Alma Mater Studiorum – Università di Bologna

DOTTORATO DI RICERCA IN

DIRITTO E NUOVE TECNOLOGIE

Ciclo XXVI

Settore Concorsuale di afferenza: 12/H3

Settore Scientifico disciplinare: IUS/20

Indagini forensi in tema di scambio di file pedopornografici mediante software di file sharing a mezzo peer-to-peer

Presentata da: Michele Ferrazzano

Coordinatore Dottorato
Prof. Giovanni Sartor

Relatore
Prof. Cesare Maioli

Esame finale anno 2014

Introduzione

Vedendo un qualsiasi telegiornale, ascoltando un radiogiornale, leggendo un quotidiano cartaceo o online si nota come stia sempre crescendo il dato relativo alle indagini e ai processi che negli ultimi anni hanno visto il ricorso a prove in formato digitale[1].

Cybercrime è il termine che gli anglosassoni usano per indicare i crimini che coinvolgono sistemi informatici; più precisamente è possibile identificare due categorie relativi ai crimini informatici:

- crimini per i quali i sistemi informatici o telematici[2] sono l'oggetto dell'offesa[3];
- crimini per i quali i sistemi informatici o di telecomunicazione sono lo strumento dell'azione criminale; più precisamente lo strumento tecnologico è utilizzato per "ingannare" l'utente[4] oppure per "agevolare" la commissione di un illecito[5].

[1] Per citare alcuni tra i casi che hanno avuto maggiore attenzione mediatica e che hanno richiesto l'impiego di tecniche di informatica forense, si pensi al caso dell'omicidio del prof. Marco Biagi a Bologna nel 2002 per il quale è stata necessaria una complessa opera di ricostruzioni di rapporti tra i terroristi mediante l'analisi dei tabulati del traffico telefonico e l'analisi di due palmari Psion ritrovati in possesso della terrorista Lioce un anno dopo, o al caso dell'omicidio di Chiara Poggi a Garlasco nel 2007 dove il computer del fidanzato Alberto Stasi è entrato nel processo al fine di dimostrare l'alibi dell'uomo secondo il quale durante le ore dell'omicidio era impegnato nella scrittura della tesi.

[2] La dizione "sistema informatico o telematico" è utilizzata per indicare in maniera generica qualsiasi genere di strumento informatico (computer, telefoni cellulari, dispositivi di memorizzazione, lavatrici...). Nella Convenzione di Budapest, all'art. 1 viene definito 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".

[3] Un esempio di crimine per il quale oggetto dell'offesa è un sistema informatico o telematico è l'infezione con virus o worm. Il primo processo in Italia per un caso di danneggiamento di sistema informatico causato da un virus informatico è il cosiddetto "caso Vierika", Tribunale Penale di Bologna, Sez. I Monocratica, Sentenza 21 luglio 2005 (e appello, Corte di Appello di Bologna, Sezione II Penale, Sentenza 30 gennaio 2008).

[4] Un esempio è il fenomeno del phishing, fenomeno di social engineering che tramite invio da parte di ignoti truffatori di messaggi di posta elettronica ingannevoli, spinge le vittime a fornire volontariamente informazioni personali quali, ad esempio, dati di carte di credito. Sul tema *cfr*. Cajani F., Costabile G., Mazzaraco G. (2008) *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria*. Giuffrè.

[5] Un esempio è il caso della copia di dati riservati protetti da proprietà intellettuale dai server aziendali per porre in essere pratiche di concorrenza sleale.

Nell'ultimo ventennio si sta assistendo ad una vera e propria deflagrazione dei reati informatici[6], sebbene la materia sia ancora ostica per molti operatori del diritto. I reati informatici sono di difficile ricostruzione non essendo chiaro quanti siano gli autori e da dove agiscano, spesso sono difficili da rintracciare e, anche quando questo dovesse accadere, può risultare complesso capire quante volte un'azione è stata commessa e quali siano tutte le vittime[7].

Più in generale, la prova informatica entra in gioco ormai nella quasi totalità dei processi (tanto penali quanto civili) in ragione del fatto che un sistema informatico è, banalmente, un mero contenitore di dati digitali e dunque di potenziali prove in formato digitali: in tutti i casi di omicidio si ricorre ai tabulati telefonici per la geolocalizzazione delle persone che sono memorizzati presso i server delle compagnie di telefonia mobile, in tutti i casi di rapina si ricorre alle registrazioni delle telecamere a circuito chiuso che sono memorizzate su supporti informatici e così via.

Una ricerca condotta da IISFA[8] nel 2012 ha evidenziato come più della metà dei reati informatici riguarda l'accesso abusivo a sistema informatico, l'infedeltà aziendale (che spesso si traduce in un accesso abusivo a sistema informatico al fine di rubare segreti industriali) e reati di pedopornografia commessi mediante l'uso di client di file sharing su rete peer-to-peer[9].

Entra dunque in gioco la più giovane tra le scienze forensi, l'informatica forense, che tratta la conservazione, identificazione, estrazione e documentazione della prova informatica. Come ogni altra scienza forense, la computer forensics riguarda l'uso di sofisticati strumenti tecnologici e procedure che devono essere seguite per garantire la conservazione della prova

[6] Braghò G. (2004) Le indagini in materia di reati informatici. In Pozzi P., Masotti R., Bozzetti M., eds. *Crimine virtuale, minaccia reale. ICT Security: politiche e strumenti di prevenzione*, Franco Angeli, 33–43.

[7] Walden I. (2007) *Computer crimes and digital investigations*. Oxford University Press.

[8] L'IISFA (International Information System Forensics Association) è un'associazione di professionisti del settore della computer forensics (giuristi, forze dell'ordine e tecnici) riconosciuta a livello internazionale (*http://www.iisfa.org/*), il cui scopo primario è la promozione dello studio, della formulazione di metodi e di standard inerenti le attività di Computer Forensics. A tal proposito la sezione italiana dell'associazione (*http://www.iisfa.net/*) risulta essere particolarmente attiva, organizzando numerosi corsi di aggiornamento e seminari sia per giuristi che per tecnici: tra questi spicca l'evento annuale dell'IISFA Forum, durante il quale vengono presentati gli ultimi risultati di studi sul tema.

[9] Attanasio A., Cajani F., Costabile G., Vannini W. (2013) Lo stato dell'arte della computer forensics in Italia. *In:* Attanasio A., Costabile G., eds. *IISFA Memberbook 2012*. Experta. 123–151.

informatica e l'esattezza dei risultati riguardanti la sua elaborazione [10]. A livello generale si tratta di individuare le modalità migliori per acquisire le prove senza alterare o modificare il sistema informatico su cui si trovano e garantire che le prove acquisite su altro supporto siano identiche a quelle originarie[11]. Diversamente dalla sicurezza informatica che si occupa di proteggere a priori un sistema informatico, l'informatica forense agisce dopo che si è verificata la violazione o, in generale, che il sistema è stato coinvolto in maniera attiva o passiva in un reato; lo scopo è l'esame e la documentazione dei dati contenuti all'interno dei reperti informatici per ricostruire i fatti accaduti: un'analisi dettagliata permette di conoscere attività, gusti, pensiero dell'utilizzatore al fine di condurre le indagini nella giusta direzione ed acquisire prove inerenti a eventi legati alla vita del suo utilizzatore.

Dopo aver analizzato nel dettaglio gli aspetti metodologici e applicativi dell'informatica forense, questo lavoro si focalizzerà sui sistemi di file sharing a mezzo peer-to-peer, nati allo scopo di condividere e distribuire dati in maniera non necessariamente illecita: si pensi allo scambio delle distribuzioni Linux che avviene spesso utilizzando il protocollo BitTorrent.

La divulgazione di materiale pedopornografico o protetto dal diritto d'autore si realizza solitamente utilizzando software di file sharing a mezzo peer-to-peer[12]: attualmente, il client più popolare in Italia è eMule, un'applicazione open source disponibile per sistemi Windows ma con versioni analoghe anche per sistemi Linux e MacOS. In questi casi, e specialmente per quanto riguarda i casi di pedopornografia, l'analisi forense si propone di verificare se effettivamente l'utilizzatore del sistema abbia commesso il reato contestato: occorre cioè individuare i file scambiati e le modalità con le quali l'utente ha proceduto alla ricerca, allo scopo di determinare se il possesso di un particolare file sia consapevole o meno. Il mero recupero di dati da un supporto informatico è tuttavia solo la prima attività da compiere, dovendo poi ricostruire gli eventi che si sono verificati affinché quegli stessi dati trovati possano essere assunti come prova in formato digitale: nel caso specifico della

[10] Marcella A., Greenfield R. (2002) *Cyber Forensics: A Field Manual for collecting, examining and preserving Evidence of Computer Crimes*. Auerbach.

[11] Maioli C. (2004) Dar voce alle prove: elementi di informatica forense. *In:* Pozzi P., Masotti R., Bozzetti M. (eds.) *Crimine virtuale, minaccia reale. ICT Security: politiche e strumenti di prevenzione*. FrancoAngeli, 66–74.

[12] Fournier R., Latapy M., Magnien C. (2013) Quantifying paedophile activity in a large P2P system. In *Information Processing and Management*, 49(1). 248–263.

pedopornografia, bisogna dimostrare che la detenzione di materiale illecito è da ricondurre ad un'azione consapevole da parte dell'utente. Attualmente questo genere di analisi forensi sono condotte molto spesso in maniera superficiale, prendendo in esame solo i file a contenuto illecito e non considerando gli aspetti di consapevolezza. Inoltre, l'attività tecnica è eseguita in maniera completamente manuale e richiede molto tempo per essere portata a termine: a parte gli strumenti software generici (come EnCase[13] o Autopsy[14]), l'analista forense non dispone di tool specifici pertanto deve approfondire l'analisi determinando il tipo di client P2P utilizzato, individuando i file che contengono tracce delle attività che si sono verificate, associando i file che sono stati scaricati e/o divulgati tramite esso, spulciando le varie cartelle e diversi file. Non esistono molti strumenti software automatici specifici sviluppati al fine di agevolare la suddetta tipologia di analisi, e comunque gli unici tool sono di tipo commerciale: si consideri peraltro che alcuni client (tra cui lo stesso eMule) sono addirittura privi di log delle attività poste in essere sul sistema oggetto di analisi.

