioni: http://www.agid.gov.it/

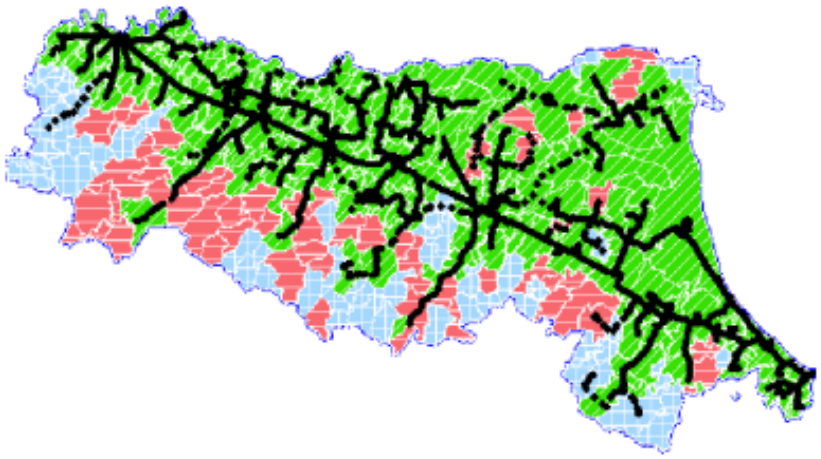


Fig. 2 - Copertura territoriale e stato di avanzamento della rete Lepida al 03/2009. Le linee continue rappresentano i centri già collegati, mentre le linee a tratteggio rappresentano i collegamenti in fase di completamento.

7.3. *Obiettivi del progetto e quadro normativo*.

La Legge n. 48 del 18 marzo 2008, nel capo terzo, ha modificato diversi articoli del *Codice di Procedura Penale* in materia di ricerca della prova, introducendo una serie di misure finalizzate all'acquisizione e alla conservazione dei dati informatici nonché alla loro preservazione da alterazioni. Nello specifico vengono innanzitutto estese e meglio definite le attività di acquisizione di dati da parte di ufficiali di P.G. in sede di ispezione o perquisizione disposte dal magistrato o eseguite d'iniziativa. Viene prevista la possibilità di acquisire dati presso fornitori di servizi informatici, telematici e di telecomunicazioni, eventualmente in copia se ritenuto opportuno dal magistrato. La necessità di assicurare misure tecniche adeguate per la conservazione dei dati viene prevista, in via generale, anche per gli ufficiali di P.G. che debbano compiere operazioni urgenti sulla scena del crimine. Essi devono impedire, oltre che l'alterazione, anche il semplice accesso ai dati stessi che, se possibile, devono essere immediatamente duplicati su idonei supporti. In tutti i casi la norma prescrive che per la duplicazione dovrà essere adottata una procedura che assicuri la conformità dei dati acquisiti a quelli originali, la loro immodificabilità e la ripetibilità degli accertamenti. Il quadro normativo approfonditamente trattato nei precedenti capitoli e qui sommariamente riportato postula una serie di interventi successivi (e se necessario anche contestuali) all'azione degli inquirenti per realizzare quegli obiettivi di ampia acquisizione e di messa in sicurezza dei dati informatici che il Legislatore si propone. Anzitutto è necessario assicurare la *custodia delle apparecchiature informatiche, l'integrità dei dati* contenuti e la loro *duplicazione*

in condizioni di assoluta sicurezza. Ma tutto ciò non è sufficiente. E' necessario anche consentire un agevole accesso ai dati ai soggetti che ne hanno la facoltà, in particolare ai difensori e agli inquirenti previa autorizzazione dell'A.G. competente. Lo scenario delineato offre quindi l'opportunità di costruire un progetto organico che dia una risposta complessiva a tutti i problemi posti dalla nuova normativa fornendo alle autorità competenti soluzioni sicure, economiche ed affidabili. Il progetto *ForensicStorage* mira quindi all'implementazione di un *servizio specialistico* sviluppato recependo le linee guida della normativa in vigore, prevedendo la custodia in ambiente protetto delle memorie di massa sottoposte a sequestro, la conservazione a lungo termine dei dati informatici in esse contenuti, la loro duplicazione e organizzazione in un sistema consultabile da remoto da parte dei soggetti legittimati. Come estensione del servizio è possibile offrire l'eventuale attività di analisi forense dei contenuti.

7.4. *Descrizione del servizio*.

Il servizio nel suo insieme si compone di fasi successive - non necessariamente dipendenti - di trattamento dei materiali sottoposti a sequestro, così schematizzate:

1. consegna e accettazione dei supporti di memorizzazione;
2. copia, clonazione e archiviazione a lungo termine delle copie;
3. indicizzazione ed organizzazione dei contenuti;
4. disponibilità dei contenuti via rete e/o su supporto rimovibile;
5. eventuale analisi dei contenuti con produzione di esiti;
6. cancellazione delle copie e distruzione/restituzione degli originali al termine dell'*iter* processuale.

Qualunque operazione svolta dal o presso il *DataCenter* verrà adeguatamente documentata con un sistema informativo costruito ad hoc. La documentazione prodotta resterà a disposizione dell'A.G., compresi i relativi verbali e le relazioni tecniche delle operazioni effettuate.

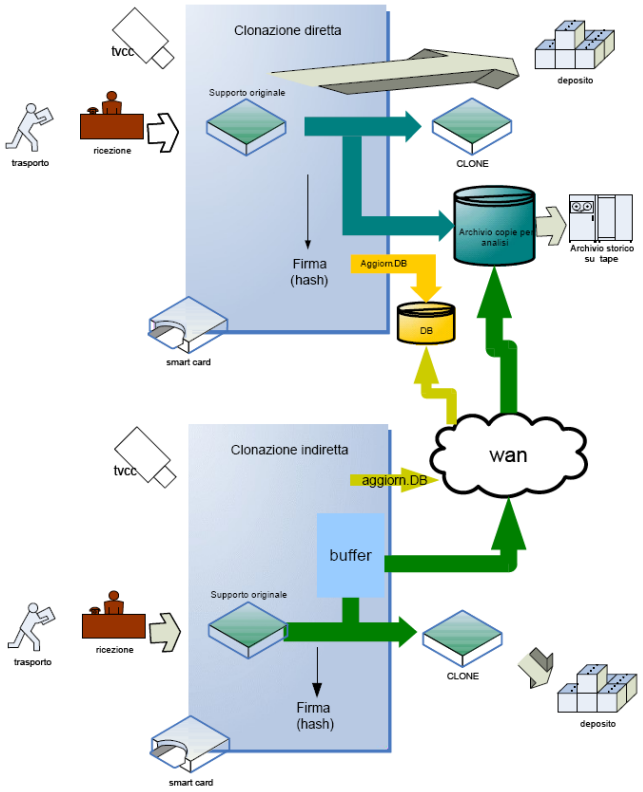


Fig. 3 - Schema del flusso di lavoro dalla consegna delle memorie di massa alla loro clonazione e archiviazione. La clonazione potrà essere effettuata presso il *DataCenter* (clonazione diretta), oppure sul campo dalle Forze dell'Ordine (clonazione indiretta).

Vengono di seguito descritte le singole fasi nel dettaglio.

7.4.1. *Consegna e accettazione dei supporti.*

Il ciclo di lavoro per la fase iniziale sarà il seguente: da un'attività condotta dalle Forze dell'Ordine[370] vengono sequestrate alcune memorie di massa (*computer*, *server*, dischi rigidi esterni, etc.); l'Autorità Giudiziaria, previa formalizzazione contrattuale con il *DataCenter* individuato, dispone un'analisi sommaria degli indizi digitali per ricevere soluzioni e suggerimenti al fine di estrarre indizi e prove utili alle indagini; dopodiché dispone la consegna degli stessi presso i locali adibiti alla custodia e allo svolgimento delle successive operazioni; la consegna degli indizi digitali avviene tramite sottoscrizione di un verbale che documenti i reperti e contestuale catalogazione con identificazione tramite etichette con codice a barre[371].

[370] Attività alla quale potrebbe partecipare anche personale tecnico esterno nella forma di ausiliari di polizia giudiziaria.

[371] Il codice a barre deve dare la possibilità di risalire al numero del procedimento penale, all'anno, alla provincia della Procura, al magistrato incaricato, all'ufficio operante e l'Ufficio di Polizia Giudiziaria che ha curato il sequestro, all'eventuale ausiliario di P.G. (uno o più tecnici temporaneamente "nominati" dal Procuratore) e infine all'avvocato e al perito di parte presenti.

Requisiti: per questa fase è necessario disporre di un ambiente adeguatamente attrezzato e dotato di controllo accessi.

7.4.2. *Copia, clonazione ed archiviazione delle copie*.

Generalmente, le necessità investigative non si limitano alla mera custodia dei reperti ma, visto che il fine è la ricerca delle cosiddette *evidences*, necessitano operazioni finalizzate alla fruizione e ricerca dei contenuti informativi. Queste operazioni, però, presuppongono che gli originali debbano essere preservati e che le operazioni avvengano sulle copie degli stessi al fine di rendere ripetibili gli accertamenti. Le copie *bit-stream* che sarà necessario produrre saranno tali per cui i dati digitali siano esattamente posizionati e strutturati come nelle memorie originarie. In questo percorso, le operazioni successive comportano quindi le seguenti fasi:

1. copia-immagine grezza delle memorie di massa, da depositare su *storage*;
2. eventuale clonazione delle stesse su memorie di massa vergini per la messa a disposizione delle parti;
3. archiviazione a lungo termine (*backup*).

Tali operazioni potranno essere effettuate sia presso il *DataCenter*, sia direttamente sul campo dalle Forze dell'Ordine, mediante l'utilizzo del dispositivo *hardware ForensicBox* che verrà descritto nel prossimo paragrafo o della piattaforma forense *ForensicWeb*, che verrà analizzata nel prossimo capitolo, entrambe queste tecnologie potranno eventualmente beneficiare dei canali trasmissivi a larga banda della rete Lepida per archiviare le immagini presso il *DataCenter* (fig. 3).

Requisiti: per questa fase è necessario disporre di idonei spazi, disporre di almeno due stazioni di lavoro[372] sotto alimentazione UPS per le operazioni di copia e clonazione. I *software* da utilizzare saranno prevalentemente di tipo *open source*. E' necessario disporre di connettività in fibra dall'ufficio verso il *DataCenter*, disponendo di *storage* NAS e *backup* su nastro dedicati, nell'ordine di svariati TB.

[372] L'*hardware* per la copia e/o clonazione, *ForensicBox*, sarà frutto di un progetto parallelo a partire da un prototipo già in avanzato stadio di sviluppo. Si veda il paragrafo 7.5.

7.4.3. *Indicizzazione ed organizzazione dei contenuti*.

I dati erogati potranno essere indicizzati e organizzati secondo vari criteri, ad esempio secondo la tipologia o il formato[373]. Come ulteriore servizio si potrà tentare il recupero dei *file* cancellati o non più allocati, secondo gli standard recepiti dai più noti *software* per l'analisi informatica forense[374]. Questi stessi *software* potranno inoltre essere erogati agli investigatori direttamente a livello di macchina virtuale.

Requisiti: per queste operazioni sarà necessario disporre di *software* sviluppati ad *hoc*, di *software open source* e di *software* commerciali, normalmente utilizzati per le indagini di informatica forense. E' anche ipotizzabile l'utilizzo di *appliance* Google[375] per creazione dell'indice e delle relazioni per una ricerca *full text filtrabile*.

7.4.4. *Disponibilità dei contenuti via rete e/o su supporto rimovibile*.

Dopo la preparazione dei dati di cui al punto precedente, su disposizione dell'A.G. i dati grezzi dovranno essere messi a disposizione degli aventi diritto.

L'erogazione dei contenuti può avvenire in due forme: su supporto trasportabile (*hard disk*, DVD, *Blu-Ray*, ecc.) via rete, tramite accesso remoto con un sistema protetto. Sulla base degli accordi precedentemente presi, l'A.G. potrà disporre che il *DataCenter* metta a disposizione degli inquirenti i dati attraverso un servizio di consultazione *online* e sicuro[376] per agevolare le ricerche degli indizi e delle prove attraverso accessi remoti. L'erogazione del servizio *online* comporterà la presenza di macchine virtuali con accesso controllato e cifratura del canale trasmissivo (fig. 4). Ogni macchina virtuale consentirà l'accesso in sola lettura alle copie-immagine delle memorie di massa e ai registri ipertestuali risultanti dall'indicizzazione dei contenuti, come descritto in precedenza. In tal modo, l'indagine del contenuto verrebbe favorita, pur nel rispetto assoluto dell'integrità e dell'inalterabilità dei dati originari.

---

[373] Documenti di testo, immagini, *file* video, fogli di calcolo, *file* cancellati-recuperati, etc.

[374] EnCase, FTK, Helix, etc…

[375] *Google Search Appliance* nella sua versione 7.6 esegue la scansione dei contenuti e crea un indice di milioni di documenti. Le sue funzioni di sicurezza garantiscono che un utente possa accedere solo alle informazioni per le quali dispone dei diritti di accesso. Per informazioni ulteriori: http://www.google.it/enterprise/gsa/.

[376] Grazie ad autenticazione tramite *smart card* dei soggetti precedentemente legittimati dall'Autorità Giudiziaria e grazie al salvataggio dei dati in forma compressa e crittografata. I certificati di attestazione dell'identità saranno emessi dall'Autorità di certificazione dopo una rigorosa verifica dell'identità del richiedente ed eventualmente controfirmati dall'A.G. in casi particolarmente delicati. I certificati per l'accesso alle informazioni saranno controfirmati dall'A.G. e saranno abilitati per periodi di validità e con scadenza ben definiti.

Requisiti: per la generazione di supporti trasportabili sono sufficienti normali attrezzature da ufficio. Per l'erogazione dei contenuti via rete è necessario disporre di almeno tre *server* con macchine virtuali, certificati e connettività di qualità. Si può ipotizzare una connettività sulla rete Lepida, la rete a banda larga delle Pubbliche amministrazioni dell'Emilia-Romagna, oppure una connettività a banda larga Fastweb. E' inoltre necessario disporre di un sistema di gestione delle *smart card* per gli utenti aventi diritto, interfacciato ad una *Directory*[377] per l'autenticazione previa disposizione da parte dell'A.G..

7.4.5. *Eventuale analisi dei contenuti con produzione di esiti.*

Su specifica disposizione da parte dell'A.G., il *DataCenter* potrebbe essere incaricato anche dell'analisi dei contenuti tramite ricerca di parole chiave, relazioni, esplorazione critica dei dati, ricerche di dati crittografati o nascosti.

Requisiti: vedi requisiti del punto precedente. E' anche ipotizzabile l'utilizzo dei sistemi di supercalcolo del *DataCenter* nei casi particolarmente complessi.

7.4.6. *Cancellazione delle copie e distruzione/restituzione dei supporti originali al termine dell'iter processuale.*

Una vola conclusa la fase di consultazione da parte di entrambe le parti, si redigerà il verbale di cancellazione delle copie immagine e verrà conservata solamente la copia di *backup* per eventuali successivi utilizzi, fra cui la possibilità di una rigenerazione dell'immagine grezza o ricostruzione della memoria di massa. Dopo un periodo di tempo dell'ordine di quattro o cinque anni o comunque al termine dell'*iter* processuale, le copie di *backup* e le memorie di massa potranno essere restituite o distrutte, come indicato dall'A.G. e nel rispetto dell'attuale normativa sulla *data retention*. Le operazioni verranno documentate con apposito verbale inviato in copia alle parti interessate.

7.5. *ForensicBox - Hardware per copia e clonazione forense.*

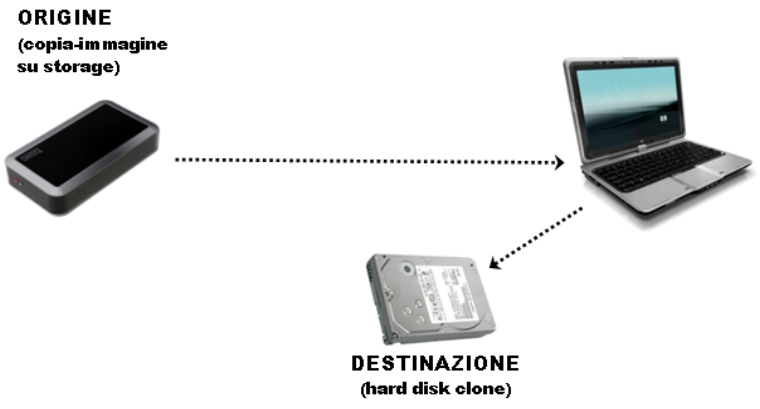
Al precedente paragrafo 7.4.2 si è accennato alle operazioni di copia e di clonazione delle memorie di massa.

La procedura fino ad oggi adottata richiede la disponibilità di un *computer* con apposito *software* forense a cui vengono collegati l'*hard disk* originale e

[377] Il concetto di '*Directory*' si basa sull'insieme delle risorse a cui possono accedere gli utenti e ai servizi attivi o attivabili fra quegli utenti e quelle risorse. Risorse e utenti fanno così parte di una sorta di mondo virtuale, chiamato Dominio, in cui vale una regolamentazione dell'accesso alle risorse da parte degli utenti, basata su un sistema di autenticazione.

l'*hard disk* di destinazione che ospiterà la copia *raw*[378] del primo, ottenuta copiando settore per settore (fig. 4a). La memoria di massa originale viene salvaguardata dall'alterazione ("scrittura") grazie all'interposizione di un cosiddetto blocco *hardware* (*write-block*). Una volta completata questa copia, che normalmente richiede svariate ore, è necessario riporre l'*hard disk* originale e, nel caso in cui fosse stabilita la necessità da parte dell'A.G., procedere alla generazione del disco clone a partire dalla copia *raw* precedentemente ottenuta (fig. 4b), tramite un'operazione di ripristino (*restore*). Anche questo secondo passaggio richiede tempi lunghi, in cui sbalzi di corrente, errori *hardware* e fattori anche esterni potrebbero rendere necessaria la ripetizione delle operazioni dall'inizio. I risultati dei processi di copia vengono infine verificati *bit* per *bit*, al fine di certificare la corrispondenza rispetto agli originali.

4a.



4b.

Fig. 4 - Schema del procedimento in due fasi comunemente usato per la copia di una memoria di massa, ad esempio un *hard disk*. 5a: copia-immagine; 5b: generazione di un disco clone.

[378] Per copia "*raw*" (= grezza) di una memoria di massa si intende la copia-immagine effettuata settore per settore e tale per cui l'impronta digitale (*hash*) calcolata sulla copia sia esattamente identica a quella calcolata sulla memoria originale.

E' in avanzata fase di progettazione un dispositivo denominato *ForensicBox*, in grado di semplificare e regolamentare secondo un rigido protocollo le operazioni fondamentali da effettuarsi a partire dalle memorie di massa originali, in modo che le copie e i cloni possano essere generati facilmente, in tempi ottimali e con certificazione di conformità delle copie rispetto agli originali.

I vantaggi concreti del *ForensicBox* (fig. 5) rispetto alle soluzioni tradizionali saranno i seguenti:

1. non obbliga la disponibilità di un *computer*, che dovrebbe essere appositamente configurato;
2. è esso stesso un *minicomputer* senza parti in movimento;
3. assolve nativamente alle funzioni di blocco in scrittura (*write-block*);
4. esegue automaticamente l'*hash* (impronta digitale) del supporto acquisito;
5. effettua la copia/clonazione su canali paralleli, ad es. su uno *storage* (anche via rete) e su un disco esterno;
6. produce un report XML corredato di marca temporale (*timestamp*);
7. offre un'interfaccia intuitiva che non richiede *input* da riga di comando;
8. è studiato per postazioni fisse o mobili.