La tematica è di ampio interesse soprattutto in relazione al reato di pedopornografia per il quale il legislatore, tanto nazionale quanto comunitario, ha emanato diverse norme nell'ultimo decennio. A livello europeo la norma principe in tema di computer forensics è la Convenzione di Budapest dove al capitolo II titolo 3, l'art. 9 tratta di reati relativi alla pornografia minorile e invita gli stati membri a legiferare al fine di punire chi produce materiale pedopornografico allo scopo distribuirlo attraverso sistemi informatici e telematici, chi offre o rende disponibile materiale pedopornografico attraverso sistemi informatici e telematici, distribuisce o trasmette materiale pedopornografico attraverso sistemi informatici e telematici, si procura materiale pedopornografico attraverso sistemi informatici e telematici per sé o per altri, possiede materiale pedopornografico in sistemi informatici e telematici o su supporti di memorizzazione digitali. Per materiale pedopornografico si intende "materiale che mostra un minore (persona di età inferiore ai 18 anni) impegnato in atteggiamenti sessuali espliciti, un soggetto apparentemente minore impegnati in atteggiamenti sessuali espliciti, oppure immagini realistiche che rappresentano un minore impegnato in atteggiamenti sessuali espliciti". La convenzione di Budapest è stata poi ratificata anche in Italia con

[13] *https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx*.
[14] *http://www.sleuthkit.org/*.

la Legge n. 48 del 27 febbraio 2008 e il suddetto articolo ha trovato collocazione nel codice penale negli artt. 600-bis e seguenti.

Come è naturale pensare, la necessità di analizzare sistemi informatici coinvolti in traffico di materiale pedopornografico non è limitata all'Europa: proprio eMule è uno dei software maggiormente diffusi in Brasile e la Polizia Federale, con l'aiuto di alcuni esperti di computer forensics, ha sviluppato EspiaMule[15], un software che consente di ricercare in fase di monitoraggio della rete eDonkey (utilizzata appunto da eMule per la condivisione e lo scambio di file) gli utenti che sono in possesso di materiale illecito, agendo come una spia all'interno della rete di eMule. Lo sviluppo di un tool con queste finalità è stato facilitato dalla disponibilità di codice sorgente di eMule, pertanto la polizia dello stato sudamericano ha avuto modo di modificarne il codice sorgente al fine di filtrare ed identificare i computer contenenti file dal contenuto illecito in condivisione. Le informazioni ottenute relative ad utenti di paesi stranieri sono poi inviate all'Interpol (tra esse, sono identificati anche diverse migliaia di utenti italiani).

L'argomento trova inoltre interesse anche in ambito accademico: diversamente da quanto accade in Italia dove le tematiche relative all'informatica forense a livello accademico sono seguite solo in pochissimi atenei, in numerose università straniere gli studi sono approfonditi nelle aule dei dipartimenti di informatica dove si formano i tecnici. A proposito di pedopornografia, un progetto europeo guidato dal dipartimento d'informatica dell'Università svedese di Karlstad assieme ad altri partner europei denominato FIVES[16] si è prefisso di portare a termine per febbraio 2011 lo sviluppo di un applicativo software assolutamente indispensabile per queste tipologie di indagini che consenta di ridurre notevolmente tempo e risorse: l'applicazione, poggiandosi su un framework denominato OCFA Forensics[17], prevede di

[15] Fagundes P. (2009) Fighting Internet Child Pornography The Brazilian Experience. *Police Chief*, 76(9), 48–55. Edilton E., Souza J. (2009) EspiaMule e Wyoming ToolKit: Ferramentas de Repressão à Exploração Sexual Infanto-Juvenil em Redes Peer-to-Peer. In *Proceedings of the Fourth International Conference of Forensics Computer Science*. 108–113.

[16] Garcia J. (2009) FIVES and P2P-based Intelligence Gathering. In: Seifi M., ed. *Proceeding of International Conference Advances in the Analysis of Online Paedophile Activity*, 27–31. Il sito del progetto FIVES (Forensic Image and Video Examination Support) è *http://fives.kau.se*.

[17] Open Computer Forensics Architecture (OCFA) è un framework modulare per la computer forensics progettato ed implementato dall'agenzia nazionale della polizia olandese. Il progetto è open-source ed è disponibile all'url *http://ocfa.sourceforge.net/*.

recuperare tutte le immagini e i video (anche estraendoli da archivi compressi) allo scopo di procedere al riconoscimento degli eventuali file positivi, ovvero contenenti minori in atteggiamenti sessuali espliciti.

L'obiettivo del presente lavoro è la definizione di una metodologia specifica per analisi forensi di sistemi informatici coinvolti in procedimenti di pedopornografia. Nell'ambito di tale definizione si rende necessario uno strumento software per l'analisi del traffico generato da software di file sharing su reti peer-to-peer, in particolare dei file scambiati e delle intenzioni dell'utente, da noi progettato, implementato e chiamato **emuleforensic**.

CAPITOLO 1

1. Aspetti metodologici e applicativi relativi alle indagini nel settore dell'informatica forense

1.1. Evoluzione dell'informatica forense

Nel 1978 il *Florida Computer Crimes Act*[18] introduceva le prime fattispecie di crimini informatici a proposito di reati contro la proprietà intellettuale, reati contro attrezzatura informatica e reati contro gli utenti di sistemi informatici.

Tra le motivazioni addotte dal legislatore, veniva evidenziato come i crimini informatici rappresentassero un grosso problema sia per il governo quanto per il settore privato giacché il danno economico cagionato sarebbe stato ingente. Pur trattandosi di un primo esperimento legislativo in tema di crimine informatico, la lungimiranza del legislatore intravedeva i pericoli derivanti dai reati informatici e pertanto auspicava uno statuto supplementare per meglio definire le varie fattispecie di illeciti informatici[19].

A distanza di alcuni anni si può fissare la data di nascita della computer forensics: è il 1984 quando il laboratorio scientifico della FBI e altre agenzie investigative americane iniziarono a sviluppare programmi da utilizzare nell'esame dei dati presenti nei computer. Nello stesso anno, per rispondere alla crescente richiesta di investigazioni in ambito informatico, fu creato all'interno della FBI il Computer Analysis and Response Team (CART) con il compito

[18] *http://www.clas.ufl.edu/docs/flcrimes/chapter2_1.html*.

[19] Le definizioni inserite nel Florida Computer Crimes Act rappresentarono in assoluto una novità mondiale in tema di crimini informatici, ma confrontati alle definizioni della Convenzione di Budapest (2001) appaiono poco accurate ed imprecise: ad esempio, al punto 4 si definisce "Computer system means a set of related, connected or unconnected computer equipment, devices, or computer software" che invece nella Convenzione di Budapest è definito come "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"; manca inoltre una definizione di "computer data" che invece è offerta dalla Convenzione di Budapest come "computer data means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function".

fondamentale di procedere nei casi in cui si rendesse necessaria l'analisi di un computer.

Un data significativa nell'evoluzione della materia è il 1994 quando il Dipartimento della Giustizia degli Stati Uniti ha pubblicato un insieme di linee guida (il cui ultimo aggiornamento[20] risale al 2009) che per accuratezza, autorevolezza ed esaustività hanno fissato uno standard e sono divenute un basilare riferimento per studi e atti successivi.

La disciplina della computer forensics ha origine in ambienti giuridici ad alta evoluzione tecnologica come gli Stati Uniti, per far fronte all'incremento della domanda di analisi dei dati digitali a fini di investigazione e di giustizia per reati informatici, non informatici ma commessi con sistemi informatici e reati per i quali si rinvengono tracce o indizi nei sistemi informatici. Proprio in questi paesi numerosi soggetti si sono specializzati nell'erogazione di servizi di informatica forense, oltre che di formazione e di vendita di strumentazione (hardware e software) per le operazioni di acquisizione, conservazione e analisi. I soggetti che si occupano di indagini informatiche sono gli operatori forensi (corti, procuratori, avvocati, detective) e i tecnici informatici.

La diffusione su scala mondiale di sistemi informatici ha comportato l'aumento del volume di dati da analizzare che possono costituire l'elemento centrale per l'individuazione o l'interpretazione di un determinato comportamento criminale o, addirittura, la fonte di prova di un delitto. Il materiale informatico contenuto in questi sistemi informatici come file, file di log, archivi elettronici, documenti, informazioni temporanei o residuali, o celate in aree nascoste e normalmente non accessibili nei dispositivi di storage, è così diventato il cuore dell'analisi effettuata dagli esperti di computer forensics.

La FBI per prima ha definito delle linee guida da seguire durante le varie fasi che descrivono le regole da seguire per il sequestro, la duplicazione, la conservazione, il recupero di dati, la ricerca di documenti, la conversione di formati e i servizi dei periti[21]. Come ogni altra scienza la computer forensics richiede che siano eseguite correttamente determinate procedure per garantire l'esattezza della conservazione della prova e dei risultati riguardanti l'elaborazione della prova informatica[22].

---

[20] *http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf*.

[21] **FBI (2007)** *Handbook of Forensic science*. Online *http://www.fbi.gov/about-us/lab/handbook-of-forensic-services-pdf*.

[22] Marcella A.J., Greenfield R.S. (2002) *Cyber Forensics: A field manual for collecting, examining and preserving evidence of computer crimes. Op. cit.*

Secondo la FBI la computer forensics è la scienza atta ad acquisire, conservare, recuperare e presentare dati che sono stati elaborati elettronicamente e sono stati memorizzati nei supporti di archiviazione del calcolatore.

Altre organizzazioni si sono prefissate l'obiettivo di fornire linee guide nell'ambito di indagini aventi per oggetto sistemi informatici: la IACIS[23], ad esempio, è un'organizzazione di volontariato no profit composta da professionisti appartenenti alle forze di polizia che è dedicata all'istruzione nel campo della computer forensics. Nello standard proposto sono stabiliti tre requisiti essenziali per condurre analisi forense:

- utilizzo di supporti sterili dal punto di vista forense;
- mantenimento dell'integrità dei supporti originali;
- identificazione univoca di stampe, copie e risultanze dell'esame.

Dai primi anni del 2000 la computer forensics è diventata progressivamente più conosciuta anche in Italia dove è nota sotto il nome di informatica forense[24] ed è definita come "la disciplina che concerne le attività di individuazione, conservazione, protezione, estrazione, documentazione ed ogni altra forma di trattamento ed interpretazione del dato informatico al fine di essere valutato come prova in un processo, e che studia a fini probatori i processi, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici (hard disk, nastri...) nonché l'analisi forense di ogni sistema informatico e telematico (computer, palmare, rete...), l'esibizione della prova elettronica, l'esibizione del dato digitale, il recupero di dati e la loro esibizione"[25].

L'informatica forense comprende dunque l'insieme di quelle attività che sono rivolte all'analisi e soluzione di quei casi in cui le prove sono da ricercare in strumenti informatici. A fronte di reati delocalizzati come terrorismo, cracking, pedopornografia, truffe on line, discriminazione razziale, phishing, violazione della privacy, spamming, ingiuria e diffamazione, frode informatica,

[23] International Association of Computer Investigative Specialist. http://www.iacis.com/.

[24] In Italia l'espressione Informatica Forense fu utilizzata per la prima volta nel 2003 durante la presentazione tenuta al I Master CSIG di Bari: le prime lezioni universitarie aventi a oggetto tale materia si tennero alla Facoltà di Giurisprudenza dell'Università di Bologna dove nel 2004/2005 si tennero i primi seminari in tale materia e dal 2004/2005 fu avviato il primo corso universitario per lo studio e l'insegnamento dell'Informatica Forense.

[25] Gammarota A. (2004) Un caso di studio di informatica forense: danneggiamento di un sistema informatico della Pubblica Amministrazione. *In:* Pozzi P., Masotti R., Bozzetti M., eds. *Crimine virtuale, minaccia reale. Ict Security: politiche e strumenti di prevenzione*. FrancoAngeli.

furto[26] e riuso di dati, violazioni al diritto d'autore, accessi abusivi, danneggiamenti informatici si avverte una certa difficoltà da parte delle forze dell'ordine nella ricostruzione degli stessi a causa soprattutto dell'estrema volatilità delle tracce digitali e della velocità con cui viene condotta l'azione criminale; come in ogni indagine occorre rispondere ad alcuni quesiti:

- dislocazione dell'autore: da dove?;
- indeterminatezza nel numero degli autori: quanti?;
- anonimizzazione dell'autore: chi è?;
- cronologia degli eventi: quando?;
- modalità esecutive: in che modo?;
- movente: perché?;
- reiterazione: quante volte?;
- offensività: contro chi?.

Particolare rilevanza assumono soggetti terzi (professionisti o enti) specializzati dotati di strutture in grado di eseguire consulenze utilizzabili nella fase processuali su hardware e software sottoposti a sequestro durante le indagini preliminari.

L'analisi forense presuppone che l'esaminatore abbia una profonda conoscenza dal punto di vista informatico di hardware, sistemi operativi, file system[27], networking, alcuni applicativi, qualche linguaggio di programmazione, tecniche di reverse engeneering, oltre che giuridiche. I dispositivi di memorizzazione devono essere "congelati" al più presto, ossia raccolti e preservati quanto prima nel tempo rispetto all'accadimento dell'evento di interesse e senza che i contenuti in essi presenti vengano alterati. Per quanto possibile è importante che durante l'esame dei reperti tutte le procedure siano controllabili e ripetibili: in altri termini qualsiasi esperto, anche indipendente o incaricato dell'attività tecnica in un secondo momento, deve essere in grado, leggendo i documenti e disponendo di una copia, di ripetere tutte le operazioni eseguite durante le indagini.

[26] Con il termine "furto" non s'intende la sottrazione di dati al possessore originario ma la copia abusiva.

[27] Sul punto, cfr. Carrier B. (2005) *File system forensic analysis*. Addison Wesley.

1.2. Definizioni e oggetto dell'informatica forense

La prima definizione completa di cui si ha traccia nella letteratura italiana ad opera di Maioli[28] qualifica l'informatica forense come "la disciplina che studia l'insieme delle attività che sono rivolte all'analisi e alla soluzione dei casi legati alla criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un computer, diretti a un computer o in cui il computer può comunque rappresentare una fonte di prova". Gli scopi dell'informatica forense sono la conservazione, identificazione, acquisizione, documentazione e interpretazione dei dati presenti su un computer. A livello generale si tratta di individuare le modalità migliori per:

- acquisire le prove senza alterare o modificare il sistema informatico su cui si trovano;
- garantire che le prove acquisite su altro supporto siano identiche a quelle originarie,
- analizzare i dati senza alterarli[29].

In sintesi, di dare voce alle prove[30]. L'informatica forense comprende le attività di verifica dei supporti di memorizzazione dei dati e delle componenti informatiche, delle immagini, audio e video generate da computer, dei contenuti di archivi e basi dati e delle azioni svolte nelle reti telematiche.

In realtà, tale definizione, pur molto dettagliata, sembrerebbe relegare l'informatica forense unicamente all'ambito penale, mentre è ormai comune utilizzare tecniche di digital forensics anche nel processo civile, in ambito giuslavoristico, in materia di diritto amministrativo o nelle investigazioni interne aziendali.

Un'altra definizione elaborata in dottrina che ha avuto ampia diffusione vede l'informatica forense come "la scienza che disciplina le metodologie per la preservazione, l'identificazione e lo studio delle informazioni contenute nei computer o nei sistemi informativi in generale, al fine di evidenziare l'esistenza di prove utili allo svolgimento dell'attività investigativa"[31] e che "studia il

[28] Maioli C. (2004) *Dar voce alle prove: elementi di informatica forense. Op. cit.*

[29] Heiser J., Kruse W. (2001) *Computer forensics. Incident Response Essentials*. Addison-Wesley.

[30] Maioli C. (2004) *Dar voce alle prove: elementi di informatica forense. Op. cit.*

[31] Fagioli G., Ghirardini A. (2013) *Digital forensics*. Apogeo.

valore che un dato correlato a un sistema informatico o telematico può avere in ambito giuridico"[32].

A seconda delle peculiarità dei dispositivi oggetto di analisi o delle modalità di raccolta dei dati, l'informatica forense può essere meglio classificata in un certo numero di branche, la cui composizione può essere oggetto di variazione nel tempo in base allo sviluppo tecnologico.

1.2.1. Disk forensics

La disk forensics è la principale e più antica branca dell'informatica forense. Per questo motivo è frequente che la dizione "disk forensics" venga sostituita da "computer forensics" o dalla più generica "informatica forense", e sue varianti in lingua inglese. La disk forensics si occupa dell'analisi di supporti informatici (hard disk, solid state disk, chiavette USB, CD-ROM…) che può seguire finalità differenti a seconda del ruolo assunto dai medesimi.

I primi casi di disk forensics risalgono agli anni Settanta, principalmente per il contrasto ai crimini finanziari. Nel 1978 in Florida l'emanazione del Computer Crime Act[33] ne formalizzò la nascita con crimini copyright privacy e pedopornografia.

Solo a partire dagli anni 2000 è emersa prepotentemente la necessità di definire standard e linee guida che consentano di conseguire un adeguato livello di attendibilità: a tale scopo, il National Institute of Justice ha pubblicato diverse guide[34] destinate prevalentemente alle forze dell'ordine finalizzate alla definizione di corrette procedure per l'analisi forense delle prove digitali e per la salvaguardia della scena del crimine.

1.2.2. Network forensics

I sistemi informatici non sono confinati all'ormai esiguo spazio che occupano ma, disponendo di una connessione di rete, comunicano con altri sistemi: soprattutto in tempi recenti e grazie alla disponibilità di connessione ad

[32] Luparia L., Ziccardi G. (2007) *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*. Giuffrè.

[33] *http://www.clas.ufl.edu/docs/flcrimes/chapter2_1.html*.

[34] *http://www.nij.gov/topics/forensics/evidence/digital/pages/welcome.aspx*.

alta velocità, sono notevoli le possibilità fornite dal cloud computing che consente ad esempio di utilizzare sistemi di archiviazione di dati remoti[35].

L'analisi forense subisce dunque tutti gli effetti portati dallo sviluppo di tecnologie basate su reti di computer poiché tende a ridursi il potere informativo fornito dal singolo sistema informatico utilizzato dall'utente finale. L'attenzione deve dunque allargarsi anche a sistemi remoti o addirittura virtuali. Senza network forensics ormai si corre il rischio di tralasciare dati fondamentali per un'indagine.

La network forensics ha come oggetto di indagine le tecniche di analisi forense tipiche di un sistema di trasmissione dati. Tale disciplina presenta una notevole complessità in quanto è costretta a seguire il percorso del dato su una moltitudine di sistemi: ad esempio, nel caso della posta elettronica l'email spedita dall'utente A all'utente B è rinvenibile non solo sui sistemi informatici in uso ad A e B per la consultazione della stessa, ma anche sui server intermedi attraversati.

1.2.3. Cloud forensics

Il termine cloud computing indica un insieme di tecnologie che consentono ad un Cloud Service Provider di erogare ai propri clienti una varietà di servizi di archiviazione ed elaborazione dei dati mediante l'utilizzo di risorse hardware e software virtualizzate e distribuite in rete[36]. Secondo la definizione del National Institute of Standard and Technologies (NIST)[37] le caratteristiche principali del paradigma elaborativo del cloud computing sono: la disponibilità di connessioni di rete a banda[38] larga, la flessibilità nell'erogazione dei servizi, l'offerta di prestazioni a consumo di tipo self-service e la condivisione delle risorse tra più utenti.

[35] Ad esempio, i sistemi di cloud storage quali Dropbox, iCloud, GoogleDrive forniscono – gratuitamente per i primi gigabyte – spazio per l'archiviazione dei dati in remoto oltre ad una serie di funzionalità accessorie come il versioning e la sincronizzazione dei file tra più sistemi.

[36] Marturana F., Tacconi S. (2013) Il digital forensics nel contest del cloud computing. *In:* Attanasio A., Costabile G., eds. *IISFA Memberbook 2012*. Experta. 123–151.

[37] Grance T., Mell J. (2011) *The NIST definition of cloud computing*. NIST. Disponibile all'url *http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf*.

[38] Il termine banda (o bandwidth) indica la quantità di dati che possono essere trasferiti attraverso una connessione in un dato periodo di tempo. La banda dipende dal tipo di mezzo fisico utilizzato (ad esempio cavo o etere nelle connessioni wifi) e dalle sue condizioni fisiche.

La cloud forensics è uno dei temi più popolari e dibattuti degli ultimi anni[39]: l'elaborazione distribuita dei dati e la mancanza di accesso fisico alle memorie di massa presenti sui server distribuiti nel cloud rappresentano un serio problema per l'investigatore che deve rivedere le tecniche di disk e network forensics nell'ottica del nuovo fenomeno. Un esempio di servizio erogato in cloud computing è la posta elettronica: l'utente non ha necessità di installare e configurare alcun software sul proprio sistema informatico, avendo la possibilità di accedere ai dati in remoto anche da altri sistemi mediante un'interfaccia di accesso come un browser.

1.2.4. Mobile forensics

La mobile forensics ha come oggetto di indagine i dispositivi mobili, e più nel dettaglio, si può dividere in:

- SIM card forensics, in cui l'oggetto analizzato è il contenuto della scheda SIM;
- Mobile Handset Forensics (o Cell Phone Forensics), in cui l'oggetto analizzato è il contenuto del dispositivo mobile (smartphone, tablet, cellulare…);
- Memory Card Forensics (o Removable Media Forensics), in cui l'oggetto analizzato è una scheda di memoria che potrebbe essere impiegata per estendere le capacità di memoria del dispositivo di memoria; in questo caso, le tecniche di analisi sono mutuate dalla disk forensics;
- Cellsite Forensics, in cui l'oggetto di indagine sono i tabulati telefonici che contengono le tracce lasciate dai dispositivi mobili lungo la rete, consentendo di geolocalizzare un dispositivi nel tempo e nello spazio.