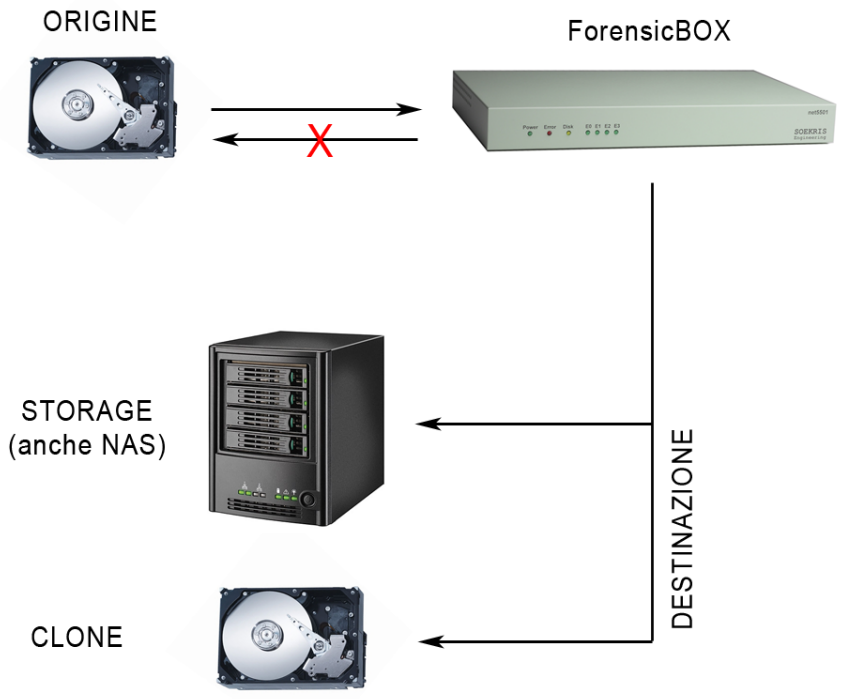


Fig. 5 - Il *ForensicBox* è in grado di produrre un clone e una copia-immagine operando in *multitasking*.

La tecnologia prescelta per la realizzazione di questo dispositivo *hardware* di tipo *embedded*, consistente nell'avere un vero e proprio *mini computer* integrato in una scheda, è la tecnologia Raspberry di terza generazione[379].

Il Raspberry Pi 3, è stato introdotto sul mercato nel febbraio 2016, sostituendo la precedente versione e offrendo performance superiori a parità di dimensioni e consumi. Nello specifico il Raspberry Pi 3, presenta le seguenti caratteristiche: Processore 1.2GHz 64-bit quad-core ARMv8, 1GB RAM, 4 VideoCore IV 3D graphics core, 4 USB ports, Micro SD card slot, ampie possibilità di connessione mediante 802.11n Wireless LAN, Bluetooth 4.1.

Lo sviluppo successivo del *ForensicBox* prevede una specifica customizzazione del *software* da utilizzare con il Raspberry Pi3 in modo da integrarne l'operatività anche con la piattaforma forense *ForensicWeb*.

Il *ForensicBox* sarà in grado di generare l'immagine grezza della memoria di massa secondo i più diffusi formati di *file* forensi[380], possibilmente di tipo *open source* e capaci di interfacciarsi con lo standard XML, come ad esempio AFF, FTK, *open*EnCase.

In realtà, il formato leader del mercato per l'analisi forense è attualmente EnCase della Guidance Software[381]. Per via della diffusione di questo formato proprietario sarò opportuno generare immagini anche in questo formato, anche se sarebbe preferibile contribuire con il presente progetto alla standardizzazione dei formati di conservazione delle evidenze digitali, adottando un formato *open source*. Il formato AFF[382] può essere ritenuto molto valido per una valutazione approfondita, dal momento che, secondo alcune sperimentazioni recenti[383], ha garantito:

1. l'ottimizzazione dei tempi di processo delle memorie di massa;
2. il più efficiente rapporto di compressione;
3. la possibilità di lettura dei *file* senza la necessità di decomprimere l'immagine.

Per quanto riguarda invece lo scambio delle informazioni digitali memorizzate, esiste già un rigoroso schema XML denominato EDRM[384] che può certamente rappresentare un'importante base di partenza.

[379] Per approfondimenti: https://www.raspberrypi.org/products/raspberry-pi-3-model-b/

[380] Per approfondimenti: http://www.forensicswiki.org/wiki/Forensic_file_formats.

[381] Per approfondimenti: http://www.guidancesoftware.com.

[382] *Advanced Forensic Format*, http://www.ijdc.net/index.php/ijdc/article/viewFile/217/286

[383] CIRSFID, http://www.dm.unibo.it/~maioli/docs/wisp2006.pdf

[384] *Electronic Discovery Reference Model*: http://www.edrm.net/.

7.6. *Descrizione dei sistemi di autenticazione, di cifratura e delle procedure di consultazione e di accesso, sia fisico che logico, al materiale informatico conservato*.

7.6.1. *Premessa*.

La normativa vigente sulla Firma Digitale[385] e la correlata tecnologia delle *smart card* consentono di realizzare procedure che operano con livelli di sicurezza intrinsecamente superiori a quelli normalmente raggiungibili con *username* e *password*. Le soluzioni realizzabili con tali tecnologie consentono, inoltre, di *informatizzare completamente tutti i procedimenti autorizzativi e di accesso a determinate risorse*, condizionando l'esecuzione di tutte le operazioni previste da *workflow* anche complessi alla sottoscrizione con Firma Digitale di documenti XML[386] che avranno pieno valore legale ed opponibilità verso terzi riguardo alle disposizioni in essi contenute, sostituendo, di fatto, le firme autografe su autorizzazioni e registri cartacei. Altra caratteristica potenzialmente utile deriva dal fatto che la normativa sulla Conservazione documentale[387] definisce procedure di conservazione dei documenti informatici che potrebbero essere adeguate a conservare con validità legale anche le copie *raw* dei supporti informatici sottoposti a sequestro, a condizione di prevedere un adeguamento delle regole tecniche esistenti (linee guida, circolari, etc.) da parte dei ministeri interessati.

In sintesi si propone di predisporre una soluzione che aderisca naturalmente alla normativa esistente, riducendo al minimo le eccezioni richieste per il caso specifico.

---

[385] Codice dell'Amministrazione digitale (D.Lgs. 7 marzo 2005, n. 82)

Decreto legislativo 4 aprile 2006, n. 159 "Disposizioni integrative e DPCM del 13.01.2004

Deliberazione CNIPA n. 4 del 17 febbraio 2005

Deliberazione CNIPA n. 34 del 18 maggio 2006 con relativo allegato

Circolare CNIPA n. 48 del 6 settembre 2005

[386] Metalinguaggio utilizzato per descrivere documenti strutturati adottato anche dai modern applicativi di *office automation* (MS Office, *Open Office*, etc.).

[387] Codice dell'Amministrazione digitale (D.Lgs. 7 marzo 2005, n. 82)

Decreto legislativo 4 aprile 2006, n. 159 "Disposizioni integrative e correttive al Decreto legislativo 7 marzo 2005, n. 82"

Deliberazione CNIPA 19 febbraio 2004, n. 11

Codice dei beni culturali e del paesaggio (D.Lgs. 22 gennaio 2004, n. 42)

7.6.2. *Strumenti di autenticazione e firma*.

Prerequisito fondamentale è che tutti gli utenti del sistema siano dotati di *firma digitale*, ovvero abbiano ottenuto una *smart card* di Firma Digitale da uno dei certificatori accreditati iscritti all'elenco pubblico disponibile presso il CNIPA. Tali *smart card* dovrebbero essere dotate anche di un *certificato di autenticazione* (identificazione) conforme allo standard CNS (Carta Nazionale dei Servizi) e, convenientemente, di un *certificato di cifratura*.

La scelta della *smart card* con certificati di Firma Digitale e autenticazione CNS è motivata dalle regole di rilascio che impongono per legge l'identificazione frontale del richiedente e la verifica del suo Codice Fiscale da parte dei certificatori accreditati. Tale riconoscimento frontale, è equiparabile a quello eseguito dal funzionario dell'anagrafe in occasione del rilascio del documento di identità. L'affidabilità di questa modalità di rilascio della *smart card* consente di ottenere una identificazione certa del titolare sia dal protocollo di comunicazione TLS/SSL che utilizza il certificato di autenticazione, sia dalle Firme Digitali apposte sui documenti con il certificato di Firma.

Analogamente, nel caso degli Avvocati si potrebbe considerare l'uso di certificati emessi dall'ente certificatore del loro Ordine professionale.

7.6.3. *Descrizione delle procedure di accesso remoto*.

Le copie dei supporti sottoposti a sequestro verrebbero rese disponibili per l'analisi con strumenti utilizzabili con applicativi specifici come, ad esempio, il *desktop* remoto di un *server* di macchine virtuali (fig. 6), oppure mediante *browser web*, come la piattaforma forense *ForensicWeb* che sarà oggetto di approfondimento nel prossimo capitolo.

Tale modalità di accesso ai supporti presenta stringenti requisiti di sicurezza ed il rispetto assoluto di una ancora più stringente normativa sulle autorizzazioni necessarie per poter consultare i supporti sequestrati.

Come già anticipato, la normativa vigente sulla Firma Digitale mette a disposizione gli strumenti per operare con un ottimo livello di sicurezza sia sul fronte dell'identificazione e della segretezza della comunicazione con il sistema, sia su quello della realizzazione di meccanismi di attribuzione delle politiche di accesso ai soggetti interessati.

L’aspetto prettamente operativo della concessione di una autorizzazione, tipicamente eseguita con apposita procedura *web*, *può essere integrato con la sottoscrizione con Firma Digitale di un documento da parte dei titolari dei procedimenti dell’Autorità Giudiziaria*. Tale documento può essere formato in modo tale da soddisfare i requisiti di visualizzazione al titolare, richiesti per la Firma Digitale, mantenendo la capacità del sistema di eseguire automaticamente ed immediatamente le istruzioni contenute nel documento stesso.

L’esecuzione delle operazioni in tal modo disposte sarebbe condizionata dalla corretta verifica della Firma Digitale e produrrebbe un documento legalmente valido ed opponibile a terzi corredato delle firme di tutti gli attori coinvolti. Sarebbe in tal modo riproducibile con *workflow* informatico l’attuale procedimento cartaceo: le singole autorizzazioni concesse dall’A.G. avrebbero il conforto di un documento informatico legalmente valido, proprio come nell’universo analogico.

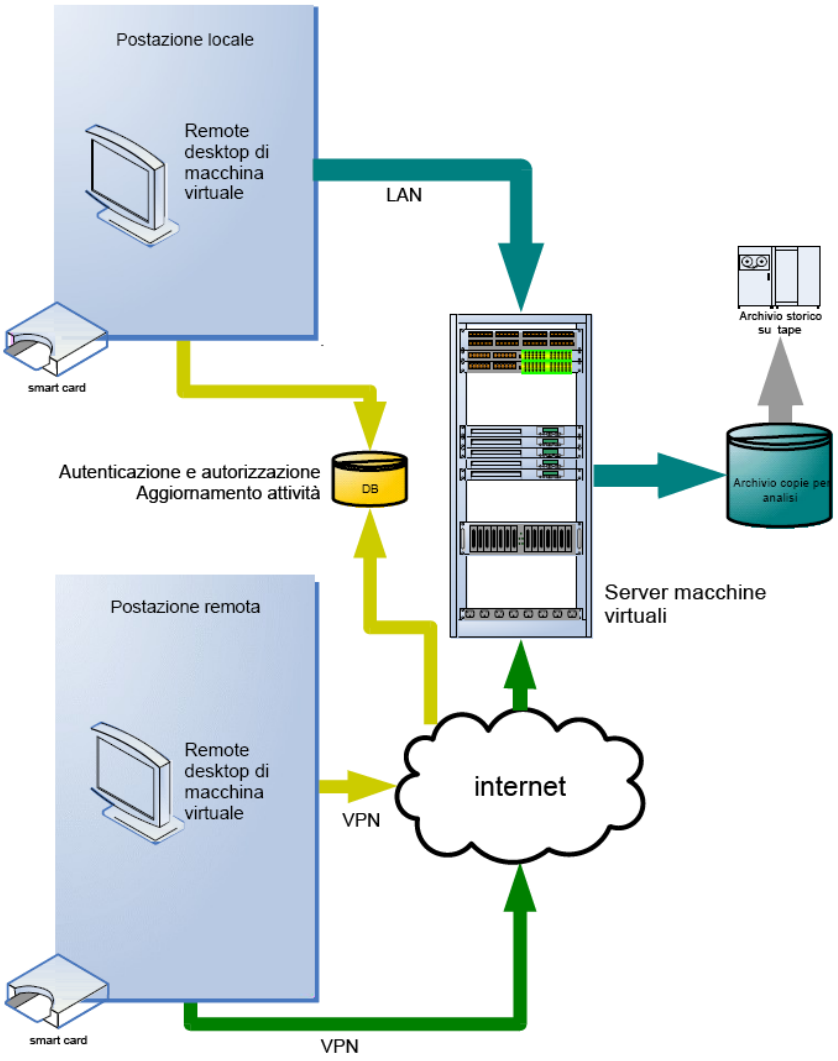


Fig. 6 - Schema del sistema di archiviazione delle copie presso il *DataCenter* e della loro consultazione da remoto, previa autorizzazione e autenticazione.

I soggetti autorizzati ad accedere ai supporti, e/o ad analizzarli con gli strumenti messi a disposizione sulle macchine virtuali, o la piattaforma forense ForensicWeb, sarebbero identificati con certezza attraverso il Codice Fiscale decodificato dal certificato di autenticazione presente sulla loro *smart card* di Firma Digitale.

Grazie alla stessa *smart card* verrà sottoscritto il registro/giornale degli accessi al sistema, producendo anche in questo caso documentazione legalmente valida e più convincente rispetto alle righe di un *file* di registro del sistema.

7.6.4. *Autenticazione e segretezza della comunicazione*.

Essendo tutti gli attori dotati di *smart card* con certificati di autenticazione e Firma Digitale, l'identificazione dell'utente avverrebbe su *server web* sicuri configurati per l'uso esclusivo del protocollo TLS/SSL con autenticazione degli utenti obbligatoria[388] e limitata all'uso delle *smart card* emesse dai certificatori accreditati CNIPA. L'autorizzazione all'accesso al servizio ed all'utilizzo delle singole risorse messe a disposizione sul sistema, sarebbe gestita grazie alla banca dati degli utenti contenente i necessari dati anagrafici, in particolare il Codice Fiscale, il certificato di autenticazione approvato dall'A.G. per l'accesso di ogni singolo soggetto e le esplicite autorizzazioni rilasciate dall'A.G. agli utenti del sistema. L'utilizzo della X.509 *Client Authentication* con certificati CNS fornisce una identificazione affidabile degli utenti: dal punto di vista tecnologico, perché il protocollo, gli algoritmi e le caratteristiche di sicurezza delle *smart card* sono estremamente più forti di qualsiasi *username* e *password*; dal punto di vista legale, perché il riconoscimento frontale e la forte responsabilità sulla custodia, attribuita dalla normativa al titolare della *smart card* di Firma Digitale, rendono l'uso dello strumento paragonabile a quello di un documento di identità.

Il *server web* sarebbe, ovviamente, dotato di un certificato TLS/SSL emesso da *certification authority* riconosciute dai *browser web* per consentire agli utenti di verificare l'autenticità del *server* stesso[389]. Verificata l'autenticità del *server* e l'identità dell'utente con gli strumenti del protocollo TLS/SSL, la comunicazione avverrebbe su canale cifrato al sicuro da occhi indiscreti ed attacchi di tipo "*man-*

[388] X.509 TLS *Client Authentication*.

[389] X.509 *Server Authentication*.

in-the-middle"[390], oggi purtroppo molto frequenti.

E' da valutare la possibilità di utilizzare la X.509 *Client Authentication* anche per l'accesso alle macchine virtuali. Alternativamente, si può prevedere uno schema che a fronte dell'accesso con *smart card* dell'utente autorizzato ad un'apposita applicazione *web*, il titolare richiede l'assegnazione di un'utenza ed una *password* di validità temporalmente limitata, mediante le quali accedere alla macchina virtuale. Anche la richiesta di assegnazione di *username* e *password* temporalmente limitati verrebbe formalizzata con apposito documento sottoscritto con Firma Digitale dal titolare, attivando l'operazione da un lato e restando disponibile come documentazione legalmente valida della richiesta dall'altro. In questo caso il protocollo di accesso effettivo sarebbe scelto fra quelli disponibili nella soluzione adottata per realizzare il *server* di macchine virtuali.

7.6.5. *Copia dei supporti sequestrati: considerazioni tecniche*.

Le copie effettuate dovranno essere certificate relativamente a:

1. conformità all'originale;
2. immodificabilità nel tempo;
3. certificazione delle procedure adottate dal personale autorizzato.

Disponendo di un accesso internet, anche mobile come UMTS o GPRS, l'incaricato dell'operazione può firmare digitalmente il *file* acquisito ed utilizzare il servizio di *marcatura temporale* dei certificatori accreditati CNIPA[391]. In tal modo, si renderebbe opponibile a terzi l'esistenza del *file* sottoposto alla data e ora dell'operazione ed il fatto che lo stesso era stato firmato con la *smart card* dell'incaricato, garantendo l'identità dell'operatore e la non modificabilità dei dati.

L'applicazione a disposizione degli incaricati produce così un documento nel quale si dichiarano le operazioni eseguite e si include sia l'impronta digitale del *file* generato, sia la marca temporale rilasciata dal certificatore. Il documento viene quindi firmato digitalmente dall'incaricato e sottoposto esso stesso a marcatura temporale. Il documento così formato potrebbe essere trasferito

[390] L'attacco del "*man in the middle*" (uomo in mezzo) è un attacco nel quale l'attaccante è in grado di leggere messaggi fra due parti vittime senza che nessuna delle due capisca che il collegamento è stato compromesso (Fonte Wikipedia).

[391] Sia la firma digitale, sia la marcatura temporale del *file* acquisito potranno essere prodotte in modalità *detached* (separata), in modo da non alterare il formato del *file* acquisito, che rimarrebbe così direttamente utilizzabile dagli applicativi *software* messi a disposizione per le analisi del contenuto.

telematicamente al sistema *web* di gestione consentendo di eseguire immediatamente tutte le operazioni preliminari alla consultazione dei supporti da parte degli aventi diritto non appena siano fisicamente disponibili al sistema.

7.6.6. *Cifratura dei supporti acquisiti e loro consultazione*.

La cifratura delle copie delle memorie di massa sequestrate andrebbe effettuata con *algoritmi crittografici simmetrici*, come ad esempio AES-256, e la chiave utilizzata[392] messa a disposizione dell'A.G. responsabile del procedimento.