1.2.5. Embedded forensics

L'embedded forensics non ha una sua dimensione ben circostanziata a causa dell'estrema diversificazione dei sistemi: questa branca si occupa di

[39] Sul punto, cfr. Garrison C., Lillard T., Schiller C., Steele J. (2010) Forensics for Network, Internet, and Cloud Computing. A Forensic Evidence Guide for Moving Targets and Data. Elsevier; Malzer E., Poisel R., Tjoa S. (2013) Evidence and cloud computing: The virtual machine introspection approach. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 4(1), 135–152.

affrontare l'analisi forense dei sistemi digitali non classificabili nelle precedenti categorie. Sono infatti sempre più numerosi gli strumenti digitali specializzati che possono contenere tracce utili ai fini di un indagine: si pensi ad esempio a consolle di videogame (PlayStation, Xbox…), sistemi di rilevamento di intrusione, sistemi informatici di gestione di autoveicoli, scatole nere e così via.

Tra tutte, questa è probabilmente la branca che presenta le maggiori criticità poiché risulta estremamente difficoltoso recuperare informazioni sulle tecniche di acquisizione e di analisi forensi degli stessi.

1.2.6. Multimedia forensics

A seguito della crescente diffusione di immagini e video in formato digitale diventa sempre più frequente la necessità di analizzare tali dati per estrarre informazioni utili da produrre come prove in un processo: il caso tipico è quello dei filmati di videosorveglianza che registrano l'evento criminoso ma risultano di difficile utilizzo a causa della scarsa qualità (risoluzione, rumore…)[40].

La multimedia forensics si occupa di estrarre informazioni utili ai fini di un'indagine da immagini e video, verificando altresì l'autenticità e la provenienza delle prove digitali. Il ricorso a tecniche di image e video forensics si rende necessario quando occorre determinare la contraffazione di un dato multimediale, la valutazione dell'attendibilità del dato (a sostegno di un'accusa o di un alibi), per migliorarne la qualità o per ricavare delle informazioni (ad esempio, la velocità di un automobile in un video piuttosto che l'apparecchio utilizzato per la cattura[41]).

1.2.7. La differenza tra informatica forense e sicurezza informatica

Infine s'intende evidenziare come vi sia differenza tra informatica forense e sicurezza informatica, sebbene le due aree di attività siano collegate. La sicurezza informatica si occupa di proteggere i dati e la funzionalità di un sistema, rappresentando dunque un ostacolo per l'informatica forense poiché la difficoltà di accesso ai dati è elevata sia per chi intende commettere attività illecite che per chi intende utilizzare gli stessi dati a fini investigativi e di prova.

[40] Battiato S., Farinella G., Puglisi G. (2012) Image/video forensics: casi di studio. *In:* Attanasio A., Costabile G., eds. *IISFA memberbook 2011*. Experta. 261–292.

[41] Battiato S., Messina G., Rizzo R. (2009) Image forensics contraffazione digitale e identificazione della camera di acquisizione: status e prospettive. *In:* Attanasio A., Costabile G., eds. *IISFA Memberbook 2009*. Experta. 49–98.

L'acquisizione dei dati contenuti all'interno del sistema da analizzare richiederà dunque l'utilizzo di tecniche di hacking che di fatto comportano la violazione del sistema[42]. L'informatica forense interviene dopo che il sistema è stato violato[43] e si occupa di preservare le prove informatiche che consentono di documentare violazioni di sicurezza, oltre che individuare potenziali elementi di prova per reati che non abbiano comportato la violazione di un sistema informatico.

1.3. L'informatica forense come scienza forense

Il metodo scientifico è la modalità con cui la scienza procede per raggiungere una conoscenza della realtà oggettiva, affidabile, verificabile e condivisibile. Da una parte si procede nella raccolta di evidenze empiriche attraverso l'osservazione sperimentale, dall'altra nella formulazione di ipotesi e teorie da sottoporre al vaglio dell'esperimento per testarne l'efficacia.

L'informatica forense in qualità di branca delle scienze forensi richiede differenti protocolli operativi e conoscenza delle norme giuridiche; i risultati non servono solo per fare ricerca ma esistono vincoli giurisprudenziali ed effetti che si esplicano sulla libertà personale. Pertanto chi si occupa di informatica forense dovrebbe principalmente nascere come "uomo di scienza", con idonee conoscenze di alcuni aspetti legislativi, che deve essere in grado di spiegare – sia nel proprio elaborato, sia nelle deposizioni in tribunale – gli esiti degli esami compiuti sui reperti, al fine di comunicare efficacemente anche con gli interlocutori che ignorano questi aspetti scientifici.

Lo scienziato forense contribuisce nella fase investigativa suggerendo e confermando ipotesi con l'obiettivo di giungere ad una fedele ricostruzione di quanto accaduto; nella fase dibattimentale egli interviene esprimendo pareri e valutazioni ed aiutando il giudice, che rimane comunque il *peritus peritorum,* a prendere la decisione finale.

[42] Per analogia, si pensi all'appartamento con livello di sicurezza elevato dotato di porta blindata e cancello: l'accesso all'appartamento sarà difficile tanto per chi intende intrufolarsi a scopo di rapina quanto per un agente di polizia che dovrà utilizzare le stesse tecniche del rapinatore per scardinare i sistemi di sicurezza.

[43] L'informatica forense viene dopo che il sistema è stato violato nei casi di reati prettamente informatici. Nei casi in cui il sistema informatico è un mero mezzo d'azione o un contenitore di dati utili a provare un reato non c'è alcuna violazione, tuttavia le tecniche d'informatica forense tornano utili per assicurare integrità e autenticità dei dati.

1.4. La prova scientifica

Negli ultimi anni la prova[44] scientifica è prepotentemente entrata nelle aule (non solo penali) dei tribunali. Lo scienziato utilizza le proprie conoscenze, i propri studi, le proprie esperienze per produrre enunciati di carattere generale. La giurisdizione opera invece in senso esattamente opposto perché il giudice utilizza le conoscenze e gli enunciati generali per affermare qualcosa su fatti specifici.

Questa constatazione ha implicazioni importantissime perché nessuna legge scientifica, nessun enunciato universale, per quanto sia certo e cogente nelle sue implicazioni, potrà dirci tutto sul caso particolare che si chiede di risolvere in un'aula di giustizia. Infatti, quel caso particolare è appunto un unicum, mentre la legge scientifica parla di una classe di fatti.

Al momento dell'ammissione, dell'assunzione e della valutazione, si usano strumenti di conoscenza attinti dalla scienza e dalla tecnica, vale a dire principi e metodologie scientifiche, metodiche tecnologiche e apparati tecnici il cui uso richiede competenze esperte.[45]

II problema di fondo è la verifica di come il ricorso alle leggi scientifiche, sempre mutevoli in virtù del continuo progresso tecnologico, possa avvenire nel rispetto dei principi del giusto processo e segnatamente del diritto di difesa, dai quali non si può prescindere, rimarcando che la condanna può venire inflitta soltanto se l'imputato risulti colpevole oltre ogni ragionevole dubbio[46].

L'aggettivo "ragionevole" significa "comprensibile da una persona razionale" e dunque oggettivabile attraverso una motivazione che faccia riferimento ad argomentazioni logiche e cioè che rispetti il principio di non contraddizione.[47] Non potrà trattarsi pertanto di un dubbio meramente psicologico, possibile o congetturale, percepito soggettivamente dal giudice. La Cassazione[48] ha affermato che la "regola dell'oltre il ragionevole dubbio" formalizzata nell'art. 533 impone di pronunciare condanna quando il dato

[44] La prova in senso giuridico, ed in particolare processuale, e la dimostrazione della sussistenza di fatti determinati e in ambito penale è disciplinata nell'art. 187 c.p.p.

[45] Dominioni O. (2005) *La prova penale scientifica*. Giuffrè.

[46] La Legge 46/2006 ha modificato l'art. 533 c.p.p., comma 1, relativo alla sentenza di condanna ed ha stabilito che il giudice pronuncia tale sentenza quando l'imputato "risulta colpevole del reato contestatogli al di là di ogni ragionevole dubbio". La prova d'accusa che lascia residuare un ragionevole dubbio è equiparata alla mancata prova.

[47] Conti C., Tonini P. (2012) *Il diritto delle prove penali*. Giuffrè.

[48] Cass. Pen., Sez. I, 21 aprile 2010, n. 19933.

probatorio acquisito lascia fuori solo eventualità remote la cui realizzazione nella fattispecie concreta non trova il benché minimo riscontro nelle emergenze processuali, ponendosi al di fuori dell'ordine naturale delle cose e della normale razionalità umana. Pertanto può ritenersi che l'accusa abbia adempiuto all'onere quando ogni differente spiegazione del fatto addebitato, basata sulle prove, appare non ragionevole; viceversa l'accusa non ha adempiuto all'onere quando le risultanze processuali non sono idonee ad escludere quella ragionevole ricostruzione alternativa che stata prospettata dalla difesa sulla base delle prove acquisite[49].

In tema di prova scientifica, dunque, il giudice dovrebbe dar conto in motivazione di aver valutato criticamente il grado di controllabilità e attendibilità del metodo scientifico, l'esistenza di revisioni critiche di esperti del settore, l'indicazione dei margini di errore conosciuto.

1.5. La digital evidence

I dati sono fatti elementari, informazioni codificate che hanno bisogno di un'interpretazione per assumere un significato e fornire conoscenza[50]. Il dato informatico è una rappresentazione in un sistema binario di sequenze di bit non immediatamente comprensibili all'uomo per cui necessita di una serie di operazioni attraverso cui si opera una trasformazione che può portare a risultati diversi (mostrato sul monitor in rappresentazione testuale o come un video, ma anche come un'immagine stampata su un foglio di carta).

Per sua natura, il dato digitale è:

- immateriale, per cui necessita di un supporto idoneo per contenerlo quali ad esempio CD-ROM, hard disk, chiavette USB;
- volatile, in quanto può essere disperso abbastanza facilmente;
- deteriorabile, modificabile in modo anche anonimo e/o involontario;
- riproducibile in un numero potenzialmente infinito di copie.

[49] Tonini P. (2013) *Diritto processuale penale. Manuale breve*. Giuffrè.

[50] A tal proposito, si critica l'utilizzo dei termini "dati, informazioni e programmi" negli articoli dalla ratifica della Convenzione di Budapest rispetto all'utilizzo del solo termine "dati" originariamente utilizzato nel testo della Convenzione. Le informazioni rappresentano il significato che viene attribuito a determinati dati sulla base delle conoscenze di chi s'interfaccia ad essi e della loro organizzazione. I programmi sono la codifica di algoritmi in un linguaggio di programmazione che, interpretato o compilato, consente di eseguire determinate operazioni; i programmi sono dunque un sottoinsieme di possibili sequenze di dati, come file di elaboratore testi, file di immagini o qualunque altro tipo di aggregato di dati.