In considerazione del fatto che le operazioni di accesso avverranno attraverso un *server* cui gli utenti accederanno remotamente, è indispensabile che il sistema stesso sia in grado di decifrare il materiale conservato per renderlo disponibile agli autorizzati. Questa necessità orienta verso la cifratura della chiave simmetrica utilizzata per i dati utilizzando la chiave pubblica di cifratura del titolare del procedimento. Quando il titolare del procedimento intende autorizzare un soggetto registrato sul sistema alla consultazione di uno specifico supporto, lo potrà fare tramite un modulo di autorizzazione via *web*. Il documento di autorizzazione risultante viene archiviato ai fini della procedura ed il sistema riceve una copia cifrata della chiave simmetrica utilizzata per quella data memoria, unitamente agli estremi (Codice Fiscale) degli autorizzati all'accesso.

Quando i soggetti autorizzati si identificano utilizzando la propria *smart card*, firmano digitalmente un documento XML che certifica data e ora della loro richiesta e, conseguentemente, ottengono dal sistema la decifratura della memoria di massa e la sua accessibilità secondo le modalità previste (consultazione remota, analisi, etc.). Al termine dell'operazione, anch'essa certificabile con documento sottoscritto digitalmente, e comunque dopo un tempo prefissato all'atto dell'autorizzazione, il sistema provvede alla rimozione dell'accesso alla risorsa.

[392] La chiave di cifratura simmetrica dovrebbe essere convenientemente archiviata su un *server* di *Key-Recovery*, per evitare di perdere l'accesso ai dati cifrati. Il *server* di *Key-Recovery* potrebbe utilizzare schemi del tipo M of N (M < N) secondo cui le informazioni necessarie a ricostruire la chiave sarebbero suddivise fra N soggetti e per ricostruirla sia sufficiente l'intervento di soli N di questi. Tale soluzione garantisce che nessuno possa autonomamente ricostruire la chiave e che la stessa sia recuperabile, anche se alcuni dei soggetti non fossero disponibili o avessero perduto le proprie credenziali.

7.7. *Descrizione del sistema di erogazione delle macchine virtuali.*

Una moderna ed efficiente organizzazione dei sistemi per la fruizione dei contenuti digitali può essere realizzata attraverso l'utilizzo di un insieme di macchine (o "*desktop*") virtuali, predisposte con applicativi idonei all'analisi forense. La proposta della virtualizzazione è operata sulla base dei numerosi punti forza che la contraddistinguono, fra cui il minore consumo energetico, l'utilizzo ottimale delle risorse *hardware*, la spiccata scalabilità, etc.. A tali *Virtual Machine* (VM) saranno state preventivamente associate in modo automatico le risorse (le immagini delle memorie di massa) oggetto dell'analisi. Inoltre, sarà messo a disposizione del personale autorizzato all'analisi un efficiente sistema di ricerca testuale dei contenuti e un indice ipertestuale dei contenuti, precedentemente organizzati per categorie (documenti di testo, video, immagini, fogli elettronici, basi di dati, ecc.). L'utente avrà così a disposizione un'interfaccia *web* tramite la quale, previa *strong authentication*, avrà l'opportunità di scegliere uno fra i procedimenti a egli associati, con facoltà di utilizzare la VM predisposta per l'analisi del materiale correlato. Alla base dell'infrastruttura di gestione e attribuzione delle macchine virtuali agli utenti risiede un servizio di *Directory*, allo scopo di garantire uniformità d'accesso e il rispetto dei vincoli autorizzativi.

Di seguito si sintetizzano i vari elementi che comporrebbero il sistema (fig. 7):

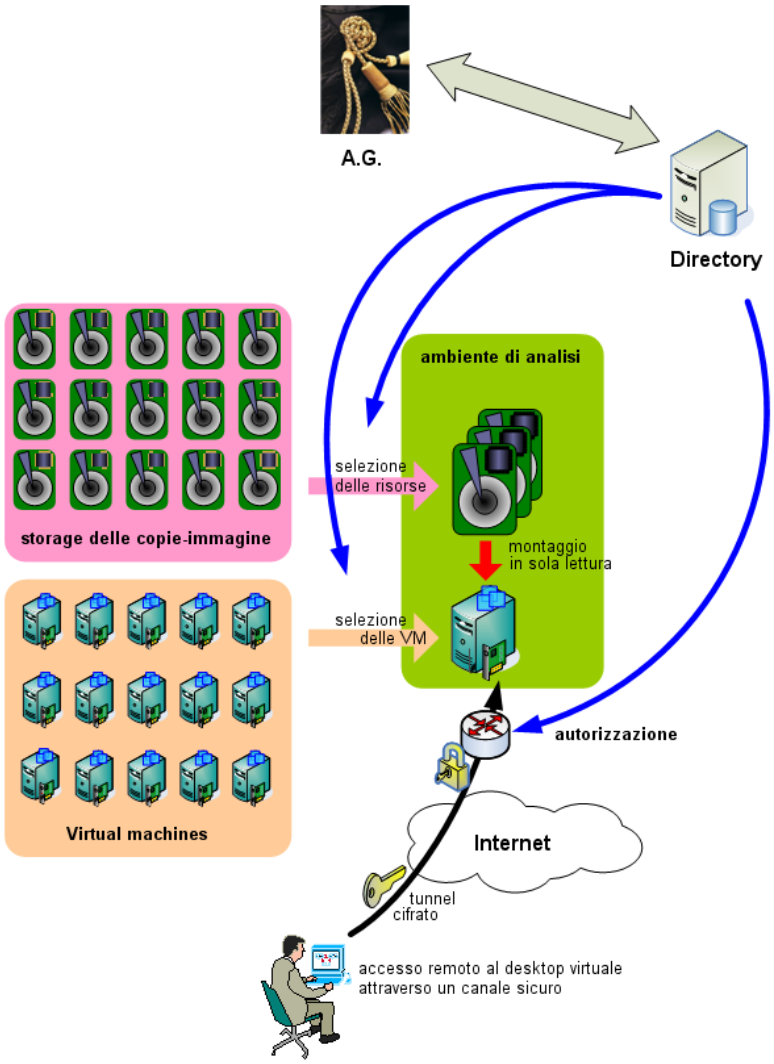


Fig. 7 - Concessione delle autorizzazioni e assegnazione delle risorse e delle macchine virtuali da parte dell'A.G.

RISORSE
infrastruttura di gestione delle macchine virtuali;
database relazionale (DBMS);
storage primario delle risorse su *hard disk*;
storage di *backup* delle risorse su nastro.

PROCEDURE
creazione e/o selezione delle macchine virtuali per l'analisi;
associazione delle risorse alle macchine virtuali;
accettazione dell'accesso da parte dell'analista con procedura di *strong authentication*;
scelta della macchina virtuale assegnata;
analisi ed individuazione dei vari elementi utili al procedimento;
creazione dell'elenco degli elementi utili;
chiusura della sessione di analisi.

SERVIZI
generazione e gestione delle autorizzazioni tramite "*Directory*";
gestione dei criteri di accesso ai sistemi e alle risorse;
gestione dei registri (*log*) delle attività;
gestione degli elenchi degli elementi utili al procedimento;
backup.

7.8. *Strutture ed infrastrutture necessarie*.

Per il servizio a regime è fondamentale disporre di un locale adibito a magazzino, per il servizio di custodia materiale delle memorie di massa, e di un locale adibito ad ufficio, quale ambiente di accettazione, acquisizione, archiviazione, analisi, produzione di esiti e consultazione.

Il locale adibito ad ufficio sarà predisposto con i seguenti impianti: impianto elettrico, isolato, protetto e alimentato sotto UPS; connettività Internet con *switch* a 4 porte e una rete in fibra verso lo *storage* con *switch* a 4 porte; impianto CCTV; controllo accessi tramite *badge*. Le postazioni di lavoro dovranno essere idealmente quattro, di tipo standard (2 *notebook* e 2 pc *desktop*). La dotazione dell'ufficio comprenderà a regime 2 *ForensicBox*, alcuni strumenti ad uso forense (blocchi *hardware*, cavi e box esterni), un UPS dedicato per 2 *computer*, un sistema per la generazione di *smart card*, un multi-masterizzatore CD-ROM/DVD/BLU-RAY, alcuni *hard disk* esterni/interni, una stampante/fax, una macchina fotografica digitale, una videocamera, un treppiede.

Sarà necessario disporre inoltre del seguente *software*: sistemi operativi e *software* di *office automation*; *software* ad uso forense (*open source* e commerciale, come ad es. EnCase e FTK); alcune licenze WM-Ware/XEN; un sistema di catalogazione interfacciato a *smart card* e a *database*; un sistema di produzione codici a barre o etichette di archiviazione per archiviazione originali.

Per quanto riguarda l'infrastruttura, si prevede un ambiente *DataCenter*, costituito da almeno 4 nodi e da un NAS di adeguate dimensioni, almeno 100TB.

7.8.1. *Costi per locali, risorse hardware e software, infrastruttura*.

a) FASE DI SVILUPPO E SPERIMENTAZIONE

	Qtà	Costo €
PREDISPOSIZIONE UFFICIO		
Posizione da definire; dimensioni 10-15mq; accesso con *badge* e porta con elettrocalamita	1	2.000
Arredi: scrivanie attrezzate, sedie, armadi ignifughi, cassettiere, cancelleria	1	-
Cablaggi: prese multiple da laboratorio con alimentazione sotto UPS; rete consultazione Internet; rete in fibra punto/punto con *storage*	1	2.000
PREDISPOSIZIONE MAGAZZINO		
Posizione in sala impianti; spazio di 2x3m racchiuso in gabbia con accesso con *badge*	1	5.000
Arredi: scaffalature; contenitori per *hard disk*	1	-

RISORSE HARDWARE		
Cablaggi: solo illuminazione interna	1	500
Personal Computer con sistema operativo, *monitor* e periferiche	2	2.000
Notebook con sistema operativo e periferiche	1	1.000
Cavi e box esterni per diverse interfacce	vari	1.000
HW per la generazione di *smart card* (*hardware* + *software*) per sperimentazione	1	1.000
Hard disk esterni/interni di riserva	2	200
Stampante/fax	1	400
RISORSE SOFTWARE		
Stampante codici a barre + lettore	1	500
Switch 8 porte G*bit*	1	200
Licenza Windows 10 per macchine virtuali	5	1.500
Licenza Mac OS X 10.11 El Capitan per macchine virtuali	1	100
Software forense (1 licenza EnCase, 1 licenza FTK, applicativi vari)	5	6.000
SISTEMI		
Licenze WM-Ware/XEN	5	5.000
Sistema di catalogazione interfacciato a *smart card* e a *database*	1	-
SW di produzione codici a barre o etichette di archiviazione	1	500
Rack con 4 *server* e *storage* locale	1	15.000
Gateway d'accesso Citrix dedicato	1	2.500
Storage su disco	100TB	3.000
Backup su nastro	100TB	3.000
TOTALE:		52.400

b) SERVIZIO A REGIME

	Qtà	**Costo €**
IMPIANTI		
Videosorveglianza interna ufficio	1	1.000
RISORSE HARDWARE		
***ForensicBox* ***	2	XXXX
UPS per 2 *computer*	1	400
Multi-masterizzatori CD-ROM, DVD, BLU-RAY	1	500
Macchina fotografica digitale, video camera, cavalletto	1	1.000
RISORSE SOFTWARE		
Licenza Windows 10 per macchine virtuali	15	1.000
***Software* forense (1 licenza EnCase, 1 licenza FTK, applicativi vari)**	5	6.000
Licenze WM-Ware/XEN	15	15.000
VARIE		
Materiali promozionali, eventi, gadget, ecc.	-	1.000
TOTALE		**25.900**

* una volta realizzati e testati, attualmente non si è ancora in grado di indicare un costo del dispositivo *hardware ForensicBox* in quanto ancora in fase di sviluppo.

7.9. *Un modello economico sostenibile*.

Al primo comma dell'articolo n. 265 del c.p.p., Spese relative al sequestro penale**,** si legge che «*le spese occorrenti per la conservazione e per la custodia delle cose sequestrate per il procedimento penale sono anticipate dallo Stato, salvo all'erario il diritto di recupero a preferenza di ogni altro creditore sulle somme e sui valori indicati nell'art. 264 (842 att.)*».

Attualmente, i costi sostenuti dalle A.G. coprono l'acquisto di unità di memoria di massa analoghe a quelle da copiare e di DVD in quantità sufficiente per le copie di *backup*.

Proponendo alle Procure il servizio di conservazione e copia/clonazione dei materiali ad un costo di poco superiore a quanto normalmente sostenuto per l'acquisto di memorie di massa di pari capacità - quindi senza oneri aggiuntivi rispetto all'uso attuale - si rimuoverebbe un impedimento importante, economico, ma soprattutto burocratico.

Il sostegno economico al progetto verrebbe originato dagli altri soggetti coinvolti nel procedimento giudiziario (imputati e parti civili, cioè avvocati e periti), tramite richiesta di un corrispettivo per l'accesso protetto agli indizi digitali, come già oggi accade per fotocopie, CD-ROM o DVD. Eventuali altre richieste di analisi forense (ad es. ricerche mirate, esportazione di documenti, analisi approfondite di sistemi, reti, immagini e video, ricostruzione di eventi informatici, ricerche steganografiche e crittografiche) saranno valutate di volta in volta sulla base di un listino specifico.

7.10. *Ipotesi strategiche*.

Ad esempio, il progetto potrebbe partecipare a pieno titolo ad un bando europeo in ambito di sicurezza informatica. Il CINECA dispone già di consulenti per i bandi europei, per cui si potrebbe produrre una documentazione ad hoc da sottoporre alla commissione europea competente.

L'Università di Bologna (CIRSFID), la Regione Emilia-Romagna (LEPIDA) e il Sistema Pubblico di Connettività potrebbero diventare partner istituzionali del progetto.

CAPITOLO VIII

Il progetto ForensicWeb

8.1. Articolazione della sperimentazione – 8.2. *Software* generazione immagini *bit-stream* USB Copy – 8.3. Linguaggio C# e architettura .NET – 8.4. Ambiente di sviluppo integrato *Visual Studio* – 8.5. *Web application* in ambiente *ASP.NET* – 8.6. I vantaggi delle applicazioni *web* – 8.7. *Internet Information Services* – 8.8. *MSQL Server Express* – 8.9. *Software* OSFMount, lettura e montaggio immagini dati – 8.10. Descrizione della *Web Application ForensicWeb*.

8.1. *Articolazione della sperimentazione*.

Stante l'elevata complessità, articolazione e costo d'avviamento del Progetto *ForensicStorage* nella sua interezza, sarà presentato a corollario di questa ricerca una parte significativa del progetto *ForensicStorage* stesso, denominato *ForensicWeb*, che permetterà di dimostrare empiricamente attraverso una rapida sperimentazione come potrebbe svolgersi un'analisi informatica forense di supporti digitali mediante l'utilizzo del protocollo operativo precedentemente illustrato e mediante l'implementazione di una specifica *web application*.

Il caso pratico riguarderà un ipotetico procedimento penale per cui normalmente nella pratica quotidiana si procederebbe ad effettuare un'attività di perquisizione e sequestro si supporti informatici, ai sensi dell'art. 357 c.p. che sarebbero quindi sigillati e messi a disposizione dell'A.G. procedente in attesa che la stessa incarichi un Consulente Tecnico o la Polizia Giudiziaria per la sua analisi che verosimilmente non sarebbe realizzata prima tre mesi dalla data del sequestro.

Attraverso questa sperimentazione si dimostrerà invece come l'applicazione del protocollo operativo previsto nell'ambito del progetto *ForensicStorage* permetterà invece di acquisire il supporto informatico in maniera contestuale o quasi contestuale al suo sequestro, rendendo fruibili nell'arco di pochi minuti i contenuti del supporto informatico sequestrato. Gli inquirenti potranno in tal guisa visionare il contenuto dei supporti sequestrati alla pari del supporto originale, potendo visionare inoltre, i contenuti dei *file* precedentemente cancellati dall'utente. La prima fase della sperimentazione ha previsto l'acquisizione dei supporti informatici sequestrati, seguendo i più recenti e rigorosi standard operativi previsti dalla vigente normativa ed in particolare dagli standard internazionali[393] ISO/IEC 27037:2012, ed i successivi ISO/IEC 27041:2015,

[393] Vedasi il Cap. 5, paragrafo 5.2, della presente tesi di ricerca.

ISO/IEC 27042:2015 e ISO/IEC 27043:2015, utilizzando un apposito *software* scritto in linguaggio Asp.net e mediante un idoneo strumento informatico, quale il *ForensicBox*[394], di cui si è parlato nel capitolo precedente, o in alternativa un comune *computer laptop* di adeguata potenza di calcolo necessaria per svolgere in tempi contenuti le operazioni di acquisizione ed invio del contenuto acquisito al *DataCente*r individuato e previsto dal protocollo attraverso una VPN appositamente realizzata che sfruttando una veloce connessione in fibra ottica, come quella presente nella rete Lepida, garantirà tutte le necessarie garanzie di affidabilità e sicurezza mediante l'implementazione di una cifratura a 256 *bit*. Ovviamente per garantire l'inalterabilità del contenuto, qualora non si utilizzi il dispositivo *ForensicBox* che prevede nativamente questa funzione, bisognerà sempre avvalersi di un dispositivo di protezione in scrittura da inserire tra il *computer laptop* ed il supporto da acquisire per evitare accidentali modifiche. Quanto acquisito verrà inviato al *server* del *DataCenter* ove in automatico verrà calcolata la stringa di *hash* SHA-1 e/o MD-5 per certificare l'assoluta autenticità e conformità della copia *bit-stream* acquisita e collocata sul *server* a quella del supporto originale sequestrato, che da questo momento in poi sarà archiviato e sigillato e collocato in un luogo idoneo per la sua conservazione.

Una volta acquisita la copia *bit-stream* non sarà infatti più necessario agire sul supporto originale, che rimarrà a garanzia dell'attività svolta garantendone in ogni caso, qualora fosse necessario la ripetibilità di ogni operazione compiuta.

Una volta riversata *server* con le dovute garanzie di ripetibilità ed autenticità, la copia *bit-stream* del supporto originale verrà elaborata da uno specifico *software* appositamente realizzato ed implementato nella *web application* denominata *ForensicWeb*, che procederà all'analisi ed al recupero dei *file* presenti all'interno del supporto informatico acquisito, ed anche al recupero dei dati un tempo presenti nel supporto attenzionato, ma cancellati dall'utilizzatore precedentemente al sequestro. Il *software* provvederà quindi alla creazione di specifiche cartelle suddivise per tipologia di *file* recuperati, ove i *file* recuperati verranno suddivisi, al fine di ottenere una loro rapida repertazione e agevolando la loro consultazione.

Nel caso pratico per semplicità e rapidità espositiva, l'acquisizione e dette operazioni si svolgeranno rispetto ad una memoria USB da 128MB, ma la procedura ed il modus operandi sarebbe il medesimo se si procedesse ad acquisire

[394] Vedasi il Cap. 7, paragrafo 7.5, della presente tesi di ricerca.

altre tipologie di supporti informatici con maggiori capacità di memorizzazioni, l'unica difformità si riscontrerebbe nella maggiore quantità di tempo richiesto.