Si può considerare digital evidence ogni dato informatico allocato su un particolare dispositivo oppure trasmesso da sistemi informatici e telematici che possa avere un qualche rilevanza processuale[51].

Ogni dato utilizzato per supportare o confutare una tesi al fine di definire come ha avuto compimento un'offesa, o per stabilire l'intenzione o l'alibi è da definirsi prova scientifica in formato digitale. Non trovando una specifica catalogazione nel codice, la prova informatica è qualificabile come prova atipica: ai sensi dell'art. 189 c.p.p., quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova[52].

Le prove digitali si pongono in una posizione in cui perde consistenza la naturale propensione dell'uomo a rapportarsi al mondo reale con l'uso dei cinque sensi, in particolare il tatto, per cui appare più difficile far assumere rilevanza a questo genere di prove. L'elevato rischio di deteriorabilità rende le prove digitali facilmente alterabili, danneggiabili o distruggibili, talvolta anche dagli stessi investigatori se non idoneamente preparati a svolgere un'indagine di informatica forense.

In fase processuale accade spesso che vengano contestate le operazioni di raccolta e conservazione dei dati digitali e queste problematiche sono dovute al fatto di dover lavorare con qualcosa di non tangibile ed invisibile alle persone che non hanno conoscenze specifiche in materia (un esempio può essere una traccia di attività illecita rinvenuta in un file di log).

[51] D'Aiuto G., Levita L. (2012) *I reati informatici. Disciplina sostanziale e questioni processuali*. Giuffrè.

[52] In materia di prove non vige nel nostro ordinamento il principio di tassatività, sicché, oltre ai mezzi di prova specificamente disciplinati dalla legge (testimonianza, esame delle parti, confronti, ricognizioni…) l'ordinamento ammette anche le c.d. prove atipiche o innominate (che il legislatore non ha a priori e nominativamente previsto), sempre che ricorrano due condizioni:

- che la prova atipica sia idonea ad assicurare l'accertamento dei fatti: che, cioè, abbia, almeno in astratto, capacità dimostrativa (tale non sarebbe, ad esempio, alla luce delle attuali conoscenze scientifiche, la prova medianica, consistente nell'accertare i fatti di causa a mezzo di una seduta spiritica);
- che la prova atipica non pregiudichi la libertà morale della persona: che non sia, cioè, contraria all'art. 188 (ad esempio, pregiudicherebbe la libertà morale della persona l'uso di strumenti di tortura nel corso di una testimonianza).

Come accade per ogni tipologia di prova, anche per la prova digitale è il proponente che ha l'onere di dimostrarne la relativa fondatezza, veridicità ed autenticità. L'utilizzo di prove digitali nei tribunali è in continuo aumento per cui è possibile trovare in aule di tribunali copie di e-mail, fotografie digitali, documenti di videoscrittura, fogli elettronici, tracciamenti di GPS, file audio, video digitali, tutti documenti che richiedono l'esigenza di riformulare molte norme del codice di procedura penale tenendo conto della caratteristica di suddette prove.

È opportuno distinguere la prova – intesa come risultato probatorio che si forma in dibattimento, nel contradditorio delle parti e sulla quale il giudice fonderà la propria decisione – dall'elemento di prova – ricavabile dalle fonti di prova, raccolto dal Pubblico Ministero durante le indagini preliminari e portato al giudice al fine di richiedere la condanna dell'imputato. Alla luce di tale distinguo sarebbe più corretto utilizzare il termine evidenza digitale[53] allo scopo di comprendere sia la prova che l'elemento di prova digitale.

L'autorevole Casey propone una definizione di digital evidence secondo la quale la prova digitale è "qualsiasi dato memorizzato o trasmesso usando un computer che supporta o respinge una teoria su come è avvenuto un fatto offensivo o che individua elementi critici dell'offesa come l'intenzionalità o l'alibi"[54]. Accanto a questa pone altre tre definizioni:

1. qualsiasi dato che possa stabilire che un crimine è stato commesso o che può fornire un collegamento tra un crimine e la sua vittima o tra un crimine e chi l'ha commesso[55];
2. ogni informazione con un valore probatorio che è memorizzato o trasmesso in forma digitale[56];
3. informazione trasmessa o memorizzata in formato binario che può essere utilizzata in tribunale[57].

Da un punto di vista prettamente tecnico sarebbe opportuno distinguere l'evidenza digitale dall'evidenza elettronica allo scopo di porre l'enfasi sui dati piuttosto che sui dispositivi elettronici che li contengono: tale distinguo viene

[53] Mason S. (2008) *International Electronic Evidence*. British Institute of International and Comparative Law; Vaciago G. (2012) *Digital Evidence*. Giappichelli.

[54] Casey E. (2004) *Digital Evidence and Computer Crime. Forensic science, computers and the Internet*. Elsevier.

[55] Definizione già fornita dallo stesso Casey nel 2000.

[56] Definizione proposta dallo Standard Working Group on Digital Evidence (SWGDE).

[57] Definizione proposta dalla International Organization Computer Evidence (IOCE).

recepito ed esplicitato nello standard ISO/IEC 27037:2012[58] dove vengono separatamente definiti il "dispositivo di memorizzazione di dati digitali", quale oggetto contenente i dati digitali di interesse, il "dispositivo digitale" e le "periferiche", questi ultimi strumenti che consentono di elaborare i dati digitali, recepirli o immetterli verso il mondo esterno, ma comunque privi di capacità di memorizzazione a lungo termine.

C'è comunque da tener presente che se un tempo i dati venivano salvati esclusivamente nei dispositivi di memorizzazione di dati digitali collegati al sistema informatico fisicamente utilizzato dall'utente finale, oggi tante informazioni sono delocalizzate da una singola postazione e conservate nel complesso in una rete. Per cui, se un crimine è commesso anche solo in parte tramite l'utilizzo di una rete, le prove sono distribuite su diversi computer e in molti casi non è materialmente possibile realizzare in contemporanea la raccolta di tutto l'hardware.

Allo stesso tempo, la presenza di una rete può indurre ridondanza, un fenomeno per cui un dato non disponibile in un punto della rete potrebbe essere rintracciato in un altro.

1.6. Le best practice

Nel disciplinare il modus operandi delle operazioni può osservarsi come l'attenzione del legislatore si sia focalizzata, giustamente, più sul risultato che deve essere ottenuto piuttosto che sul metodo da seguirsi: la canonizzazione all'interno di norme giuridiche di procedure tecniche a livello informatico più che rappresentare una garanzia, avrebbe portato, alla lunga, ad effetti contrari e distorsivi rappresentati dall'evoluzione costante della disciplina e dalle peculiarità proprie di ciascun caso[59].

Fino all'ottobre 2012 le metodologie erano definite in alcune *best practices* del settore, volte a delineare i paradigmi dell'agire tecnico in ambito forense, attraverso una metodologia di base che miri: a) all'acquisizione della prova senza alterare o danneggiare il dispositivo originale; b) all'autenticazione del reperto e dell'immagine (*bit stream image*) acquisita; c) a garantire la ripetibilità dell'accertamento; d) a un'analisi senza modificazione dei dati originari; e) alla massima imparzialità nell'agire tecnico. A livello pratico,

[58] Si veda paragrafo 1.7.1. Lo standard ISO/IEC 27037:2012.

[59] Maioli C., Sanguedolce E. (2012) *I "nuovi" mezzi di ricerca della prova fra informatica forense e L. 48/2008*. Altalex, 07 maggio 2012.*http://www.altalex.com/index.php?idnot=18096*.

tuttavia, l'attuazione e lo sviluppo di procedure condivise si scontrano con due ordini di limiti, riconducibili, da un lato, alla "variabile tecnologica" rappresentata sia dalle caratteristiche dei supporti in cui i dati sono contenuti sia dall'habitat tecnologico in cui il dispositivo s'inserisce ed opera (si pensi ad esempio all'acquisizione di dati contenuto all'interno di un hard disk in un ambiente di *trust computing*, ossia dotato di meccanismi di cifratura del contenuto); dall'altro, rileva la "variabile soggettiva", costituita dal soggetto che opera e dagli obiettivi connessi all'azione: per le Forze di Polizia il fine sarà quello di acquisire elementi utili alle indagini preservandone l'autenticità, per la Magistratura sarà di collegare tali risultanze a fatti penalmente rilevanti, per il Consulente tecnico della difesa o il difensore nell'ambito delle investigazioni difensive sarà di controllare che i processi seguiti consentano un idoneo esercizio del diritto di difesa[60].

1.7. Gli standard ISO l'informatica forense

ISO (Organizzazione Internazionale per la Standardizzazione) e IEC (Commissione Elettrotecnica Internazionale) formano il sistema specializzato per la standardizzazione a livello mondiale. Gli enti nazionali che sono membri dell'ISO e dell'IEC partecipano allo sviluppo degli standard internazionali attraverso commissioni tecniche istituite dalle rispettive organizzazioni per occuparsi di campi specifici dell'attività tecnica. Le commissioni tecniche di ISO ed IEC collaborano in ambiti di mutuo interesse. Prendono parte ai lavori anche altre organizzazioni internazionali, governative e non governative, in collaborazione con ISO ed IEC.

Il compito principale della commissione tecnica congiunta è di redigere gli standard internazionali i cui progetti, adottati dalla commissione tecnica congiunta, 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 vari standard promossi dall'ISO, di recente sono stati presentati documenti che riguardano l'informatica forense che si candidano a norme tecniche di riferimento effettivamente discusse e riconosciute a livello internazionale:

[60] Signorile O. (2009) Computer Forensics Guidelines: un approccio metodico-procedurale per l'acquisizione e analisi delle digital evidence. In *Ciberspazio e Diritto*, 2, 197–209.

- 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, in discussione e previsto per l'emissione il 28 febbraio 2015 relativamente a linee guida sulla garanzia di idoneità e adeguatezza dei metodi di investigazione;
- ISO/IEC 27042, in discussione e previsto per l'emissione il 28 febbraio 2015 relativamente a linee guida per l'analisi e l'interpretazione di prove digitali;
- ISO/IEC 27043, in fase di sviluppo, relativamente a principi e processi per l'investigazione di incidenti informatici.

1.7.1. Lo standard ISO/IEC 27037:2012

L'unico standard attualmente emanato in versione definitiva, il 15 ottobre 2012, è lo standard ISO/IEC 27037:2012, un documento che nella sua definizione richiama altri standard ISO/IEC[61] e contiene delle linee guida che si possono certamente considerare come il protocollo operativo di riferimento nel settore dell'informatica forense per le fasi di identificazione, raccolta, acquisizione e conservazione delle prove digitali necessarie in una qualsiasi indagine che necessita di mantenere l'integrità delle prove digitali.

Lo standard ha lo scopo di offrire una guida ai soggetti responsabili dell'identificazione, raccolta, acquisizione e conservazione delle potenziali prove digitali:

- il Digital Evidence First Responders (DEFR), soggetto autorizzato, preparato e qualificato per intervenire per primo sulla scena di un incidente raccogliendo ed acquisendo le prove digitali con la responsabilità della loro gestione;

[61] 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.

- il Digital Evidence Specialists (DES), soggetto che svolge le mansioni di un DEFR ed ha conoscenze specialistiche, capacità ed abilità nella gestione una grande varietà di questioni tecniche;
- specialisti di incident response;
- dirigenti dei laboratori di informatica forense.

Il documento prevede che i soggetti responsabili gestiscano le potenziali prove digitali con metodologie che risultino adeguate su scala mondiale, con l'obiettivo di facilitare l'investigazione riguardo i 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[62].

A causa della fragilità delle prove digitali, è necessario mettere in atto una metodologia adeguata per assicurare l'integrità e l'autenticità delle potenziali 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.

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

[62] Lo standard non si occupa di documenti analogici che vengono convertiti in formato digitale.

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[63] e ISO/IEC 27002[64], ed i 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.

1.8. Fasi dell'informatica forense alla luce degli standard ISO

In letteratura, l'informatica forense è sempre stata definita su cinque (talvolta quattro) fasi[65]: identificazione; acquisizione (con raccolta e conservazione); analisi; valutazione e presentazione (nelle versioni a quattro fasi, queste ultime due erano raggruppate).

Tuttavia, prendendo in esame le varie definizioni di informatica forense, lo stato della tecnologia, varie linee guida definite nelle best pratice e, in ultimo, quanto correttamente definito ed illustrato all'interno degli standard ISO/IEC sul tema, il processo dell'informatica forense andrebbe più correttamente diviso in sette fasi secondo il seguente schema: identificazione; raccolta; acquisizione; conservazione e trasporto; analisi; valutazione; presentazione.

1.8.1. Identificazione

La prova digitale ha una forma fisica e una forma logica: la forma fisica è data dalla tecnica di impressione dei dati sul supporto (ad esempio, magnetizzazione della materia nel caso dei supporti magnetici o la rappresentazione in pit e land dei supporti ottici[66]); la forma logica è la

[63] ISO/IEC 27001:2013 - ISO/IEC 27001 - Information security management.

[64] ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security controls.

[65] Carrier B., Spafford E. (2003) Getting physical with the digital investigation process. *International Journal of Digital Evidence*, 2(2).

[66] Sui supporti ottici i bit sono impressi sotto forma di pit e land: i pit sono le incisioni nel substrato di plastica del disco (larghi circa 0.6 micron) mentre i land sono le zone lasciate intatte. Il substrato è posto vicino alla superficie superiore del disco ed è metallizzato al fine di

rappresentazione virtuale dei dati in bit che possono assumere il valore di 0 oppure di 1.

L'identificazione è il processo di ricerca, ricognizione e documentazione di potenziali prove in formato digitale, ovvero dei dispositivi di memorizzazione di bit che possono essere rilevanti ai fini dell'indagine, individuando dove possibile anche i dati che si possono trovare all'esterno o in spazi virtuali come ad esempio sistemi cloud. Non si tratta comunque solo di una banale ricerca di dispositivi ma occorre definire le giuste priorità tenendo conto del rischio di volatilità dei dati, allo scopo di minimizzare il danneggiamento di potenziali prove digitali e di ottenere il dato più integro e genuino possibile[67].

1.8.2. Raccolta

Una volta identificati i dispositivi digitali 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.

La raccolta è la fase del trattamento di dati digitali in cui i dispositivi che possono contenere potenziale prove digitali vengono rimossi dalla loro posizione originale per essere trasportate in un laboratorio o, più in generale, 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.

I dispositivi contenenti potenziali prove digitali possono essere nello stato acceso oppure nello stato spento. A seconda dello stato e della finalità dell'indagine, nonché dei limiti giuridici, metodologie e strumenti diversi possono essere richiesti.

La raccolta è l'operazione che viene solitamente preferita dalle forze dell'ordine perché rispetto all'acquisizione, descritta nel paragrafo successivo, presenta alcuni vantaggi:

---

riflettere il raggio laser. Durante la lettura ogni transizione pit-land e land-pit viene interpretata come un bit 1, mentre le aree piane, che si trovano prima e dopo ogni transizione, sono qualificate come uno o più bit 0 consecutivi. I pit ed i land sono allineati in una traccia a spirale, che inizia vicino al diametro interno del disco e termina in prossimità del diametro esterno.

[67] Vacca J. (2005) *Computer forensics. Computer Crime Scene Investigation*. Charles River Media.

- semplicità e tranquillità: 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[68]; 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;
- tangibilità: la tangibilità del supporto trasmette maggiore tranquillità agli operatori e all'indagato che potrebbe non disporre di conoscenze tecniche e giuridiche adeguate per valutare l'attività tecnica in essere;
- conservazione di ulteriori prove non digitali: oltre al dato digitale, un reperto informatico potrebbe essere utilizzato per rilevare altre tipi di prove quali ad esempio impronte digitali[69].

Tuttavia, in diverse 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.

In ogni caso, il processo di raccolta non si deve limitare al solo dispositivo che contiene i dati digitali ma va esteso al materiale che lo riguarda quale, a

[68] Si pensi al caso di sistemi informatici che utilizzano un insieme di hard disk gestiti in modalità RAID dove la sequenza di connessione degli stessi è indispensabile per la ricostruzione, e dunque l'accesso in lettura, dei dati contenuti all'interno del volume logico.

[69] A tal proposito, la raccolta di dispositivi dovrebbe richiedere accortezza non solo in relazione all'integrità del dato digitale ma anche di questi ulteriori elementi: ad esempio, occorrerà utilizzare dei guanti laddove si renda necessario preservare un'impronta digitale.

titolo esemplificativo, post-it con password, quaderni con appunti e alimentatori. Inoltre il processo di raccolta va documentato in dettaglio per giustificare la scelta di un metodo al posto di un altro. I supporti informatici vanno imballati con cura tenendoli lontano da fonti di calore in modo da non rischiare di corrompere il supporto e di causare la perdita accidentale di dati.

Da un punto di vista giuridico, la raccolta è la fase che trova riscontro nel sequestro probatorio[70], 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.

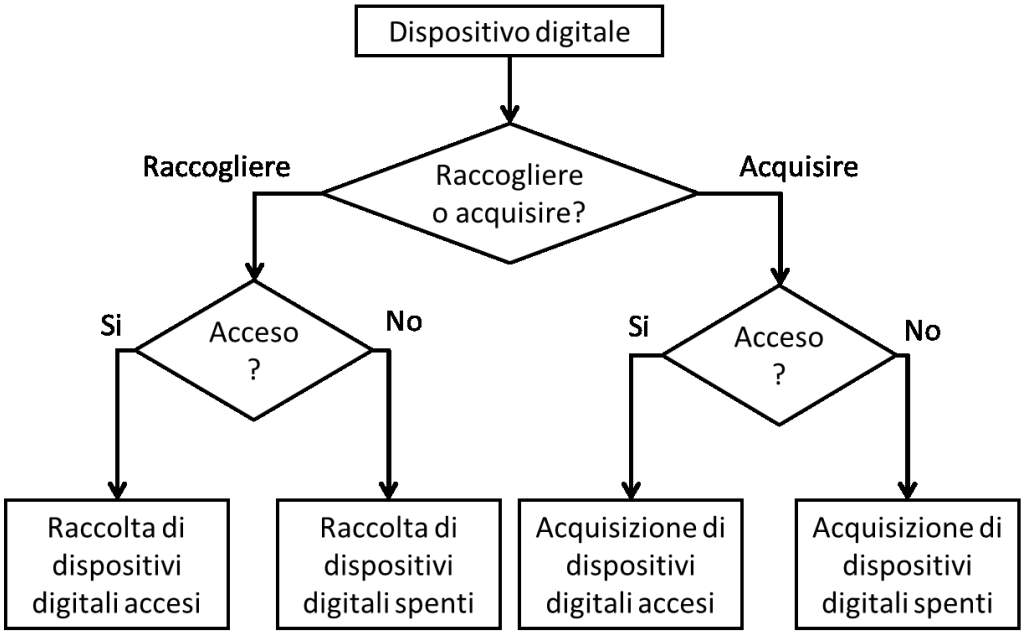


Figura 1 – Criterio decisionale circa l'opportunità di raccogliere o acquisire una potenziale evidenza digitale[71]

Qualora si dovesse propendere per la raccolta, in caso di dispositivi spenti lo schema da seguire è il seguente.

[70] Articoli 253 e seguenti c.p.p.

[71] Traduzione della figura 1 riportata nello standard ISO/IEC 27037:2012.

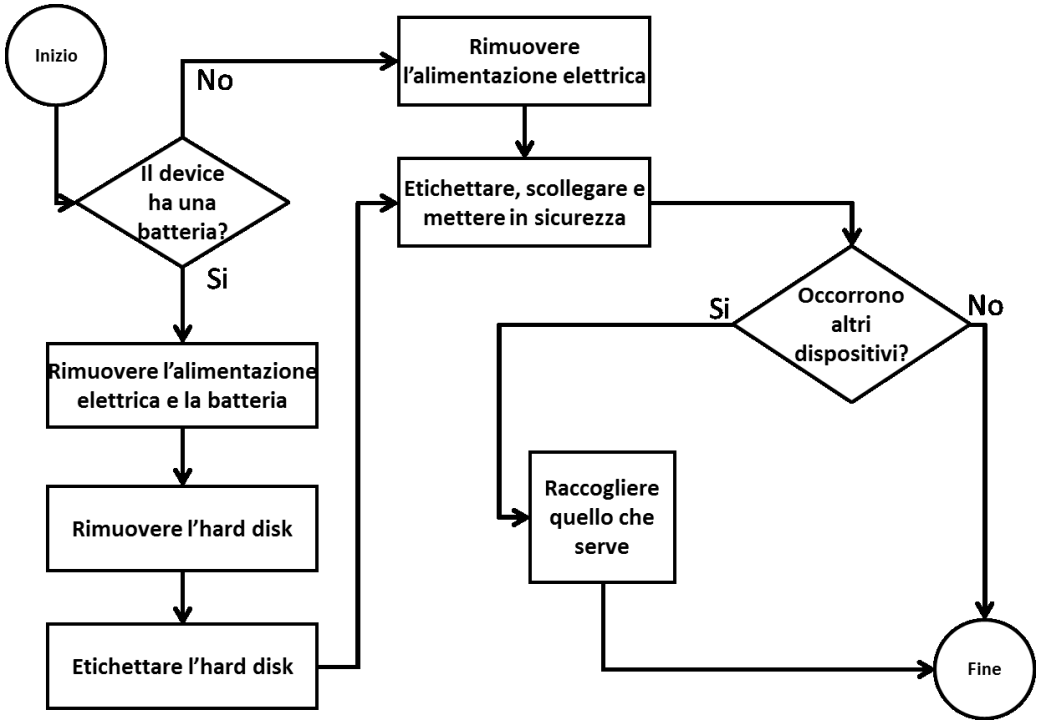


Figura 2 - Linee guida per la raccolta di dispositivi digitali spenti[72]

Quando invece si entra in contatto con un dispositivo acceso, la schema è più complesso perché richiede la valutazione di alcuni elementi che andrebbero persi definitivamente dopo lo spegnimento del sistema.