Le evidenze recuperate dalla *web application ForensicWeb*, sia nello spazio allocato della memoria acquisita sia in quello non allocato, oltre ad essere suddivise per tipologia di *file* nelle rispettive cartelle, verranno singolarmente marcate con una firma digitale che produrrà una stringa alfanumerica, questa stringa verrà quindi inserita automaticamente dalla *web application* in un *database* generale che permetterà agli inquirenti, qualora risultasse utile o necessario di effettuare rapidamente e con la massima sicurezza ricerche di *file* incrociate tra differenti attività investigative. Sarà così possibile accertare ad esempio se un determinato *file* o una determinata immagine o più immagini erano presenti anche su altri supporti sequestrati in date e luoghi diversi e nell'ambito di procedimenti penali differenti. Funzionalità che potrebbe permettere di collegare tra loro indagini o imputati che apparentemente non risultavano avere alcuna connessione, aprendo così nuovi ed ulteriori scenari investigativi. Questi *file* e queste informazioni potranno essere rapidamente poste nella disponibilità dell'Autorità Giudiziaria e della Polizia Giudiziaria.

Infatti gli organi inquirenti autorizzati potranno agevolmente ed in tutta sicurezza accedere alla *web application ForensicWeb*, mediante una rete VPN (*Virtual Private Network*) dedicata tra loro ed il DataCenter, previa autenticazione che potrà avvenire mediante.

8.2. *Software generazione immagini bit-stream USB Copy*.

Per quanto riguarda l'attività di copia forense, è stato sviluppato il programma USB Copy basato sul *software open source* DDriveWrite è stato appositamente realizzato per effettuare copie *bit-stream* fedeli all'originale comprensivi dei settori di avvio dei supporti estraibili e le aree di memoria non allocate. Questo potente *software* è stato implementato in maniera trasparente, ovvero automatica ed invisibile all'operatore all'interno della piattaforma *ForensicWeb* (fig. 1).

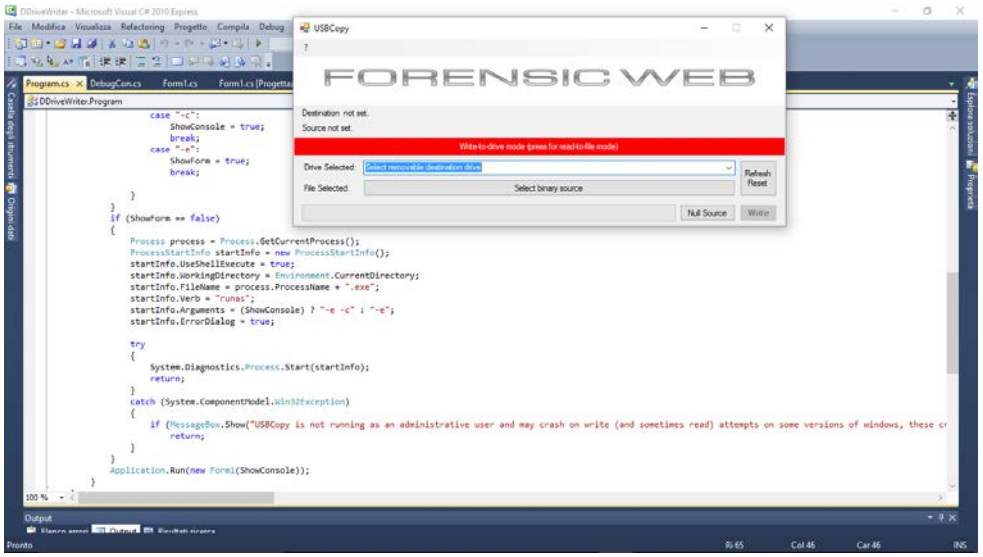


Figura 1. *Screenshot ForensicWeb USB Copy*.

Il *software* USB Copy permette di realizzare una fedele copia bit a bit del supporto originale acquisito rendendo l'immagine acquisita in formato ".IMG", nell'esempio pratico qui esposto produrrà una fedele immagine ".IMG" del dispositivo USB da 128MB analizzato. Detto programma è basato sul *software* di pubblico dominio DDriveWrite, realizzato interamente in linguaggio C# in ambiente di sviluppo *Visual Studio*, e permette la lettura e la scrittura diretta dell'immagine del disco rigido o di una memoria, analogamente a quanto avviene utilizzando il commando di copia "dd" in ambiente Linux. Permette inoltre di realizzare immagini di disco "bootabili" ovvero contenenti applicazioni avviabili all'accensione del *computer*.

Per una esposizione più chiara ed esaustiva della piattaforma forense in oggetto è necessario ora procedere all'analisi dei linguaggi e delle architetture *web* che costituiscono la struttura portante della *web application ForensicWeb*.

8.3. *Linguaggio C# e architettura .NET.*

Introduzione a C# e .NET.

Il *framework* .NET è l'infrastruttura sulla quale è stata creata la struttura portante che costituisce la nuova piattaforma creata da Microsoft per lo sviluppo di applicazioni *component-based*, *n-tier*, per internet, per l'accesso ai dati, per dispositivi mobili, o semplicemente per le classiche applicazioni *desktop*. La piattaforma .NET è composta da diverse tecnologie, strettamente accoppiate fra loro.

L’architettura .NET.

L’architettura del *framework* .NET è illustrata nella figura 2. Essa si appoggia direttamente al sistema operativo, nella figura viene indicato Windows, ma esistono e sono anche a buon punto progetti per portare .NET su ambienti diversi, ad esempio Mono su Linux.

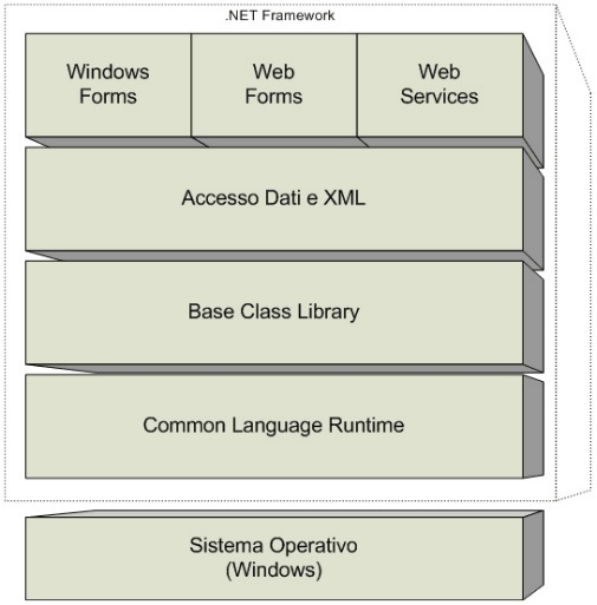


Figura 2. L'architettura del framework.NET

Il *framework*.NET consiste di cinque componenti fondamentali.

Il componente anima e cuore dell’intero *framework*, è il *Common Language Runtime* (CLR). Esso fornisce le funzionalità fondamentali per l’esecuzione di un’applicazione *managed* (gestita appunto dal CLR). Il CLR, a basso livello, si occupa inoltre dell’interfacciamento con il sistema operativo.

Lo strato immediatamente al di sopra del CLR, è costituito dalla *Base Class Library* (o .NET *Framework Class Library*) di .NET, cioè un insieme di classi fondamentali, utili e necessarie a tutte le applicazioni ed a tutti gli sviluppatori. Ad esempio la BCL contiene i tipi primitivi, le classi per l’*Input/Output*, per il trattamento delle stringhe, per la connettività, o ancora per creare collezioni di oggetti. Dunque, per chi avesse esperienza con altre piattaforme, può essere pensato come un insieme di classi analogo a MFC, VCL, Java.

Naturalmente altre classi specializzate saranno sicuramente mancanti nella BCL. Al di sopra della BCL, vengono quindi fornite le classi per l'accesso alle basi di dati e per la manipolazione dei dati XML, che, sono semplici da utilizzare ma estremamente potenti e produttive.

Lo strato più alto del *framework* è costituito da quelle funzionalità che offrono un'interfacciamento con l'utente finale, ad esempio classi per la creazione di interfacce grafiche *desktop*, per applicazioni *web*, o per i sempre più diffusi *web service*.

Il componente CLR.

Il componente più importante del *framework* .NET è come detto il CLR, *Common Language Runtime*, che gestisce l'esecuzione dei programmi scritti per la piattaforma .NET. Chi proviene dal linguaggio Java non farà fatica a pensare al CLR come ad una macchina virtuale del tutto simile concettualmente alla *Java Virtual Machine* che esegue *bytecode* Java. Il CLR si occupa dell'istanziazione degli oggetti, esegue dei controlli di sicurezza, ne segue tutto il ciclo di vita, ed al termine di esso esegue anche operazioni di pulizia e liberazione delle risorse.

In .NET ogni programma scritto in un linguaggio supportato dal *framework* viene tradotto in un linguaggio intermedio comune, detto CIL (*Common Intermediate Language*) o brevemente IL, ed a questo punto esso può essere tradotto ed assemblato in un eseguibile .NET, specifico per la piattaforma su cui dovrà essere eseguito. In effetti, a *run-time*, il CLR non conosce e non vuole conoscere in quale linguaggio lo sviluppatore ha scritto il codice, il risultato della compilazione, è un modulo *managed*, indipendente dal linguaggio utilizzato, è possibile scrivere le applicazioni direttamente in linguaggio IL (fig. 3).

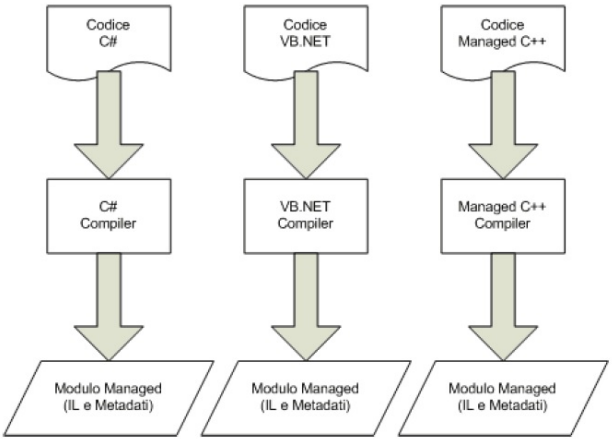


Figura 3. Compilazione del codice in moduli *managed*.

La Figura 3 mostra il processo di compilazione del codice sorgente in moduli managed. Un modulo *managed* contiene sia il codice IL che dei metadati. I metadati non sono altro che delle tabelle che descrivono i tipi ed i loro membri definiti nel codice sorgente, oltre ai tipi e relativi membri esterni referenziati nel codice.

Il CLR però non esegue direttamente dei moduli, esso lavora con delle entità che sono chiamate *assembly*. Un *assembly* è un raggruppamento logico di moduli *managed*, e di altri *file* di risorse, ad esempio delle immagini utilizzate nell'applicazione, dei *file* html o altro ancora, ed in aggiunta a questi *file*, ogni *assembly* possiede un manifesto che descrive tutto il suo contenuto, ciò rende possibile il fatto che ogni *assembly* sia una unità autodescrittiva.

I compilatori .NET, ad esempio il compilatore C#, attualmente creano un *assembly* in maniera automatica a partire dai moduli, aggiungendo il *file* manifesto. Un *assembly* può essere non solo un'eseguibile, ma anche una libreria DLL contenente una collezione di tipi utilizzabili eventualmente in altre applicazioni.

La compilazione JIT.

Il codice IL non è eseguibile direttamente dal microprocessore, almeno da quelli attualmente in commercio, e nemmeno il CLR può farlo, in quanto esso non ha funzioni di interprete. Dunque esso deve essere tradotto in codice nativo in base alle informazioni contenute nei metadati. Questo compito viene svolto a tempo di esecuzione dal compilatore JIT (*Just In Time*), altrimenti detto JITter. Il codice nativo viene prodotto *on demand*. Ad esempio la prima volta che viene invocato un metodo, esso viene compilato, e conservato in memoria. Alle successive chiamate il codice nativo sarà già disponibile in *cache*, risparmiando anche il tempo della compilazione *just in time*.

Il vantaggio della compilazione JIT è che essa può essere realizzata dinamicamente in modo da trarre vantaggio dalla caratteristica del sistema sottostante. Ad esempio lo stesso codice IL può essere compilato in una macchina con un solo processore, ma potrà essere compilato in maniera differente su una macchina biprocessore, sfruttando interamente la presenza dei due processori. Ciò implica anche il fatto che lo stesso codice IL potrà essere utilizzato su sistemi operativi diversi, a patto che esista un CLR per tali sistemi operativi.

CTS e CLS.

Dati i differenti linguaggi che è possibile utilizzare per scrivere codice .NET compatibile, è necessario avere una serie di regole atte a garantirne l'interoperabilità, la compatibilità e l'integrazione dei linguaggi.

Una classe scritta in C# deve essere utilizzabile in ogni altro linguaggio .NET, ed il concetto stesso di classe deve essere uguale nei diversi linguaggi, cioè una classe come intesa da C#, deve essere equivalente al concetto che ne ha VB.NET oppure C++ *managed*, o un altro linguaggio.

Per permettere tutto questo, Microsoft ha sviluppato un insieme di tipi comuni, detto *Common Type System* (CTS), suddivisi in particolare, in due grandi categorie, tipi riferimento e tipi valore, ma ogni tipo ha come primo antenato un tipo fondamentale, il tipo *object*, in tal modo tutto sarà considerabile come un oggetto. Il *Common Type System* definisce come i tipi vengono creati, dichiarati, utilizzati e gestiti direttamente dal CLR, e dunque in maniera ancora indipendente dal linguaggio. D'altra parte ogni linguaggio ha caratteristiche distintive, in più o in meno rispetto ad un altro. Se non fosse così, l'unica differenza sarebbe nella sintassi, cioè nel modo di scrivere i programmi.

Un esempio chiarificante può essere il fatto che C# è un linguaggio *case sensitive*, cioè sensibile alla differenza tra lettere minuscole e maiuscole, mentre non lo è VB.NET. Per garantire allora l'integrazione fra i linguaggi è necessario stabilire delle regole, e nel far ciò Microsoft ha creato una specifica a cui tali linguaggi devono sottostare. Tale specifica è chiamata *Common Language Specification* (CLS).

Naturalmente ogni linguaggio può anche utilizzare sue caratteristiche peculiari, e che non sono presenti in altri, in questo caso però il codice non sarà accessibile da un linguaggio che non possiede quella particolare caratteristica, nel caso contrario, cioè nel caso in cui, ad esempio, un componente è scritto facendo uso solo di caratteristiche definite dal CLS,. allora il componente stesso sarà detto CLS-*compliant*. Lo stesso CTS contiene tipi che non sono CLS-*compliant*, ad esempio il tipo UInt32, che definisce un intero senza segno a 32 bit, non è CLS *compliant*, in quanto non tutti i linguaggi hanno il concetto di intero senza segno.

Gestione della memoria.

In linguaggi come C e C++, lo sviluppatore si deve occupare in prima persona della gestione della memoria, cioè della sua allocazione prima di poter

creare ed utilizzare un oggetto e della sua deallocazione una volta che si è certi di non dover più utilizzarlo. Il CLR si occupa della gestione della memoria in maniera automatica, per mezzo del meccanismo di *garbage* collection. Tale meccanismo si occupa di tener traccia dei riferimenti ad ogni oggetto creato e che si trova in memoria, e quando l'oggetto non è più referenziato, cioè il suo ciclo di vita è terminato, il CLR si occupa di ripulirne le zone di memoria a questo punto non più utilizzate. Tutto ciò libera il programmatore da buona parte delle proprie responsabilità di liberare memoria non più utilizzata, e d'altra parte dalla possibilità di effettuare operazioni pericolose nella stessa memoria, andando per esempio a danneggiare dati importanti per altri parti del codice.

8.4. Ambiente di sviluppo integrato *Visual Studio*.

Visual Studio è lo strumento di punta che Microsoft dedica a chi sviluppa su piattaforma Windows. Fin dalla sua prima versione, datata 1997, la sua missione era già quella di fornire un ambiente di sviluppo grafico ed integrato che aiutasse lo sviluppatore a gestire i progetti in maniera semplice, ma efficace, aumentandone quindi la produttività.

La versione successiva, Visual Studio 6.0, rimase sul mercato per quattro anni e fu una versione di "transizione" perché nel 2002 uscì la prima versione del Visual Studio.NET, il cui nome deriva dal *framework* .NET e di cui la versione attuale è diretta evoluzione.

La novità principale fu che, per la prima volta, Microsoft incluse, in un solo prodotto, il supporto a differenti linguaggi (C++, J++). L'intenzione era quella di ridurre la complessità attuale, in cui ogni linguaggio o tecnologia possedeva uno strumento dedicato ed obbligava lo sviluppatore a dover familiarizzare con molti ambienti differenti.

La rivoluzione stava nell'introduzione di un linguaggio *assembly* intermedio, chiamato MSIL e supportato da differenti linguaggi, ma soprattutto viene introdotto il nuovo linguaggio C#, che di lì a breve ottenne un ottimo successo anche in ambienti *open source*.

Finalmente l'interoperatività tra i linguaggi non era più un sogno, era possibile scrivere una routine in Visual Basic.NET ed utilizzarla poi in C# senza alcun problema; inoltre, scrivendo qualche riga di codice, era possibile anche effettuare chiamate a routine C++, il che doveva stabilire anche la fine dell'era di

COM. Dalla prima versione è iniziata quindi una serie di *upgrade* cadenzati con i quali Microsoft rilascia una nuova versione orientativamente ogni due anni ed un *service pack* negli anni dispari. Ad ogni nuovo rilascio le novità interessano sia l'ambiente di sviluppo, sia le tecnologie ed i linguaggi oltre che l'introduzione di nuove tecnologie e linguaggi, come la tecnologia LINQ, introdotta con il *Visual Studio* 2008 ed il linguaggio F#, introdotto con il *Visual Studio* 2010.

Nel corso degli anni Visual Studio diventa sempre di più fulcro di ogni attività legata allo sviluppo, anche di quelle non propriamente legate al codice, come dimostra il supporto fornito dallo sviluppo di pacchetti di SQL *Service Integration Services* o SQL *Server Reporting services*. Parallelamente al Visual Studio Microsoft propone una soluzione per la gestione del ciclo di vita dei progetti, il primo tentativo si chiama *Source Safe*, ed è semplicemente un *version control system* che si appoggia alla condivisione dei *file* di Windows. Rapidamente il prodotto diventa abbastanza obsoleto, soprattutto con l'avanzare di internet e delle vpn; lavorare in una vpn su internet con *Visual Source Safe* era infatti decisamente lento anche per team piccoli, era necessaria quindi una nuova soluzione. Nel 2005 esce quindi la prima versione di *Team Foundation Server*, la parte "*server*" di Visual Studio che è molto di più di una semplice evoluzione di Visual Source Safe. TFS include naturalmente un *Version Control System*, ma stavolta basato su *database* SQL ed accesso tramite *web services*; il risultato è una maggiore affidabilità e velocità anche su *team* distribuiti con molti sviluppatori.

8.5. *Web application in ambiente ASP.NET.*

La piattaforma *ForensicWeb* è stata sviluppata in ambiente ASP.NET, con il termine "Applicazione *web*" si intende un'applicazione risiedente in un *server web* alla quale si accede tramite un *browser* Internet o un altro programma con funzioni di navigazione operante secondo gli *standard* del *World Wide Web*. Per completezza va detto che con un termine simile, Servizi *web* o *web Service*, si intende un nuovo modo di realizzare applicazioni distribuite ad oggetti, in cui gli oggetti comunicano tra loro attraverso la rete tramite i protocolli SOAP (basato sullo *standard* XML) e HTTP.

Le applicazioni tradizionali.

Un'applicazione tradizionale è un'insieme di funzioni che consentono all'utente di svolgere più velocemente compiti che senza l'elaboratore avrebbero

richiesto molto tempo o attività che senza elaboratore non avrebbe potuto essere realizzate. Dal punto di vista tecnologico essa può essere costituita da un singolo programma "monolitico" (es. applicativi a tracciati proprietari), da un insieme di procedure *software* cooperanti (es. programmi COBOL nell'ambiente CICS) o da programmi *client-server* (es. *client* C di *database* Oracle).

Mentre le prime applicazioni erano completamente testuali e, per l'utente, era necessaria la conoscenza di comandi da fornire all'applicazione stessa per ottenere i risultati desiderati, attualmente le applicazioni presentano un'interfaccia grafica caratterizzata da menù, bottoni, icone: l'utente può quindi interagire, in modo più semplice ed immediato, con l'applicazione grazie a questi elementi grafici. Nonostante il notevole miglioramento a livello utente, un'applicazione tradizionale rimane strettamente dipendente dalla piattaforma e dal sistema operativo sul quale viene installata.

Un'applicazione tradizionale effettua chiamate esplicite al sistema operativo sottostante (per interagire, ad esempio, con i dispositivi di *input* e di *output*): quindi la stessa applicazione non funziona su piattaforma diverse. Questo comporta, per lo sviluppatore, la realizzazione della stessa applicazione in modi differenti: devono infatti, essere sviluppate tante applicazioni (per quanto concerne le parti che effettuano chiamate al sistema operativo) quanti sono i sistemi operativi sui quali si vuole installare l'applicazione.

Il *Client/Server*.

Il paradigma *Client/Server* è un modello di interazione tra processi *software*, ove i processi interagenti si suddividono tra *client*, che richiedono i servizi, e *server*, che offrono servizi. L'interazione *client/server* richiede perciò una precisa definizione di un'interfaccia di servizi, che elenca quelli messi a disposizione dal *server* stesso. Il processo *client* è tipicamente dedicato ad interagire con l'utente finale; esso svolge un ruolo attivo, in quanto genera autonomamente richieste di servizi. L'interazione con l'utente implica:

- *Data-entry*.
- Gestione video.
- Gestione finestre.
- Menù e maschere.
- Gestione cursori.

Per quanto riguarda il *data-entry* il *client* può elaborare la sequenza di dati che l'utente immette, ossia il *client* ha il compito di verificare e convalidare i dati: è, infatti, inutile appesantire la comunicazione con dati che non verrebbero accettati dal *server*. Tuttavia certe volte servono delle informazioni che il *client* non possiede, ma che solo il *server* conosce, allora il *client* deve prelevarle interrogando il *server*. Il processo *server* è reattivo: svolge una computazione solo a seguito di una richiesta da parte di un qualunque *client* ed è sempre in esecuzione per essere pronto a rispondere alle richieste.

Non è necessario che i processi *server* e *client* siano allocati su macchine diverse: la distinzione fra processi *client* e *server* è un ottimo paradigma per la costruzione del *software*, indipendentemente dall'allocazione dei processi sulle architetture fisiche sottostanti. Questa architettura viene denominata a due componenti (o *two tier*) in quanto in essa sono presenti un *client*, con funzioni sia di interfaccia utente sia di gestione dell'applicazione, e un *server*, dedicato alla gestione dati. Le prime applicazioni a due livelli sono state sviluppate per accedere a *database* di grandi dimensioni e le regole utilizzate per la gestione dei dati con l'interfaccia utente erano incorporate nell'applicazione *client*.

Il compito del *server* consisteva, semplicemente, nell'elaborare il maggior numero possibile di richieste di memorizzazione e recupero dati.

Le applicazioni a due livelli eseguono molte delle funzioni dei sistemi autonomi, ovvero presentano un'interfaccia utente, raccolgono ed elaborano l'input dell'utente, eseguono l'elaborazione richiesta e segnalano lo stato della richiesta. Questa sequenza di comandi può essere ripetuta per il numero di volte necessario. Poiché il *server* fornisce solo l'accesso ai dati, il *client* utilizza le proprie risorse locali per eseguire la maggior parte dell'elaborazione.

L'applicazione *client* deve includere informazioni sulla posizione in cui risiedono i dati e sulla loro organizzazione nel *database*. Dopo aver recuperato i dati, il *client* è responsabile della loro formattazione e visualizzazione. Uno dei principali vantaggi offerti dal modello *client*/*server* è rappresentato dal fatto che, consentendo a più utenti di accedere contemporaneamente agli stessi dati dell'applicazione, gli aggiornamenti eseguiti in un *computer* vengono immediatamente resi disponibili a tutti i *computer* che hanno accesso al *server*.

Tuttavia questo comporta, nel caso in cui sempre più *client* effettuino le loro richieste allo stesso *server*, un sovraccarico del *server* stesso. Per ovviare a questo problema e ottenere un accesso più rapido ai dati e tempi di sviluppo più brevi, benché applicazioni aziendali su scala ridotta continuino

ad avvalersi della semplicità e della flessibilità offerte dai prodotti a due livelli, si è diffusa un'architettura alternativa detta a tre componenti (o *three tier*), in cui è presente un secondo *server*, detto *server* applicativo, responsabile di gestire la logica applicativa comune a più *client*. In questa architettura, il *client* è assai semplice e si occupa del solo interfacciamento con l'utente finale. Il *client* invia le richieste al *server* applicativo, e quest'ultimo dialoga con il *server* per la gestione dei dati secondo le modalità illustrate in precedenza.

Nelle applicazioni che si basano su questo modello l'elaborazione viene distribuita tra il *client* e il *server* e la logica aziendale viene gestita a livello intermedio. Nella maggior parte dei sistemi vengono eseguite le tre seguenti operazioni che corrispondono ai tre livelli del modello (fig. 4):

- *Interfaccia utente ed esplorazione*: questo livello include tutte le operazioni per l'interazione con l'utente: non solo fornisce un'interfaccia grafica che consente agli utenti di interagire con l'applicazione, immettere i dati e visualizzare i risultati delle richieste, ma gestisce anche la modifica e la formattazione dei dati pervenuti al *client*. Nelle applicazioni *web* le operazioni di questo livello vengono svolte dal *browser*.

- *Logica aziendale*: questo livello è il dominio dello sviluppatore di applicazioni distribuite. La logica aziendale, fondata sulle regole che governano l'elaborazione delle applicazioni, gestisce i collegamenti tra utente e dati. Le funzioni governate da tali regole simulano fedelmente le operazioni aziendali giornaliere e possono riferirsi a singole operazioni o a serie di operazioni.

- *Servizi per la gestione dei dati*: questo livello fornisce i servizi di gestione dei dati tramite un archivio strutturato o non strutturato, che consente di accedere e gestire i dati dell'applicazione. In un'applicazione possono essere resi disponibili i servizi corrispondenti a uno o più archivi di dati.

- Nell'architettura a tre livelli, ciascuna delle funzionalità principali è isolata dalle altre, in modo che il livello di presentazione sia indipendente dalle regole di elaborazione e dalla logica aziendale, che a loro volta sono separate dai dati. Questo modello richiede un maggior impegno in termini di analisi e di progettazione preliminari, ma consente di ridurre in misura significativa i costi di manutenzione e nel lungo periodo aumenta la flessibilità funzionale.

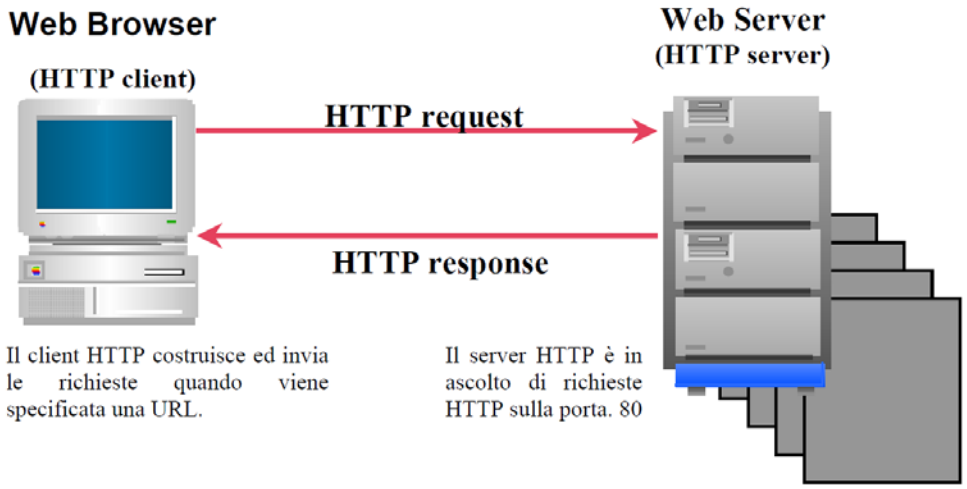


Figura 4: Il Protocollo HTTP.

8.6. *I vantaggi delle applicazioni web*.

I componenti fondamentali di un'applicazione *web* sono analoghi a quelli di una tradizionale applicazione *client*/*server*: nell'ambito del *web*, tuttavia, l'interazione tra *client* e *server* è molto più articolata per consentire l'integrazione di componenti di varia natura. Un'applicazione *web* si basa su elementi *software* standard, indipendenti dalle caratteristiche della particolare applicazione e dalla piattaforma *software* e *hardware* su cui viene eseguita.

Nella maggior parte dei casi, un'applicazione *web* si sviluppa su tre livelli (applicazione *three tier*): livello di presentazione, intermedio e dati; in alcuni casi si possono avere applicazioni multilivello (o *multi tier*).

Non sempre i livelli logici di un'applicazione *web* corrispondono a locazioni fisiche sulla rete; infatti si possono avere casi in cui tutti e tre i livelli risiedono sulla stessa macchina fino ad arrivare alla corrispondenza di ciascun livello con una macchina fisica. Il livello di presentazione costituisce l'interfaccia utente dell'applicazione *web* e corrisponde a quello che, nelle applicazioni *client*/*server* standard, è il *client*. Esso è costituito da vari componenti combinati tra loro: *browser*, documenti HTML, *applet* Java, controlli ActiveX. La capacità di utilizzo di questi elementi da parte del *client* è uno dei problemi principali nella realizzazione di questo livello. Il livello intermedio di un'applicazione *web* corrisponde alla logica elaborativa dell'applicazione: esso è in grado di soddisfare le richieste di dati e di elaborazione del *client*. Le modalità di realizzazione del

livello intermedio dipendono dalle caratteristiche e dalle tecnologie supportate dal *server web* e/o dai componenti installati sul *server* applicativo.

In funzione della tipologia di applicazione da sviluppare, è possibile dover prevedere funzionalità particolari, quali la gestione delle transazioni per il flusso affidabile dei dati o la gestione della sicurezza nell'accesso all'applicazione e della riservatezza nella trasmissione delle informazioni.

Il livello intermedio di un'applicazione *web* può essere costituito da un insieme di *script*, componenti e programmi interagenti tra di loro e con il *server web* tramite le seguenti tecnologie:

• *Common Gateway Interface* (CGI): consente l'attivazione di un programma su richiesta del *client* (portabile su qualsiasi applicazione).

• *Internet Server Application Interface* (ISAPI): consente l'esecuzione di una libreria dinamica (DLL) all'interno dello spazio di memoria del *server web* (funziona solo su piattaforma Windows).

• *Active Server Pages* (ASP): consente l'interpretazione di *script* nell'ambiente del *server web* e la creazione in modo dinamico di documenti *web* (sviluppato soprattutto per piattaforma e *server web* Windows).

• PHP: consente l'interpretazione di *script* nell'ambiente del *server web* e la creazione in modo dinamico di documenti *web* (sviluppato soprattutto per piattaforma Unix/Linux e *server web* Apache).

• Java Servlet: consente di eseguire classi Java su richiesta del *client* (portabile su qualsiasi piattaforma).

Il livello dati fornisce servizi non direttamente disponibili tramite il *server web*; questi servizi sono generalmente forniti da applicazioni indipendenti dall'ambiente *web*.

Tipici esempi di applicazioni presenti a questo livello sono:

• *Server* dati (DBMS).

• *Server* di *mail* (POP, SMTP).

• *Server* di documentazione elettronica.

In genere è opportuno prevedere dei componenti dell'architettura dell'applicazione che fungono da connettori tra il livello intermedio e il livello dati; infatti, utilizzando dei connettori per l'interazione con applicazioni esterne non standard, si facilita la manutenibilità nel caso in cui queste vengano modificate o sostituite (es. ODBC, OLEDB, JDBC).

In un sistema basato sul *web*, le applicazioni vengono eseguite all'interno di un *browser* che inoltra le richieste ai *server web* utilizzando un protocollo detto HTTP (*HyperText Transfer Protocol*) (fig. 5).

Il livello di presentazione di un'applicazione basata sul *web* viene creato per mezzo di HTML (*HyperText Markup Language*).

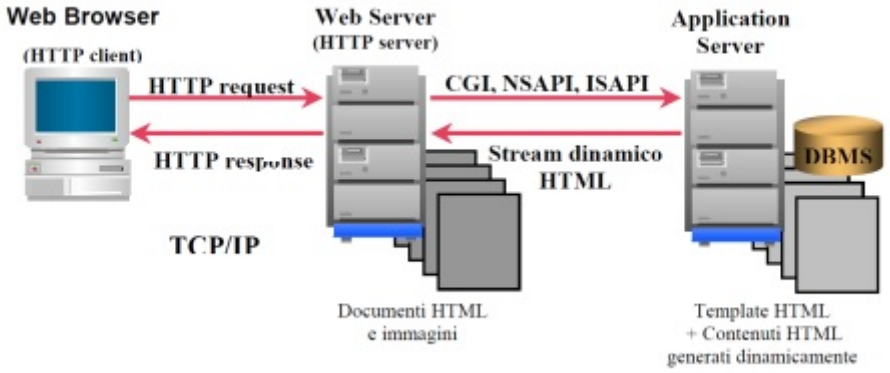


Figura 5: Stratificazione fisica di un Sistema *web*.

Il funzionamento di un'applicazione *web* è molto semplice: un *client* inoltra una richiesta al *server web*, che risponde elaborando la richiesta ed inviando all'utente la pagina HTML. Il vantaggio di HTTP e HTML è che sono supportati da tutte le principali piattaforme. Il *server web* costituisce il punto di accesso al livello intermedio: quando un *client* inoltra una richiesta HTTP, l'applicazione del livello intermedio deve caricare ed eseguire gli oggetti aziendali per sfruttare i vantaggi dello sviluppo multilivello. Malgrado il codice e le pagine HTML, che costituiscono il livello di presentazione, risiedano nel *server*, è possibile separare gli elementi dell'interfaccia utente, la logica aziendale e il codice per l'accesso ai dati. Se l'applicazione *web* è ben progettata, si possono sfruttare tutti i vantaggi dello sviluppo multilivello; si possono condividere le risorse specifiche del processo tra numerosi utenti (risorse quali la memoria e le connessioni al *database*); si può rispondere a ciascuna richiesta "http" reperendo i dati ed eseguendo le transazioni che operano su più fonti dati; inoltre lo sviluppo basato sul *web* elimina o riduce in modo significativo i problemi di configurazione lato-*client*. Le applicazioni *web* sono, per definizione, distribuite. Con l'aumentare delle potenzialità di elaborazione del *client*, aumentano anche le potenzialità di distribuzione dell'elaborazione tra il *client* e il *server*.

Assegnando al *client* una parte dell'elaborazione, è possibile aumentare la velocità di risposta dell'applicazione. La distribuzione dell'elaborazione, tuttavia, comporta anche una maggiore complessità della progettazione delle applicazioni.

Quando si distribuisce l'elaborazione tra *client* e *server*, è necessario tenere presenti due obiettivi di progettazione. Innanzitutto, è necessario ridurre al minimo le comunicazioni sulla connessione HTTP; in questo modo, infatti, l'elaborazione locale sarà più rapida ed indipendentemente dalla velocità della connessione stabilita.

Il secondo obiettivo di progettazione da considerare è rappresentato dalla necessità di esporre al *client* solo le risorse del *server* assolutamente necessarie per eseguire le operazioni di elaborazione. Ogni richiesta del *client* deve essere qualificata con la massima precisione, in modo che il *server* non debba rispondere al *client* richiedendo ulteriori informazioni e aumentando, pertanto, il numero di comunicazioni sulla connessione HTTP. La realizzazione di applicazioni *web* presenta quindi alcune problematiche sconosciute alle applicazioni tradizionali; queste problematiche derivano dalla natura stessa del *web*, pensato originariamente non per la realizzazione di applicazioni ma per la distribuzione di documenti. Un classico esempio, è quello relativo al mantenimento dello stato dell'applicazione: il modello d'interazione di base del *web* è privo del concetto di connessione, quindi lo sviluppatore deve utilizzare informazioni codificate nella richiesta HTTP e nelle risorse condivise, durante la sequenza d'interazioni per stabilire la continuità dell'applicazione.

La progettazione di un'applicazione *web* deve anche tener conto dell'ampiezza della banda di trasmissione disponibile e del carico di lavoro stimato per il *server*.

Dalle considerazioni sull'ampiezza di banda derivano le scelte relative alla quantità di dati da inviare ad un *client* in risposta ad una richiesta. Tuttavia, all'ottimizzazione dell'uso dei mezzi trasmissivi può contribuire un'attenta ripartizione del carico di elaborazione tra *client* e *server*.

Inoltre, la presenza di applicazioni esterne particolarmente complesse, sulla stessa macchina del *server web*, può rendere meno efficiente l'applicazione *web* sottraendole risorse preziose: in questi casi può essere opportuno distribuire il carico di lavoro su macchine diverse.

Nonostante queste problematiche, un'applicazione *web*, soprattutto nell'ambito di una Intranet aziendale, permette di avere alcuni vantaggi.

La presenza di una sola applicazione *server* per tutte le applicazioni *client*

semplifica le implementazioni e riduce i costi di gestione dei PC *client*.
E' possibile utilizzare installazioni standard e il *client* può gradualmente aggiornarsi mentre accede alle varie applicazioni. Inoltre, in un ambiente aziendale in cui il controllo sul *software* della macchina di un utente potrebbe essere rigido, si possono produrre applicazioni per uno specifico *browser*, consentendo in tal modo agli sviluppatori di sfruttarne appieno le capacità. Infine le applicazioni *web* permettono di lavorare da casa o da una postazione che non sia l'ufficio, senza pregiudicarne in alcun modo la funzionalità.

8.7. *Internet Information Services*.

Microsoft Internet Information Services (spesso abbreviato in IIS) è un complesso di servizi *server* Internet per sistemi operativi Microsoft Windows.

Inizialmente distribuito come *Option Pack* per il sistema operativo Windows NT, venne poi integrato in Windows 2000 e Windows *Server* 2003.

La versione corrente, integrata in Windows *Server* 2012 R2, è la 8.5 ed include i servizi *server* per i protocolli FTP, SMTP, NNTP e HTTP/HTTPS. Le prime versioni includevano anche un servizio per il protocollo Gopher.

8.8. *MSQL Server Express*.