[72] Traduzione della figura 3 riportata nello standard ISO/IEC 27037:2012.

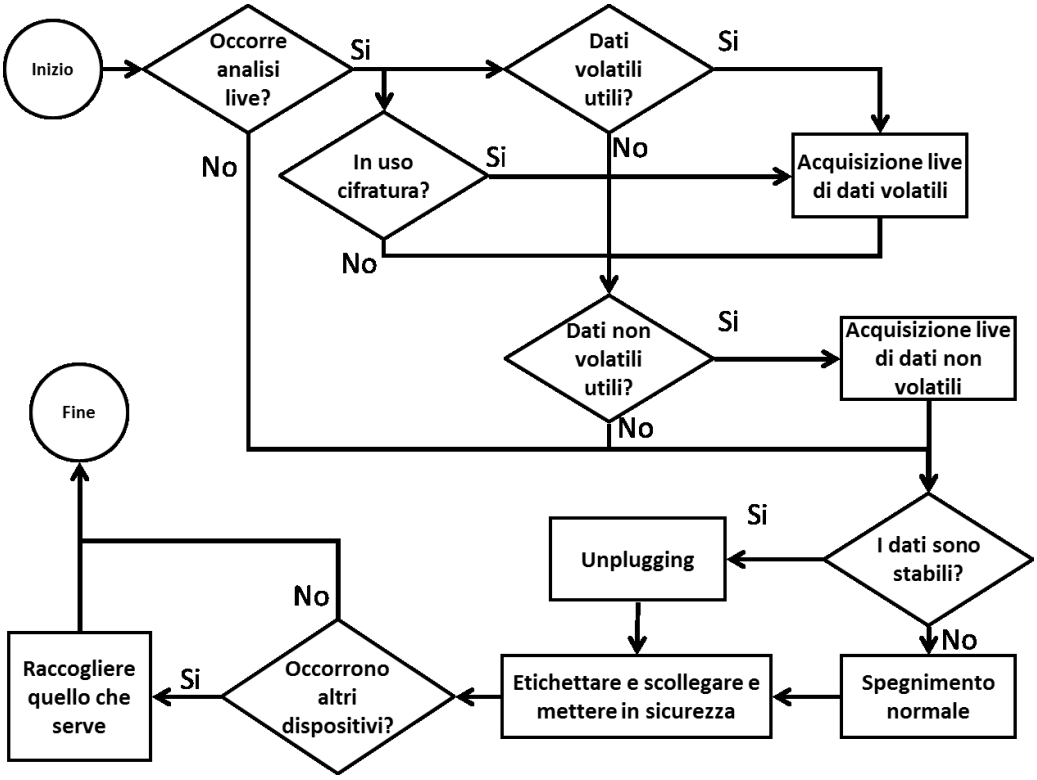


Figura 3 – Linee guida per la raccolta e acquisizione di dispositivi digitali accesi[73]

Si noti che dopo lo spegnimento del sistema (con unplugging o con spegnimento normale), la procedura si riconduce a quella dello schema precedente per i dispositivi spenti.

1.8.3. Acquisizione

L'acquisizione è il processo di produzione di una copia di evidenze digitali detta copia forense (o bit-stream image, o immagine bit a bit), ovvero una copia completa del supporto compresi spazio non allocati e slack space[74]. Le modalità

[73] Traduzione e sintesi delle figure 2 e 4 riportate nello standard ISO/IEC 27037:2012.

[74] 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. Ad esempio, nell'ultimo caso i dati dello slack space sono sempre dati parzialmente sovrascritti che si collocano nella parte finale di un settore tra la fine del file che aveva allocato il settore stesso e la sua fine. La ricerca per

operative e gli strumenti da utilizzare dipendono dalla situazione, dal costo e dai tempi, ma in ogni caso devono essere dettagliatamente documentati affinché risultino, laddove possibile, riproducibili e verificabili da un consulente tecnico di una delle altre parti.

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[75]. L'identicità tra sorgente e destinazione può essere facilmente provata mediante algoritmi di hash[76], 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 – quale ad esempio l'acquisizione di un sistema live[77] – questa verifica non è possibile pertanto

parola chiave è senza dubbio la metodologia migliore per ricercare elementi utili all'interno di esso.

[75] EWF è un formato proprietario di dati utilizzato per copie forensi ideato da EnCase ma ormai supportato dalla gran parte di software per l'informatica forense.

[76] L'hash 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.

[77] 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, 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, cfr. Gabrini D., Perri P., Specchio G. (2012) Live forensics. *In:* Attanasio A., Costabile G., eds. *IISFA Memberbook 2011*. Experta. 151–200.

occorre ricorrere ad un'approfondita documentazione del processo di acquisizione, anche mediante riprese video e fotografiche.

Nel caso in cui la macchina fosse ancora accesa al momento del sequestro occorre effettuare una prima analisi immediata sul posto perché lo spegnimento provocherebbe la perdita di dati volatili presenti in memoria RAM o nell'area di swap[78] e l'inaccessibilità dei dati protetti da cifratura.

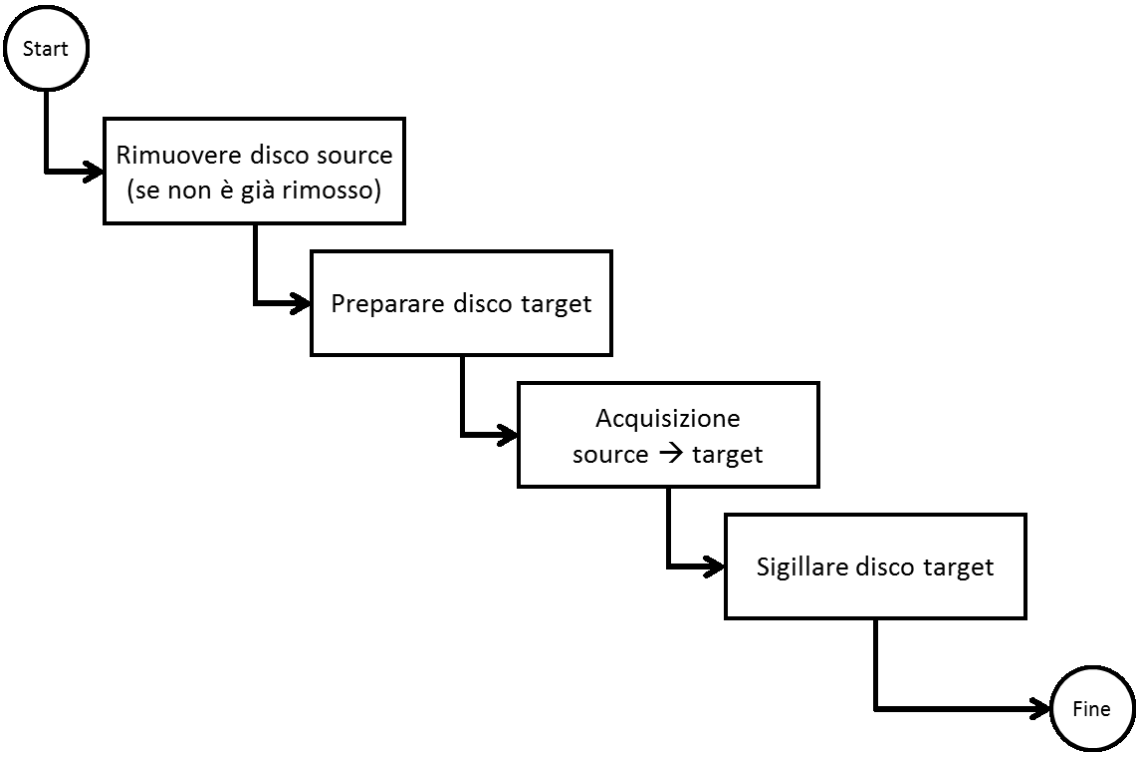


Figura 4 – Linee guida per l'acquisizione di dispositivi digitali spenti[79]

L'analisi live deve dunque verificare le connessioni di rete, le porte[80] aperte, i programmi in esecuzione e il loro comportamento, gli utenti correnti, file, moduli del kernel e device in uso[81].

[78] Con il termine swap si intende l'estensione della capacità della memoria volatile (RAM) oltre il limite fisico attraverso l'utilizzo di uno spazio su un altro supporto fisico di memorizzazione, ad esempio il disco fisso. L'uso dello swap è una delle tecniche impiegate dal sistema operativo per la gestione della memoria virtuale.

[79] Traduzione della figura 5 riportata nello standard ISO/IEC 27037:2012.

[80] La porta di rete è lo strumento utilizzato per permettere ad un computer di effettuare più connessioni contemporanee verso altri calcolatori, facendo in modo che i dati contenuti nei

Quindi può essere spenta e disconnessa dalla rete per condurre l'analisi post-mortem, ossia a macchina spenta, che consta in un'indagine sui dati residenti (file di dati e programmi), analisi di file del sistema e registri di log.

Le indagini non vanno svolte sull'hard disk originale ma su una sua copia bit stream: la copia fisica rispetto a quella logica permette di preservare dati apparentemente non presenti sul disco che invece vengono messi in evidenza con un'analisi forense.

1.8.4. Conservazione e trasporto

La 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.

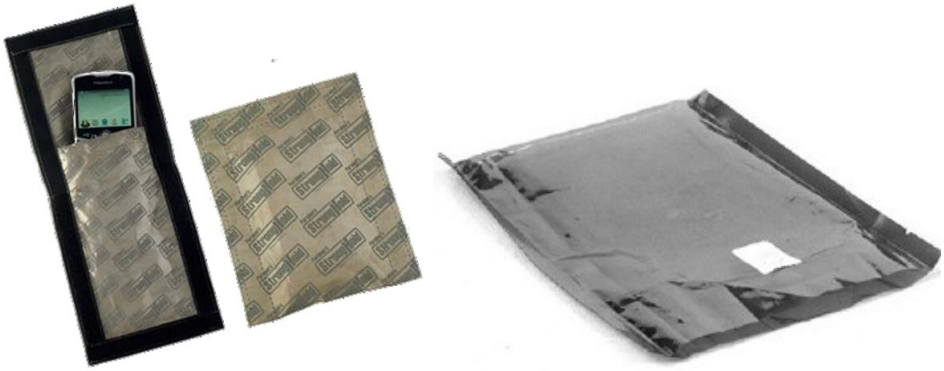


Figura 5 – Materiale per la conservazione finalizzata all'integrità dei dati contenuti all'inter di supporti informatici tipo cellulari e smartphone (a sinistra) e hard disk magnetici (a destra)

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.

pacchetti in arrivo vengano indirizzati al processo che li sta aspettando. Il termine è la traduzione dell'inglese port.