SQL *Server Express* è un prodotto di *database* gratuito e facile da usare, basato sulla tecnologia SQL *Server* 2010. È progettato per offrire una piattaforma di *database* di semplice utilizzo, in modo da consentire un *deployment* estremamente rapido in tutti gli scenari di destinazione previsti. Questa facilità di utilizzo caratterizza l'intero prodotto, a partire dal programma di installazione con interfaccia grafica, semplice e affidabile, che guida l'utente in tutto il processo di installazione. Insieme a SQL *Server Express* vengono forniti gratuitamente altri strumenti con interfaccia grafica, che includono Express Manager (versione alfa) e SQL *Computer Manager*, che semplificano le operazioni di base sui *database* e sono rivolti agli sviluppatori dilettanti. La progettazione e lo sviluppo di applicazioni di *database* sono resi più semplici dall'integrazione con i progetti di Visual Studio. È stata inoltre introdotta la possibilità di eseguire il *deployment* di applicazioni di *database* semplicemente spostandole come normali *file* di Windows. In questo modo risultano più semplici anche la manutenzione e l'applicazione di *patch*, che possono essere automatizzate.

Oltre a utilizzare lo stesso motore di *database* affidabile e ad alte prestazioni delle altre versioni di SQL *Server* 2010, SQL Server Express utilizza anche le stesse API di accesso ai dati, ad esempio ADO.NET, SQL *Native Client* e T-SQL.

Questo prodotto differisce, infatti, delle altre edizioni di SQL *Server* 2010 solo per gli aspetti seguenti:

- supporto di una sola CPU;
- limite di 1 GB di memoria per il pool di *buffer*;
- dimensione massima dei *database* limitata a 4 GB.

Funzionalità quali la chiusura automatica e la possibilità di copiare *database* come semplici *file* sono attivate per impostazione predefinita in SQL *Server Express*, mentre sono assenti le funzionalità di *Business Intelligence* e per la disponibilità elevata. Se necessario è possibile espandere il sistema in modo estremamente semplice, perché le applicazioni basate su SQL *Server Express* sono in grado di interagire in modo completamente trasparente con SQL *Server* 2010 *Standard Edition* ed *Enterprise Edition*. Grazie al *download web* i *file* possono essere ottenuti gratuitamente, in modo pratico e veloce.

SQL *Server Express* è stato sviluppato pensando a due diversi tipi di utilizzo. Il primo riguarda l'utilizzo del prodotto come *server*, soprattutto come *server web* o di *database*. Nel secondo caso il prodotto viene utilizzato come archivio dati *client* locale, una situazione in cui l'accesso ai dati utilizzati dalle applicazioni non dipende dalla rete. Semplicità e facilità di utilizzo sono obiettivi di progettazione chiave.

8.9. *Software OSFMount, lettura e montaggio immagini dati.*

Successivamente alla creazione dell'immagine del supporto acquisito, in formato ".img" mediante l'utilizzo del *software* implementato nella piattaforma forense *ForensicWeb* nel nostro esempio pratico, la memoria USB da 128MB, il passo successivo consisterà nel "montaggio" di tale *file* di immagine per poterlo rendere intelleggibile al sistema, e procedere quindi alla sua analisi ed elaborazione. Questa fondamentale funzione è stata realizzata utilizzando il *software open source* OSFMount, anch'esso implementato nella *web application ForensicWeb*. Il *software* OSFMount risulta essere estremamente valido e versatile, permettendo di montare *file* di immagine dei dischi o dei supporti di memoria precedentemente acquisiti mediante copia forense *bit-stream* o *bit* a *bit*, e di montarla come unità esterna accessibile ad un sistema operativo Microsoft

Windows. Per impostazione predefinita del programma i *file* di immagine vengono montati in sola lettura in modo che i *file* di immagine originali non vengano modificati. Il *software* OSFMount supporta anche la creazione di dischi RAM, cioè un disco montato nella RAM del sistema, permettendo così notevoli vantaggi in termini di velocità nell'accesso ai dati rispetto all'uso di un comune *hard disk*, infine anche il montaggio di immagini in formato .ISO è supportato.

Nello schema seguente vengono indicati i numerosi formati di lettura e montaggio supportati dal *software* OSFMount (fig. 6).

Image Format	Read
Raw Image (.IMG, .DD)	✓
Raw CD Image (.ISO, .BIN)	✓
Split Raw Image (.00n)	✓
Nero Burning ROM Image (.NRG)	✓
System Deployment Image (.SDI)	✓
Advanced Forensics Format Images* (AFF)	✓
Advanced Forensics Format Images w/ meta data* (AFM)	✓
Advanced Forensics Format Directories* (AFD)	✓
VMWare Image (.VMDK)	✓
EnCase EWF (.E01)	✓
SMART EWF (.S01)	✓
VHD Image (.VHD)	✓

Figura 6: Formati *file* immagine supportati in montaggio e lettura dal *software* OSF Mount.

8.10. *Descrizione della Web Application ForensicWeb.*

Il sistema *ForensicWeb*, parte integrante e fondamentale del più vasto e generale progetto *ForensicStorage*, nasce proprio dalla coniugazione ed evoluzione di queste tecnologie e linguaggi di programmazione e sviluppo di applicazioni *web*, per offrire all'Autorità Giudiziaria e alla Polizia Giudiziaria nuovi strumenti operativi di acquisizione e analisi dei supporti di memoria sequestrati nell'ambito dell'attività di repressione e contrasto della criminalità informatica e non solo. Illustrate le tecnologie di base utilizzate per implementare la piattaforma operativa forense *ForensicWeb*, di seguito s'illustrerà la dimostrazione pratica dell'utilizzo della piattaforma mediante la simulazione di una attività investigativa posta in essere dalla Polizia Giudiziaria nell'ambito di un sequestro di un dato supporto informatico, consistente nella nostra simulazione in una *memory key* Iomega da 128MB, come si è già avuto modo di precisare

l’esiguità della capacità di memoria del supporto da acquisire è giustificata dalla necessità di sviluppare un’attività di acquisizione, *upload* al *server* del *DataCenter* ed elaborazione e raccolta dei dati compatibile con i tempi dell’esposizione della presente tesi di dottorato. Analoghe attività svolte su supporti informatici di maggiori capacità si svolgerebbero con le stesse identiche modalità operative ma con tempi operativi di gran lunga superiori da parte della *web application ForensicWeb*. Il primo passo essenziale, consiste nella procedura di autenticazione effettuata sul portale *ForensicWeb* da parte di operatori di giustizia ed investigatori autorizzati all’accesso (fig. 7). L’autenticazione verrà effettuata in questa fase sperimentale mediante inserimento di “*username*” e “*password*”, tuttavia il protocollo operativo prevede a regime l’utilizzo di s*mart card* con certificati di Firma Digitale e autenticazione CNS, così come indicato al paragrafo 7.6 del precedente capitolo.

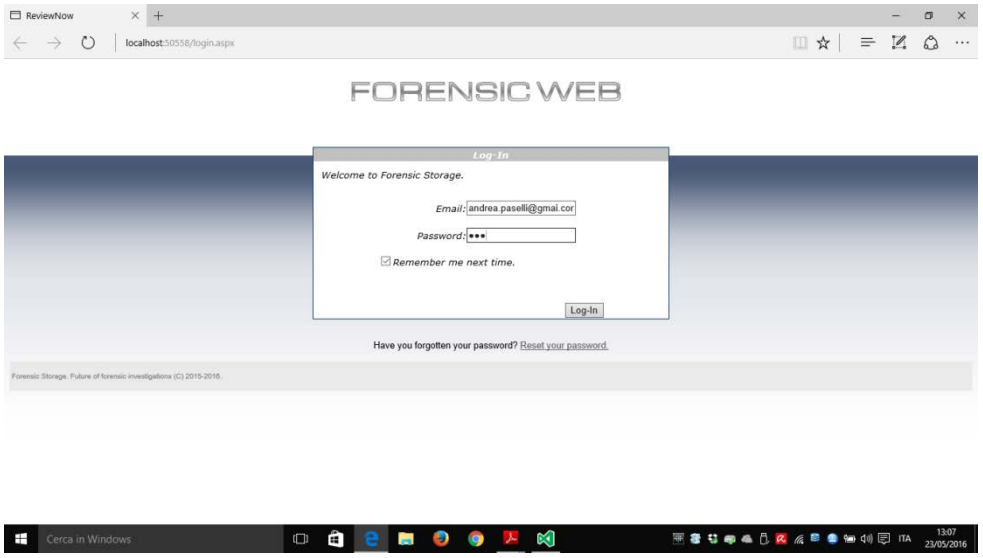


Figura 7: Schermata di Login alla *web application* con credenziali.

Successivamente all’autenticazione, l’operatore potrà accedere al menu principale del *ForensicWeb*, dove potrà accedere ai numerosi strumenti e servizi già implementati ed a quelli che saranno via via realizzati (fig. 8).

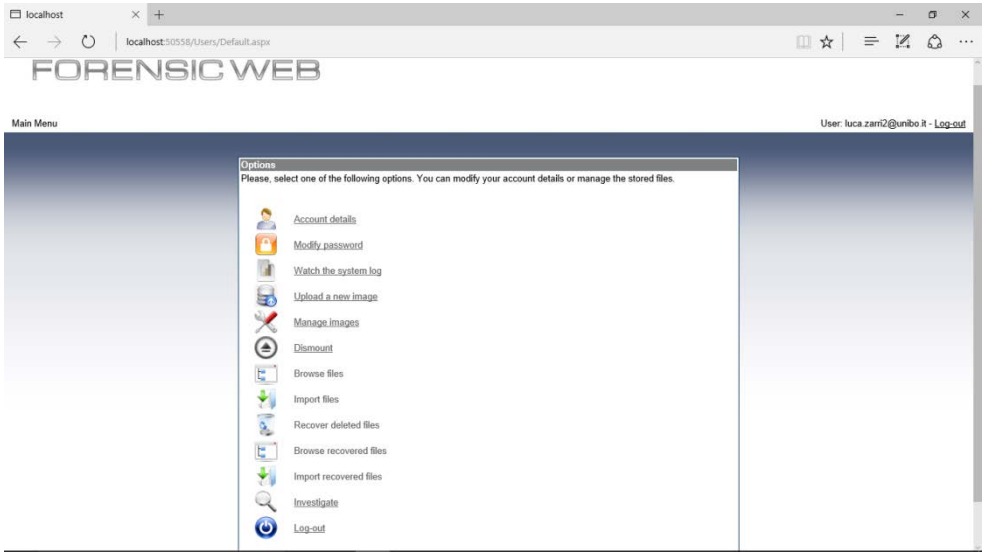


Figura 8: Menu Principale della *Web Application*.

Da questo menu sarà possibile effettuare l'*upload*, cioè l'invio di una immagine dati precedentemente acquisita dall'operatore mediante il descritto *software USB Copy* sulla piattaforma *ForensicWeb*, attraverso la selezione del *file* contenente l'immagine dati da questo menu di ricerca e selezione (fig. 9).

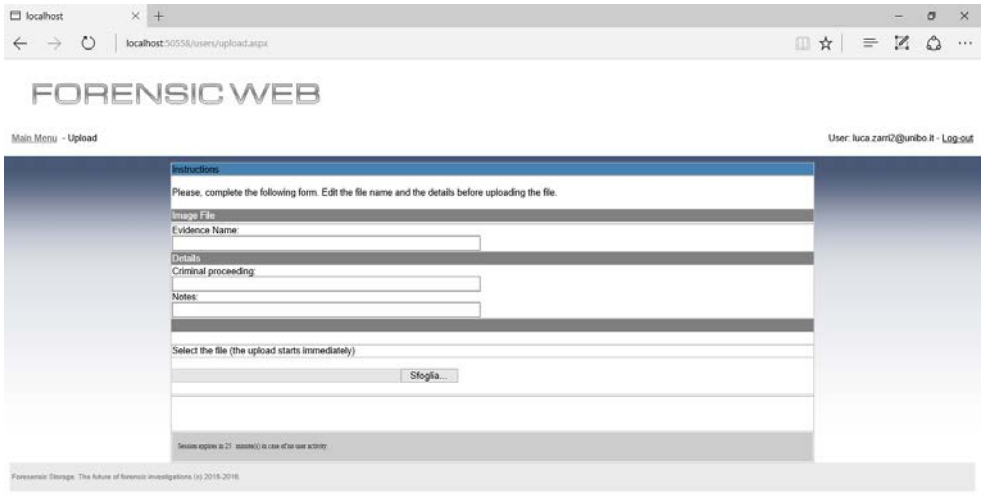


Figura 9: Schermata di *upload* di una immagine dati acquisita con il *software* USB Copy.

Ultimata la fase di *upload* dell'immagine dati, sulla piattaforma *ForensicWeb* sarà possibile accedere alla pagina di gestione delle immagini dati memorizzate e procedere eventualmente al loro "montaggio", in modo da renderla intelleggibile e farla riconoscere al sistema proprio come se si trattasse di una memoria esterna appena collegata, con tutte le garanzie tecniche di autenticità ed inalterabilità del dato digitale acquisito (fig. 10).

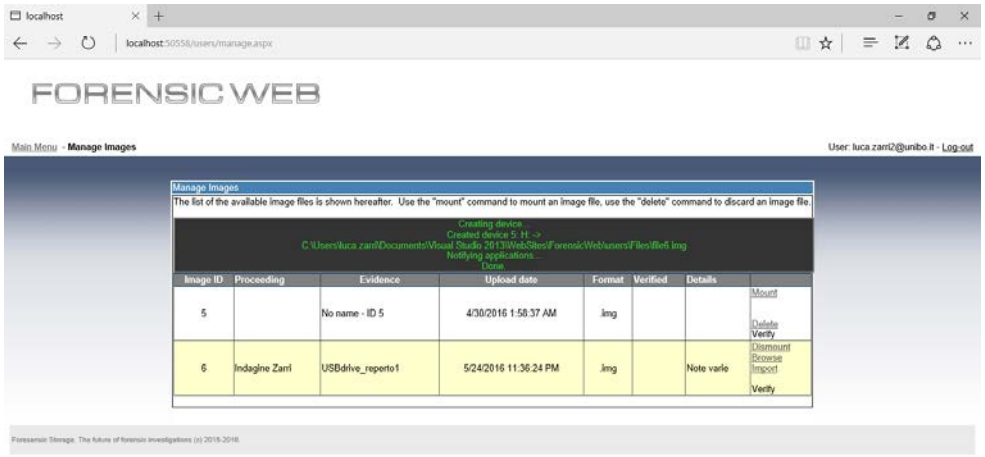


Figura 10: Schermata gestione delle immagini memorizzate e loro montaggio.

Si procederà pertanto a selezionare l'immagine della chiavetta USB Iomega da 128MB precedentemente acquisita, questa semplice operazione permetterà alla piattaforma forense avvalendosi della potenza di calcolo computazionale del *DataCenter* di visualizzare i contenuti del supporto di memoria acquisito e di svolgere tutte le elaborazioni di raccolta, classificazione e recupero dei *file* ivi contenuti, per svolgere la ricerca della prova digitale.

Si potrà quindi avere pieno accesso a tutte le cartelle ed i *file* presenti nello spazio allocato della chiavetta di memoria acquisita, come se fosse stata semplicemente collegata ad una porta USB del *computer* in uso, con la sostanziale differenza che si tratta invece di una memoria virtuale assolutamente fedele al supporto originale, liberamente accessibile senza che questa attività di esplorazione dei contenuti comporti alcuna alterazione dei dati originali, come accadrebbe invece esplorando i contenuti sul supporto originale. Sarà inoltre possibile raccogliere e catalogare tutti i *file* presenti in specifiche e separate cartelle per una ricerca più rapida ed agevole. Infine, la piattaforma *ForensicWeb* potrà agevolmente recuperare tutti i dati, qualora non siano stati completamente sovrascritti, presenti sul supporto precedentemente cancellati dall'utilizzatore.

Nello *screenshot* successivo si può vedere come è possibile effettuare l'esplorazione dei *file* e delle cartelle contenute all'interno dell'immagine *bit-stream* acquisita (fig. 11).

Figura 11: Schermata di visualizzazione con diagramma ad albero del contenuto di un *file* immagine dati precedentemente acquisito con copia *bit-stream*.

Nello *screenshot* che segue è invece presente la finestra, mediante la quale è possibile impostare i filtri di ricerca ritenuti utili ai fini dell'individuazione della prova digitale ricercata, come ad. esempio filtrare la ricerca di una specifica tipologia di *file* oppure effettuare una ricerca mediante l'utilizzo di una parola chiave (fig. 12).

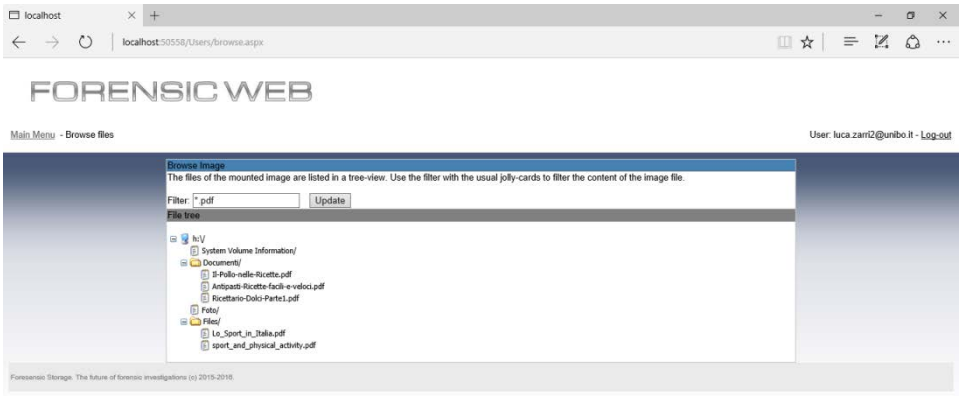


Figura 12: Schermata azione del filtro di visualizzazione del contenuto del *file* immagine acquisito.

Come si è già illustrato, la *web application* in esame permette di recuperare anche i *file* non più visibili nello spazio allocato del dispositivo acquisto poiché precedentemente cancellati dall'utilizzatore. Questa possibilità di recupero è possibile allorquando il settore[395] o le celle di memoria ove era presente il *file* cancellato non siano stato in seguito completamente sovrascritte da altre informazioni (fig. 13).

[395] Il settore è l'unità più piccola della formattazione di basso livello che riguarda la struttura fisica del disco rigido, ed ha una capacità di 4096 byte (Fonte Wikipedia).

Figura 13: Schermata riportante la procedura di recupero dei *file* nei settori non allocati del supporto di memoria acquisito (procedura di *undelete*).

La funzione di *recovery* è stata implementata sulla *web application ForensicWeb* sfruttando il *software open source* "Kickass Undelete", un *software* di recupero dati estremamente potente e versatile che supporta svariati *filesystem* tra i quali FAT ed NTFS. Si è provveduto pertanto ad effettuare una approfondita ricerca dei *file* precedentemente cancellati dalla memoria USB Iomega da 128MB con questa funzionalità di *recovery* implementata, la schermata che segue rappresenta il *report* ottenuto al termine della procedura di recupero, permettendo all'investigatore di recuperare svariati *file* cancellati (fig. 14).

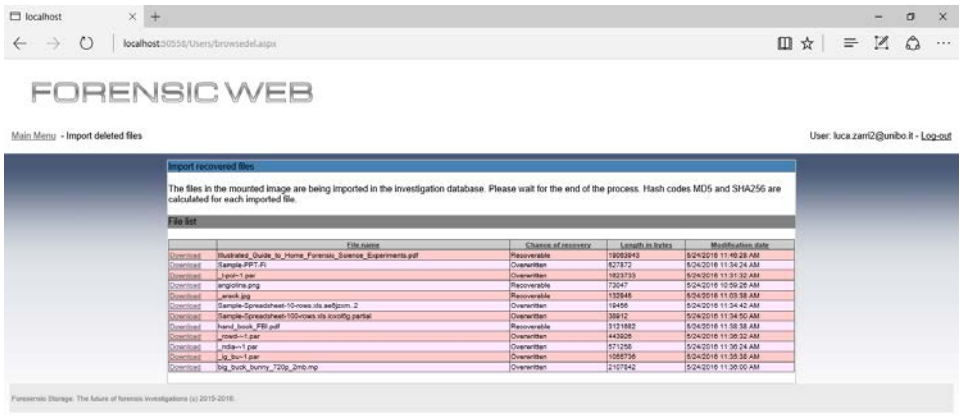


Figura 14: Schermata di *report* ottenuta al termine della procedura di recupero effettuata con la *web application*, con l'ausilio del *software open source* Kickass Undelete.

Al termine del processo di raccolta e recupero dei *file* presenti all'interno del supporto esaminato, verrà generato un *database* complessivo comprendente tutti i dati ed i documenti individuati, che permetterà all'operatore di avere immediata evidenza delle risultanze operative dell'attività forense svolta (fig. 15).

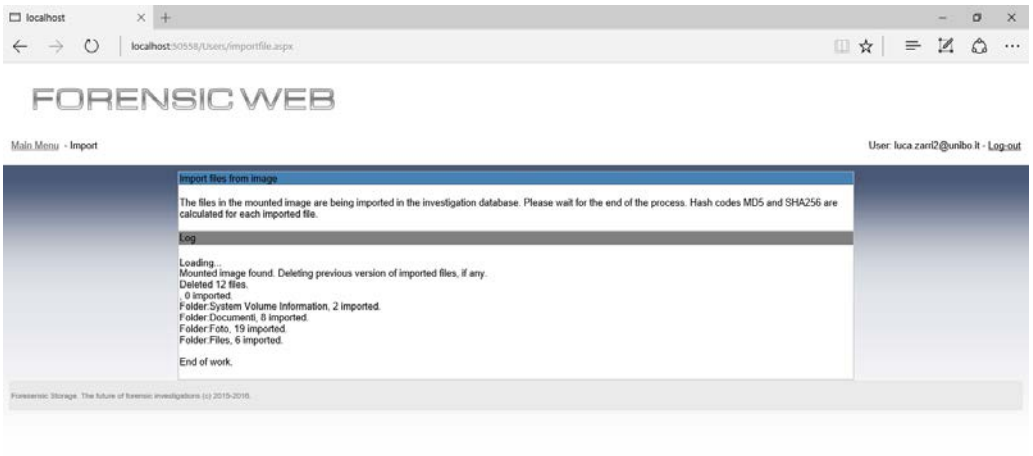


Figura 15: Schermata importazione dei *file* all'interno di un *database* complessivo e generazione di un *database* di tutti i documenti individuati all'interno dei *file* allocati del supporto informatico acquisito, nel caso di esempio chiavetta di memoria USB Iomega da 128MB.

Infine una ulteriore ed importantissima possibilità che offre lo sviluppo del progetto della *web application ForensicWeb* è data dalla possibilità di effettuare non solo ricerche mirate ad individuare la prova digitale del singolo caso di volta in volta analizzato, come ad esempio la ricerca della *digital evidence* all'interno della memoria USB Iomega da 128MB utilizzata per questa dimostrazione, ma bensì di effettuare anche ricerche incrociate di dati, immagini, parole chiave all'interno del materiale informatico sequestrato ed archiviato all'interno del *DataCenter* attraverso la piattaforma forense *ForensicWeb*. Questa funzione è resa possibile grazie all'assegnazione univoca ad ogni *file* recuperato di una firma digitale corrispondente alla propria stringa di *hash*, tutte queste stringhe via via generate nelle successive acquisizioni ed analisi dei supporti informatici sequestrati a seguito dell'attività investigativa. Sarà così possibile verificare se nell'ambito di attività investigative diverse, effettuate in luoghi e tempi diversi e a carico di imputati differenti siano presenti uno o più elementi di correlazione, permettendo così in taluni casi di aprire nuovi scenari investigativi o dimostrare eventuali attività criminali svolte in concorso tra soggetti diversi, ecc.

Per concludere, si evidenzia anche l'implementazione dell'*Health Monitor Log*, che permette di visualizzare ed avere sempre sotto controllo lo stato del sistema ed avere traccia dell'attività che è stata svolta sullo stesso, con particolare riguardo agli accessi al sistema (fig. 16).

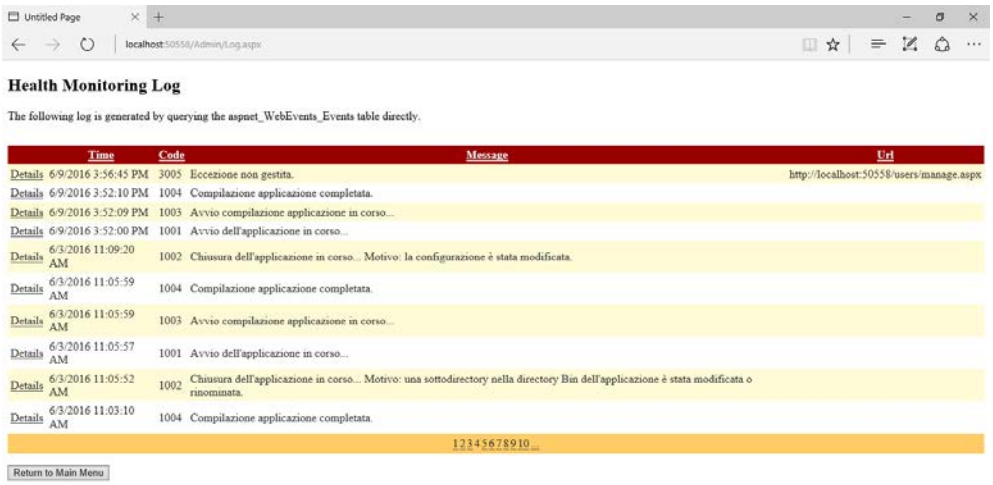


Figura 16: Schermata *Health Monitor*, che visualizza lo stato del sistema *ForensicWeb*.

Conclusioni

A conclusione di questa esposizione risulta evidente come ogni articolo normativo, ogni manuale di diritto, ogni testo consultato per poter definire compiutamente il concetto di prova digitale e affrontarne le relative implicazioni processuali, ne ha evidenziato l'aspetto riguardante la sua fragilità, inconsistenza ed immaterialità. Che la *digital evidence* sia per sua stessa natura estremamente fragile e vulnerabile è facile da intendere, fragile al punto che si è resa necessaria una Convenzione *ad hoc* predisponente le cautele necessarie ai fini della sua conservazione e non alterazione. Non solo, negli ultimi anni sono stati creati e perfezionati standard internazionali operativi quali lo ISO/IEC 27037:2012, ed i successivi e più recenti standard ISO/IEC 27041:2015, ISO/IEC 27042:2015 e ISO/IEC 27043:2015 che hanno progressivamente elevato le *best practice* operative dando valenza scientifica a questa attività di ricerca.

Molte criticità tuttavia sono ancora presenti, in *primis* la mancanza di un protocollo operativo che almeno in ambito nazionale possa uniformare tutte le attività di sequestro, analisi e ricerca della prova digitale, nonché l'archiviazione della stessa, svolte dalla Polizia Giudiziaria. La realtà operativa ci svela che successivamente al loro sequestro i supporti informatici dopo essere stati impacchettati e sigillati vengono troppo spesso conservati in luoghi non idonei alla loro conservazione, quali ad esempio locali adibiti a deposito presenti nei vari uffici di Polizia Giudiziaria; la loro eventuale analisi demandata per ogni singolo caso ad un diverso Consulente Tecnico, ciascuno con i propri tempi e *modus operandi*, sicuramente non contribuiscono a rendere certi i tempi, i costi e soprattutto il rigoroso rispetto delle modalità operative e l'applicazione ad ogni singolo caso dei più elevati e rigorosi standard tecnici ed operativi.

Attraverso il progetto *ForensicStorage* ed in particolare con la *web application ForensicWeb*, si è inteso proporre un nuovo scenario operativo definendo le possibilità tecniche al fine di realizzare un nuovo protocollo operativo versatile e di facile utilizzo da mettere a disposizione dell'A.G. e della P.G. finalizzato a consentire il prosieguo dell'attività d'indagine in tempi molto rapidi e con un notevole contenimento dei costi di giustizia rispetto ad una normale CTU.

Si è voluto creare un ambiente di lavoro favorevole e accessibile a qualsiasi operatore di giustizia, anche se sprovvisti di particolari conoscenze tecniche ed

informatiche, offrendo loro la possibilità di visionare contenuti di supporti digitali, acquisiti e memorizzati conformemente a quanto previsto dalla nuova normativa e nel rispetto degli standard operativi più recenti.

Il progetto, come si è avuto modo di rappresentare, permette la virtualizzazione dei contenuti dei supporti informatici di ogni tipo e dimensione e la visualizzazione dei contenuti presenti, e nella modalità *recovery* anche quelli precedentemente cancellati dall'utente. Le informazioni ed i *file* così recuperati possono essere fruiti e consultati in tutta sicurezza dall'Autorità Giudiziaria, dalla Polizia Giudiziaria delle rispettive postazioni di lavoro certificate.

Permettendo in tal guisa una disponibilità pressoché immediata da parte degli organi inquirenti con le più ampie garanzie rispetto all'autenticità e genuinità della prova informatica, della ripetibilità delle operazioni svolte e nel pieno rispetto dell'attuale normativa *privacy*, tutto questo a costi ridotti e prestabiliti che inevitabilmente una volta ammortizzato il costo di impianto potranno beneficiare delle conseguenti economie di scala nella gestione operativa.

Lo scrivente auspica che l'adozione del progetto *ForensicStorage*, o un analogo progetto possano presto portare alla creazione di protocolli operativi più efficienti, sicuri e finalmente all'altezza degli standard operativi richiesti.

Bibliografia

S. ALLEGREZZA *"Le misure coercitive nelle* «Model Rules for the Procedure of the European Public Prosecutor's Office»", in F. RUGGIERI, T. RAFARACI, G. Di PAOLO, S. MARCOLINI, R. BELFIORE, (a cura di), *Processo penale, lingua ed Unione Europea,* Padova, 2013.

R. ANGELETTI, *"La costruzione e la valutazione della prova penale",* Torino, 2012.

C. ALTHEIDE, H. CARVEY, *Digital Forensics with Open Source Tools,* Elsevier, Waltham, 2011.

A. C. AMATO, G. SARACENI, *I Reati Informatici. Elementi di teoria generale e principali figure criminose*, Giappichelli Editore, Torino, 2015.

E. APRILE, F. SPIEZIA, *Le intercettazioni telefoniche ed ambientali. Innovazioni tecnologiche e nuove questioni giuridiche,* Giuffrè Editore, Milano, 2004.

S. ATERNO, *La computer forensics tra teoria e prassi,* in *Ciberspazio e diritto,* Mucchi Editore, 2006.

S. ATERNO, F. CAJANI, G. COSTABILE, M. MATTIUCCI, G. MAZZARACO, "*Computer forensics e indagini digitali, Manuale tecnico giuridico e casi pratici*", Vol. II, Edizioni Experta, 2012.

S. BATTIATO, G. MESSINA, S. RIZZO, Im*age Forensics. Contraffazione Digitale e identificazione della camera d'acquisizione: status e prospettive,* Forlì, in IISFA Memberbook, Experta Edizioni, Forlì, 2009.

D. BIANCHI, *Internet e il danno alla persona. I casi e le ipotesi risarcitorie,* Giappichelli Editore, Torino, 2012.

A. BONOMO, "*I nuovi strumenti di comunicazione telematica ed informatica: aspetti tecnici e questioni giuridiche*", Roma, 2011.

M. BOZZETTI, P. POZZI, *L'Osservatorio FTI - Sicurforum Italia sulla Criminalità ICT (OCI),* in *Cyberwar o sicurezza? II Osservatorio Criminalità ICT,* a cura di M. BOZZETTI, P. POZZI, Franco Angeli, Milano, 2000.

R. BORRUSO, G. BUONOMO, G. CORASANITI, G. D'AIETTI, *Profili penali dell'informatica*, Giuffré Editore, Milano, 1994.

F. BRAVO, *"Indagini informatiche e acquisizione della prova nel processo penale"* in Rivista di Criminologia, Vittimologia e Sicurezza Vol. III - n. 3, Vol. IV - n. l - Settembre 2009-Aprile 2010, p.235.

F. BRUGALETTA, F. M. LANDOLFI (a cura di), *Il Diritto nel Cyberspazio,* Edizioni Simone, Napoli, 1999.

D. BUSO, *La rete Internet come strumento di investigazione nel contesto della criminalità informatica*, Corso di formazione dirigenziale.

A. CAMON, *Le intercettazioni nel processo penale*, Giuffrè Editore, Milano, 1996.

S. CARNEVALE, *"Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare"*, in Diritto penale e processo, 2009, pp. 469 ss.

E. CASEY, *Digital evidence and computer crime*, Elsevier Academic Press, 2004.

L. CHIRIZZI, *Computer Forensic, la ricerca della fonte di prova informatica*, Laurus Robuffo, Roma, 2006, p. 20.

C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, CEDAM, Padova, 2007.

F. CORDERO, *Prove illecite*, in *Tre studi sulle prove penali*, Giuffrè Editore, Milano, 1963, p. 149.

G. COSTABILE, *Computer forensics e informatica investigativa alla luce della Legge n.48 del 2008*, in Cyberspazio e diritto, Vol. XI, n.3, 2010, p.477.

D. D'AGOSTINI, *Diritto Penale dell'Informatica - dai computer crimes alla digital forensics*, Rimini, 2007.

D. D'AGOSTINI, Le indagini sulle *reti informatiche*, in *Diritto penale dell'informatica*, Experta Edizioni, Forlì, 2007.

D. D'AGOSTINI, *Diritto penale dell'informatica, dai computer crimes alla digital forensic*, Experta Edizioni, Forlì, 2007.

G. D'AIUTO, L. LEVITA, *I reati informatici. Disciplina sostanziale e questioni processuali*, Giuffrè Editore, Milano, 2012.

M. DANIELE, *La prova digitale nel processo penale*, Rivista di diritto processuale Anno LXVI (seconda serie) – N.2, CEDAM, Bologna, 2011.

C. DELLE FAVE, *Manuale di Polizia Giudiziaria. Procedure, atti da redigere, modalità operative*, Maggioli Editore, Rimini, 2013.

D. DE NATALE, *Responsabilità penale dell'internet service provider per omesso impedimento e per concorso nel reato di pedopornografia*, in GRASSO, SICURELLA (a cura di), Lezioni di Diritto Penale Europeo, Giuffrè Editore, 2007.

V.S. DESTITO, G. DEZZANI, C. SANTORIELLO, *Il diritto penale delle nuove tecnologie*, Cedam, Padova, 2007.

G.T. ELMI, *Corso di Informatica Giuridica*, III Ed., Simone Editore, Napoli, 2010.

G. FAGGIOLI, *Computer crimes*, Giuridiche Simone, Napoli, 1998.

L. FILIPPI, *L'intercettazione di comunicazioni,* Giuffrè Editore, Milano, 1997.

L. FILIPPI, *Gli impianti utilizzabili*, in P. FERRUA, E. MARZADURI, G. SPANGHER, (a cura di), *La prova penale*, Torino, 2012.

G. FINOCCHIARO, F. DELFINI, *Diritto dell'Informatica*, UTET, Wolters Kluwer, Milano, 2014.

R. FLOR, *"Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht del 27 febbraio 2008 sulla c.d. Online Durchsuchung. La prospettiva delle investigazioni ad alto contenuto tecnologico ed il bilanciamento con* i *diritti inviolabili della persona. Aspetti di diritto penale sostanziale",* in Riv. trim. Dir. Pen. Enc., 3, 2009, p.695 ss.

R. FLOR, *"Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di Internet",* in Diritto Penale Contemporaneo, 2010, p.4.

R. FLOR, *"La Corte di giustizia considera la direttiva europea 2006124/CE sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?",* in Diritto penale contemporaneo, 28 aprile 2014, p.3.

E. FLORINDI, *Computer e Diritto. L'informatica giuridica nella società dell'informazione e della conoscenza*, Giuffrè Editore, Milano, 2012.

N. GALATINI, voce *"Inutilizzabilità"* (Dir. Proc. Pen.), in Enc. Dir., I Aggiornamento, Milano, 1998, p. 690.

P. GALDIERI, *Teoria e pratica nell'interpretazione del reato informatico,* Giuffrè Editore, Milano, 1997.

D. GABRINI, P. PERRI, G. SPECCHIO *Live forensics. In:* A. ATTANASIO, G. COSTABILE, eds. *IISFA Memberbook,* Experta Edizioni, Forlì, 2011.

C. P. GARRISON, *Digital Forensics for Network, Internet, and Cloud Computing*, Syngress, 2010.

A. GHIRARDINI, G. FAGGIOLI, *Digital Forensics,* Apogeo, Milano, 2013.

A. GHIRARDINI, G. FAGGIOLI, *Computer Forensics,* Apogeo, Milano, 2010.

E. GIANNANTONIO, *Manuale di diritto dell'informatica,* Cedam, Padova, 1994.

C. GIUSTOZZI, *"Il malware di stato"* in Riv. Elettronica di Diritto, Economia, Management, n.3 - 2013, p.p. 194 ss.

V. GREVI, *"Appunti in tema di intercettazioni telefoniche operate dalla polizia giudiziaria",* in Riv. it. Dir. Proc. Pen., 1967, p. 724.

M. IASELLI, *Compendio di Informatica Giuridica*, V Ed., Simone Editore, Napoli, 2012.

G. ILLUMINATI, *La disciplina processuale delle intercettazioni*, Giuffrè Editore, Milano, 1983.

S. IPPOLITO, *Informatica, internet e diritto penale*, III ed., Giuffrè Editore, Milano, 2010.

F. IZZO, *Norme contro la pedofilia, Commento alla L. 269/98*, Giuridiche Simone, Napoli, 1998.

T. A. JOHNSON, *Forensic Computer Crime Investigation*, Taylor & Francis, 2005.

O. KERR, *Searches and Seizures in a digital world*, in Harvard Law Review, 2005, Vol. 119.

J.F. KOROSE, K.W. ROSS, *La sicurezza nelle reti,* in *Reti di calcolatori e internet,* Pearson Addison Wesley, Milano, 2005.

J. LEIGHTON JOHN, *Digital Forensics and Preservation*, Digital Preservation Coalition, 2012.

G. LOCATELLI, G. SARNO, *Gli atti di investigazione difensiva nel procedimento penale,* CEDAM, Padova, 2006.

A. LOGLI, *"Commento alla sentenza n°753/2007"*, in Cass. Pen., 7-8, 2008 pagg. 2956-2957.

E. LORENZETTO, *"Le attività urgenti di investigazione informatica e telematica" in Sistema penale e criminalità informatica"* a cura di L. LUPARIA, Giuffrè Editore, Milano, 2009.

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

L. LUPARIA, *"La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Legge 18 marzo 2008, n. 48"*, in Dir. Penale e processo, 6, 2008, p. 670.

C. MAIOLI, "*Dar voce alle prove: elementi di informatica forense*", in *Crimine virtuale, minaccia reale*, a cura di P. POZZI, R. MASOTTI e M. BOZZETTI, Franco Angeli, 2004.

C. MAIOLI, R. CUGNASCO, *Profili normativi e tecnici delle intercettazioni. Dai sistemi analogici al voice over IP*, Gedit Edizioni, Bologna, 2008.

C. MAIOLI, *Questioni di Informatica Forense*, Aracne Editore, Roma, 2015.

M. MANZIN, *"Del contraddittorio come principio e come metodo; ID., Avvocati custodi del processo: alle radici della deontologia forense"*, in M. MANZIN, P. MORO, (a cura di) *Retorica e deontologia* forense, Giuffrè Editore, Milano, 2010.

L. MARAFIOTI, *"Digital evidence e processo penale"* in Rivista Giuridica DeJure Giuffrè Editore.

D. MINOTTI, *I reati commessi su internet, in Internet nuovi problemi e questioni controverse*, a cura di G. CASSANO, Giuffrè Editore, Milano, 2001.

M. MONTAGNA, *"La giustizia penale differenziata"*, G. SPANGHER, A. GAITO, (a cura di), Tomo III, Giappichelli Editore, Torino, 2011, p.77.

A. MONTI, *"No ai sequestri indiscriminati di computer"*, in Diritto dell'Internet, 3, 2007, p. 268.

M. G. NOBLETT, M. M. POLLITT, L. A. PRESLEY, *Recovering and Examining Computer Forensic Evidence*, «Forensic Science Communications», 2000.

F. NOVARIO, *Le Prove Informatiche nel processo civile*, Giappichelli Editore, Torino, 2014.

R. ORLANDI, *"Questioni attuali in tema di processo penale e informatica"*, in Riv. Dir. e Proc. Pen., 2009, p.129.

F. C. PALAZZO, *"I confini della tutela penale: selezione dei beni e criteri di criminalizzazione"* in Riv. Dir. e Proc. Pen, 1992, p.453 ss.

M. PALMIRANI, M. MARTONI, *Informatica giuridica per le relazioni aziendali*, Giappichelli Editore, Torino, 2012.

C. PECORELLA, *"Diritto penale dell'informatica"*, CEDAM, Padova, 2006.

C. PECORELLA, R. DE PONTI, *"Impiego dell'elaboratore sul luogo di lavoro e tutela penale della privacy"*, www.penalecontemporaneo.it, 2011.

G. POMANTE, *Internet e criminalità*, Giappichelli Editore, Torino, 1999.

E. QUAYLE, M. TAYLOR, *Child Pornography - An Internet Crime*. Brunner – Routledge Publisher, 2003.

E. QUAYLE, M. TAYLOR, *Viewing Child Pornography on the Internet: Understanding the offence, managing the offender, helping the victims*, Lyme Regis, Russell House Publishing, 2005.

U. RAPETTO, D. MANCINI, *Novità legislative in materia di Crimine Informatico*, Roma, 2008.

S. RODOTA', *Il mondo nella rete. Quali i diritti, quali i vincoli,* Laterza, Roma – Bari, 2014.

A. E. RICCI, *"Digital evidence e irripetibilità delle operazioni acquisitive"*, in Dir. Pen. Proc., 2010, 3, p.p. 343 e ss.

T. SAMMES, B. JENKINSON, *Forensic Computing*, Springer, 2007.

G. SARTOR, *Corso d'informatica giuridica*, Vol. I, Giappichelli Editore, Torino, 2008.

G. SARTOR, "*The Nature of Legal Concepts: Inferential Nodes or Ontological Categories*", in: Proceeding of the Conference on "*Approaching the Multilanguage Complexity of European Law: Methodologies in Comparison*", a cura di G. AJANI, G. PERUGINELLI, G. SARTOR e D. TISCORNIA, Firenze: European Press Academic Publishing, 2007.

C. SARZANA, *Informatica e diritto penale*, Giuffrè Editore, Milano, 1994.

C. SARZANA, *"La criminalità informatica: aspetti processuali"* in Quaderni del C.S.M., 1994, p. 348.

C. SERRA: *Pedofilia e Internet: caratteristiche e spunti di ricerca*, Rivista Minori giustizia, Franco Angeli Editore, 2001.

O. SIGNORILE, *Computer Forensics Guidelines: un approccio metodico procedurale per l'acquisizione e l'analisi della digital evidence,* in *Ciberspazio e Diritto,* Enrico Mucchi Editore, Modena, 2009.

D. SIRACUSANO, A. GALATI, G. TRANCHINA, E. ZAPPALA, *Diritto processuale penale*, Giuffrè Editore, Milano, 1996.

M. SOFFIENTINI, *Privacy. Protezione e trattamento dei dati*, IPSOA Manuali, Wolters Kluwer, Milano, 2015.

G. SPANGHER, *"Trattato di Procedura Penale"*, in Giulio Garuti (a cura di), Modelli differenziati di accertamento, Vol. VII, UTET, Torino, 2011.

A. TESTAGUZZA, *Digital Forensics. Informatica giuridica e processo penale*, CEDAM, Bologna, 2015.

M. TONELLOTTO, *Computer forensics: l'acquisizione della prova informatica*, Edizioni Accademiche Italiane, 2015.

P. TONINI, *La prova penale*, CEDAM, Padova, 2000.

P. TONINI, *Manuale di procedura penale*, Giuffrè Editore, Milano, 2004.

P. TONINI, *"Documento informatico e giusto processo"*, in Diritto Penale e Processo, 2009, pp. 406 e ss.

J. VACCA, *Computer forensics. Computer Crime Scene Investigation*. Charles River Media, Boston, 2005.

G. VACIAGO, *Digital Evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Giappichelli Editore, Torino, 2012.

F. ZACCHÉ, *La prova documentale*, in G. UBERTIS, G.P. VOENA (diretto da), *Trattato di procedura penale*, vol. XIX, Giuffrè Editore, Milano, 2012.

F. ZACCHÉ, *"L'acquisizione della posta elettronica nel processo penale"*, in Processo Penale e giustizia, Anno III, n.4, 2013.

S. ZANERO, E. HUEBNER, *The Case for Open Source Software in Digital Forensics,* in *Open Source Software for Digital Forensics,* Springer, Berlino, 2010.

G. ZICCARDI, *Manuale breve Informatica Giuridica,* Giuffrè Editore, Milano, 2006.

G. ZICCARDI, *Privacy, sicurezza informatica, computer forensics e investigazioni digitali,* Tomo II, Seconda Edizione, Giuffrè Editore, Milano, 2011.

G. ZICCARDI, *Informatica giuridica, privacy, sicurezza informatica, computer forensics e investigazioni digitali,* Giuffrè Editore, Milano, 2012.

G. ZICCARDI, *Internet, controllo e libertà,* Raffaello Cortina Editore, Milano, 2015.

G. ZICCARDI, *Il computer e il giurista*, Giuffrè Editore, Milano, 2015.

Sitografia

- http://www.idc.com
- https://it.wikipedia.org/wiki/Cracker_%28informatica%29
- https://it.wikipedia.org/wiki/Phishing
- http://www.legislation.gov.uk/ukpga/2003/42/contents
- http://www.poliziadistato.it/articolo/23399/
- http://www.osservatoriopedofilia.gov.it/
- http://www.minori.it/sites/default/files/direttiva_europea_13dic2011.pdf
- http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:32011L0093
- http://www.interlex.it/testi/giurisprudenza/ch060530.htm
- http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF
- http://www.pcmag.com/article2/0,2817,2341476,00.asp
- https://www.sec.gov/about/laws/soa2002.pdf
- http://epic.org/privacy/intl/data_retention.html
- https://www.eff.org/deeplinks/2010/03/beginning-end-data-retention
- http://www.wired.com/threatlevel/2008/03/times-reporter
- http://www.mixminion.net/minion-design.pdf
- http://www.torproject.org/index.html
- http://pws.winstonsmith.info
- http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2014.pdf
- https://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf
- http://www.ictlex.net/?p=459
- http://www.cftt.nist.gov/disk_imaging.htm
- http://www.nannibassetti.com/dblog/articolo.asp?articolo=12
- http://www.ictlex.net/?p=516
- http://www.ictlex.net/?p= 692
- http://www.scintlex.it/database/notizie/notizia_pdf.php?id=241
- https://www.law.cornell.edu/rules/frcrmp/rule_41
- http://www.penale.it/page.asp?mode=l&IDPag=72
- http://sig.umd.edu/publications/Swaminathan_TIFS_200803.pdf
- https://www.utica.edu/academic/institutes/ecii/publications/articles/B49F9C4A-0362-765C-6A235CB8ABDFACFF.pdf
- http://documents.mx/documents/karamatli-modern-botnets.html
- http://www.penale.it/giuris/meri_161.htm
- http://www.blackhat.com/presentations/bh-dc-07/Rutkowska/Presentation/bh-dc-07-Rutkowska-up.pdf
- http://conventions.coe.int/treaty/en/reports/html/185.htm
- http://www.ictlex.net/?p=889
- http://www.ictlex.net/?p=626
- http://www.ictlex.net/?p=119
- http://jolt.richmond.edu/v10i5/article52.pdf
- http://www.interlex.it/testi/giurisprudenza/ve050331.htm
- http://www.interlex.it/regole/tribvebz.htm
- http://www.penale.it/page.asp?mode=1&idpag=764

- http://www.ictlex.net/?p=889
- http://www.ictlex.net/?p=566
- http://www.gdf.gov.it/reparti-del-corpo/territorio/lazio/roma/nucleo-speciale-frodi-telematiche.
- http://www.carabinieri.it/arma/oggi/reparti/organizzazione-mobile-e-speciale/ros
- http://www.poliziadistato.it/articolo/23393-Polizia_postale_e_delle_comunicazioni/
- http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.63.7643&rep=rep1&type=pdf
- http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf
- http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf
- http://www.cs.princeton.edu/courses/archive/fall08/cos521/hash.pdf
- https://eprint.iacr.org/2006/105
- http://www.nightgaunt.org/testi/interlex/sha1.htm
- http://recordmydesktop.sourceforge.net/about.php
- http://www.pewinternet.org/2010/06/11/the-future-of-cloud-computing
- http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.
- http://www.infoworld.com/article/2649377/security/debate-rages-over-german-government-spyware-plan.html
- http://www.wired.com/2007/07/fbi-spyware
- https://www.wired.com/2009/04/fbi-spyware-pro/#ixzz0vH9IUa6v
- http://www.theregister.co.uk/2007/03/07/wiretap_trends_ss8
- http://www.dagospia.com/rubrica-3/politica/girone-dantesco-intercettazioni-2009-2013-procura-80146.htm.
- http://www.uscourts.gov/statistics-reports/wiretap-report-2014
- http://www.eff.org/issues/calea?f=summary.html
- https://www.giustizia.it/giustizia/it/mg_1_2_1.wp?facetNode_1=1_8%282008%29&facetNode_2=1_8%28200811%29&previsiousPage=mg_1_2&contentId=SAN47260
- https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df
- http://www.anagram.com/berson/skyeval.pdf
- http://www.embedded-solutions.at/en/
- http://papers.ssrn.com/sol3/papers.cfm?abstract_id=317501
- https://www.wireshark.org/
- http://www.tcpdump.org
- http://chaosreader.sourceforge.net
- http://ettercap.github.io/ettercap/
- http://www.scopemed.org/?mno=170752
- http://www.colorado.edu/policylab/Papers/Secure_Voip_writeup%20v3_2%20_2_.pdf
- http://www.oecd.org/internet/ieconomy/guidelinesforcryptographypolicy.htm
- http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf
- http://voipcallrecording.com/
- http://csrc.nist.gov/index.html
- http://www.altalex.com/index.php ?idnot=9407

- https://www.emc.com/collateral/analyst-reports/idc-digital-universe-2014.pdf
- http://www.camera.it/parlam/leggi/08048l.htm
- http://www.agid.gov.it/
- http://www.dm.unibo.it/~maioli/docs/fti_informatica_3009.doc
- http://en.wikipedia.org/wiki/Chain_of_custody
- http://www.lepida.it/
- http://www.google.it/enterprise/gsa/
- http://www.forensicswiki.org/wiki/Forensic_file_formats
- http://www.guidancesoftware.com
- http://www.ijdc.net/index.php/ijdc/article/viewFile/217/286
- http://www.dm.unibo.it/~maioli/docs/wisp2006.pdf
- http://www.edrm.net
- https://www.raspberrypi.org/products/raspberry-pi-3-model-b/

Normative

Costituzione Italiana.
https://www.senato.it/documenti/repository/istituzione/costituzione.pdf

Legge n. 98 del 1974 (Protezione libertà individuale).
https://www.blia.it/leggiditalia/?a=1974&id=98

Legge 23 dicembre 1993, n. 547 (Modificazioni ed integrazioni delle norme del codice penale e del codice di procedura penale in tema di criminalità informatica).
http://www.interlex.it/testi/l547_93.htm

Legge n. 48 del 18 marzo 2008. (Ratifica Convenzione del Consiglio d'Europa).
http://www.parlamento.it/parlam/leggi/08048l.htm

D.Lgs. 21 novembre 2007, n. 231 (Normativa sull'antiriciclaggio).
http://www.camera.it/parlam/leggi/deleghe/07231dl.htm

D.Lgs. 29 dicembre 1992 n. 518 (Tutela dei programmi per elaboratore).
http://www.interlex.it/testi/dl518_92.htm

Raccomandazione numero 9 del 1989 del Consiglio d'Europa.
http://www.privacy.it/CER-89-2.html

D.Lgs. 1° settembre 1993, n. 385 (Testo Unico Leggi in materia Bancaria e Creditizia).
http://www.consob.it/main/documenti/Regolamentazione/normativa_ln/dlgs385_1993.htm

D.Lgs. 7 marzo 2005 n. 82 (Codice dell'Amministrazione digitale).
http://www.camera.it/parlam/leggi/deleghe/05082dl.htm

Raccomandazione Consiglio d'Europa del 1989.
http://www.privacy.it/CER-89-2.html

Legge 15 febbraio 1996, n. 66 (Norme contro la violenza sessuale).
http://www.salute.gov.it/imgs/C_17_normativa_1557_allegato.pdf

Legge 3 agosto 1998 n. 269 (Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù).
http://www.camera.it/parlam/leggi/98269l.htm

Legge 6 febbraio 2006 n. 38 (Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet).
http://www.camera.it/parlam/leggi/06038l.htm

Legge 1 ottobre 2012 n. 172 (Ratifica ed esecuzione della Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e l'abuso sessuale, fatta a Lanzarote il 25 ottobre 2007).

http://www.penale.it/page.asp?IDPag=1087

Direttiva UE 2011/93/UE del 13 dicembre 2011 (Nuove norme contro l'abuso, lo sfruttamento sessuale dei minori e la pornografia minorile).

http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:IT:PDF

Direttiva UE 2004/68/GAI del 22 dicembre 2003 (relativo alla lotta contro lo sfruttamento sessuale dei bambini e la pornografia infantile).

http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=URISERV%3Al33138

Direttiva UE 06/24/CE del 15 marzo 2006.

D.Lgs. 30 maggio 2008, n. 109.

http://www.parlamento.it/parlam/leggi/deleghe/08109dl.htm

Legge 22 aprile 1941 n. 633 (Protezione del diritto d'autore e di altri diritti connessi al suo esercizio).

http://www.interlex.it/testi/l41_633.htm

Explanatory Report della Convenzione sul Cybercrime.

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b

Convenzione Europea per la tutela dei diritti dell'uomo e delle libertà fondamentali del 4 novembre 1950.

http://www.echr.coe.int/Documents/Convention_ITA.pdf

D.D.L. Ratifica ed esecuzione degli Accordi di estradizione e sulla mutua assistenza giudiziaria tra Stati Uniti e U.E. del 25 giugno 2003.

http://www.gazzettaufficiale.it/eli/id/2009/03/27/009G0034/sg;jsessionid=vE1rb1BwK36x7I504En4bg__.ntc-as2-guri2a

Legge 16 marzo 2009, n. 25 Ratifica ed esecuzione degli Accordi di estradizione e sulla mutua assistenza giudiziaria tra Stati Uniti e U.E. del 25 giugno 2003.

http://www.camera.it/parlam/leggi/09025l.htm

Disegno di Legge n. 4599 recante "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet" presentato il 13 gennaio 2004.

http://www.senato.it/leg/14/BGT/Schede/Ddliter/20826.htm

Legge 31 dicembre 1996, n. 675 (Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali).

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/28335

D.Lgs. 30 giugno 2003 n. 196 (Testo Unico in materia di protezione dei dati personali).

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248

Direttiva 95/46/CE (Tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/432175

Legge 30 settembre 1993 n. 388 (Accordo di Schengen, eliminazione graduale dei controlli alle frontiere comuni).

http://www.camera.it/bicamerali/schengen/fonti/legge388.htm

Testo Unico in Materia di Protezione dei Dati Personali, comunemente denominato «Codice della Privacy», del 27 giugno 2003, che ha recepito le norme previste dalla Direttiva.

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1311248

Direttiva n. 2002/58/CE del 12 luglio 2002 (Trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche).

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/35284

D.Lgs. 11 maggio 1999 n. 135 (Disposizioni integrative della Legge 31 dicembre 1996, n. 675, sul trattamento di dati sensibili da parte di enti pubblici).

http://www.lexitalia.it/leggi/dlvo_1999-135.htm

Legge 7 agosto 1990, n. 241 (Nuove norme sul procedimento amministrativo).

http://www.bosettiegatti.eu/info/norme/statali/1990_0241.htm

Legge 25 maggio 1970 n. 300 (Statuto dei Lavoratori, Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e nell'attività sindacale nei luoghi di lavoro e norme sul collocamento).

http://www.comune.jesi.an.it/MV/leggi/l300-70.htm

Direttiva 97/66/CE del 15 dicembre 1997 (sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni).

http://www.interlex.it/testi/97_66ce.htm

D.Lgs. 13 maggio 1998 n. 171.

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/46056

Direttiva 2002/58/CE del 12 luglio 2002 (sul trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche).

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/35284

Counterfeit Access Device and Computer Fraud and Abuse, U.S.A. 1984.
https://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_%28CFAA%29

The Internet Safety Act 2009 U.S.A. del 14 maggio 2009.
http://thomas.loc.gov/cgi-bin/query/z?c111:S.1047:

Sarbanes Oxley Act 2002 U.S.A. del 30 luglio 2002.
https://www.sec.gov/about/laws/soa2002.pdf

Sexual Offences Act del 2003.
http://www.legislation.gov.uk/ukpga/2003/42/pdfs/ukpga_20030042_en.pdf

Rule 41 Federal Rules of Criminal Procedure (Search and Seizure).
https://www.law.cornell.edu/rules/frcrmp/rule_41

Title 18 U.S.C. §§ 2701-12 Stored Communication Act.
https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121

The Stored Communications Act (SCA, codified at 18 U.S.C. Chapter 121 §§ 2701–2712.
https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121

Electronic Communications Privacy Act, 18 U.S.C. § 2510 del 1986.
https://it.ojp.gov/privacyliberty/authorities/statutes/1285

Stored Communications Act, 18 U.S.C. § 2701.
https://www.law.cornell.edu/uscode/text/18/2701

Pen Register Act, 18 U.S.C. § 206.
https://www.law.cornell.edu/uscode/text/18/part-II/chapter-206

Foreign Intelligence Surveillance Act (50 U.S.C. § 1801-1885C).
https://www.law.cornell.edu/uscode/text/50/chapter-36

Giurisprudenza