[81] Convey G. (2007) Collecting volatile and non-volatile data. *IISA Journal*, August 2007, 28–31.

1.8.4.1. La catena di custodia

Nella fase di conservazione è fondamentale la catena di custodia, ossia la lista dettagliata di ciò che è stato fatto con le copie acquisite, che deve essere mantenuta 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 anello debole in questa catena potrebbe vanificare l'intero lavoro. In alcuni ordinamenti giuridici (quali ad esempio Colombia o Cile) la catena di custodia è prevista all'interno del codice di procedura penale.

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	

Figura 6 - Esempio di catena di custodia per un reperto informatico

1.8.5. Analisi

Le fasi finora descritte sono abbastanza meccaniche e ripetitive, richiedono esclusivamente una metodologia di lavoro. 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 rilevanti 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 meno 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.[82]

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:

- e-mail: la posta elettronica è una delle fonti più importanti perché mantiene un numero molto alto di informazioni (non solo il testo, ma anche la data, il mittente o il destinatario…);

[82] 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 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; e possibile rinvenire anche tracce della cronologia degli ultimi siti visitati;
- 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[83]; 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[84] o tramite l'analisi di file di log) che a scovare ed analizzare eventuale codice maligno presente nella macchina.

[83] 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.

[84] 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

1.8.6. Valutazione

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.

Va chiarito che il motivo per il quale è necessaria una fase di valutazione del reperto sta nel fatto che il bit vale 0 oppure 1, dunque un'informazione assolutamente povera. Potendo il reperto informatico subire alterazioni, inquinamenti, contraffazioni, occorre accertare se si siano verificati questi eventi, se erano potenzialmente verificabili e chi eventualmente avrebbe potuto compiere queste azioni. Altro aspetto riguarda le operazioni di acquisizioni, per cui bisogna valutare se esse siano state compiute con rigore e in modo corretto nel rispetto della normativa vigente.

Una volta valutati questi requisiti, vanno quindi formulati giudizi in merito all'attendibilità del reperto informatico, nel senso della sua integrità e verificando eventuali alterazioni, e alla sua autenticità, accertando l'autore o gli autori.

1.8.7. Presentazione

L'ultima fase dell'esame forense consiste nella presentazione di tutte le prove rinvenute dal consulente e delle sue conclusioni 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. Questo mezzo è fondamentale per far entrare la "conoscenza" delle attività tecniche svolte in fase di indagine.[85] Deve contenere argomentazioni scientifiche a verifica di tutte le supposizioni. In maniera esaustiva si devono indicare la metodologia usata per analizzare i dati, gli strumenti utilizzati, le scoperte fatte, fornendo una

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.

[85] A proposito di tale aspetto è opportuno precisare che talvolta rappresentare in modo cartaceo tutto ciò che e disponibile in formato elettronico è un'operazione piuttosto complessa soprattutto per la mole dei dati.

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 dovranno illustrare le fasi percorse.

La relazione sarà tanto più efficacemente illustrata ove si affiancheranno anche strumenti audiovisivi (ad esempio slide, registrazioni…), simulazioni e dimostrazioni pratiche a supporto della deposizione.

1.9. Il laboratorio di informatica forense

In via preliminare è doveroso osservare che il laboratorio di informatica forense è un laboratorio scientifico che deve tenere presente una serie di prescrizioni definite all'interno degli standard internazionali universalmente accettati quali, primi tra tutti, ISO/IEC 17025 e ISO/IEC 27037. L'obiettivo principale del laboratorio deve essere il raggiungimento del massimo livello delle garanzie, legali e tecniche, sulla bontà dei risultati, ricordando il pesante riflesso che tali attività hanno comunemente sulla vita delle persone.

Il laboratorio di informatica forense si occupa dell'identificazione, acquisizione ed analisi di elementi di prova da sistemi digitali a fini legali. Data la rapida evoluzione della disciplina e la continua produzione di nuovi sistemi, il laboratorio dovrebbe essere in contatto con altri laboratori omologhi al fine di costituire network investigativo, anche allo scopo di comparare i risultati delle indagini tecniche sia in base ai diversi strumenti software e hardware impiegati, sia in relazione alle varie tipologie di indagini che con il tempo si presentano. Tutto ciò al fine di determinare con sempre maggiore precisione dei protocolli di indagine applicabili nella maggioranza dei casi, evitando di lasciare alla fantasia, all'improvvisazione, all'inesperienza ed all'iniziativa personale dei tecnici la quale ultima va, invece, fortemente impiegata alla presenza di nuove fattispecie di situazioni da indagare[86].

1.9.1. Attività da laboratorio di informatica forense

Le operazioni normalmente eseguite in un laboratorio di informatica forense sono:

[86] Cowen D. (2013) *Computer Forensics InfoSec Pro Guide*. McGraw Hill.

- acquisizioni integrali da dispositivi di memorizzazione di dati digitali di qualsiasi tipo (hard disk, solid state disk, floppy disk, CD, DVD, Blu-Ray, pendrive USB…), nonché di dati digitali memorizzati su dispositivi fisici geograficamente distanti (pagine web, posta elettronica, file in cloud…);
- analisi dei supporti al fine di scoprire ulteriore hardware (dispositivi di memorizzazione di dati digitali, stampanti, videocamere…) che non erano già stati identificati;
- identificare il funzionamento e la gestione del file system di sistemi elettronici nuovi, di scarsa diffusione, ignoti o embedded (ad esempio *cinefonini*[87], fotocopiatrici…);
- recupero di dati (file in chiaro, file cancellati, dati individuati in settori cancellati o slack space) dai vari tipi di file system e di sistemi operativi atti a gestirli, sia relativi al contenuto che ai dati esterni (nomi, date e orari, organizzazione dei file sul file system…);
- ricerca di dati per parola chiave, per tipologia di file, per nome, per contenuto, per intervallo temporale e così via;
- ricostruzione di eventi ed autori analizzando le tracce (timestamp, file di log…) presenti sul reperto analizzato;
- analisi di file cifrati o steganografia al fine di procedere ad attacchi finalizzati all'accesso alle informazioni nascoste;
- analisi di immagini, fotogrammi video, video, registrazioni audio, finalizzata all'individuazione di elementi utili ai fini dell'indagine o al miglioramento degli stessi;
- analisi di traffico di rete finalizzato all'individuazione degli estremi di una comunicazione e del relativo contenuto;
- costruzione delle relazione tra reperti informatici e persone alla luce dei risultati;

[87] Il termine cinefonino è utilizzato per indicare uno smartphone di produzione cinese che risulta estremamente simile tanto nelle forme quanto nel funzionamento ad un apparecchio di un produttore più noto; tuttavia, il cinefonino è equipaggiato con hardware più economico e un sistema operativo più leggero che abbassa notevolmente il prezzo del bene sul mercato. La diffusione è limitata sia per gli aspetti qualitativi dell'hardware e del software, sia per la complessità di approvvigionamento che di norma avviene solo mediante siti di e-commerce esteri o di aste (ad esempio eBay). Ai fini dell'informatica forense un apparecchio di questo tipo risulta di elevata complessità di analisi in ragione del fatto che non esiste alcuno standard di produzione e il numero di pezzi circolanti sul mercato è basso.

- ricostruzione di ambienti di analisi virtualizzati mediante l'uso di macchine virtuale[88].

1.9.2. Ruoli e compiti del personale del laboratorio di informatica forense

Importante nel laboratorio di informatica forense è la definizione di ruoli e responsabilità del personale operante. In molte realtà di piccole dimensioni una persona potrebbe assumere anche più, o tutti, i seguenti ruoli:

- responsabile del laboratorio: persona responsabile per il corretto svolgimento di tutte le attività di analisi forense, per l'interpretazione giuridica dei dati tecnici individuati, nonché per la gestione amministrativa tra cui valutazioni di investimenti;
- responsabile per l'indagine: persona con competenza mista tra il tecnico il e giuridico che ha il compito di supervisionare tutte le analisi forensi che attengono uno stesso caso, raccoglierne i risultati, sintetizzarli ed interpretarli anche da un punto di vista legale per poi presentarli formalmente in dibattimento;
- specialista tecnico: operatore tecnico che svolge e coordina le analisi forensi e trascrive documentazione di riepilogo squisitamente tecnica soddisfando le richiesta del responsabile per l'indagine;
- analista: operatore tecnico forense in grado di utilizzare specifici tool per svolgere determinate analisi al fine di coadiuvare l'attività dello specialista tecnico che rimane controllore e responsabile comunque per un certo insieme di analisi.

1.9.3. Gestione documentale del laboratorio di informatica forense

Per quanto concerne i processi di documentazione, il laboratorio efficace gestisce almeno la seguente tipologia di documentazione:

- i movimenti di materiali in ingresso ed uscita ivi inclusi i reperti da analizzare che devono essere accompagnati da un documento di catena di custodia;

[88] Questo genere di analisi è particolarmente indicato per soddisfare una richiesta di esperimento giudiziale (artt. 218 e 219 c.p.p.). Peraltro, a differenza di quanto accade per altre scienze forensi, nell'informatica forense un esperimento giudiziale che fa uso di macchine virtuali potrebbe portare a risultati estremamente prossimi, se non addirittura aderenti, ai fatti realmente accaduti.

- registrazione delle persone che hanno accesso al laboratorio, motivo e durata dell'accesso, responsabile dell'accesso;
- i fascicoli di indagine relativi a ciascun caso affrontato;
- le comunicazioni formali interne al laboratorio e quelle da e verso l'esterno;
- i report delle indagini tecniche e tutte le versioni dei documenti;
- tracciamento di costi ed entrate per aree di gestione e per caso;
- inventario degli strumenti tecnici impiegati, del loro testing, del loro impiego;
- gestione della qualità mediante produzione di un manuale di qualità;
- gestione degli standard operativi;
- documentazione utili per la formazione[89].

1.9.4. Strumenti hardware e software per l'acquisizione

Le attività forensi richiedono un metodo improntato a garantire che il dato sia trattato in modo adeguato e che preservi le sue caratteristiche e la sua genuinità per tutta la durata dell'attività d'indagine. Per le prime attività tecniche esistono strumenti software open source e gratuiti che consentono di avvicinarsi alla digital forensics senza particolari investimenti[90]; tuttavia spesso gli strumenti opensouce non sono ottimizzati per determinati compiti, né sono costantemente aggiornati, pertanto è certamente importante – se non necessario – usufruire di attrezzature più professionali che consentano di eseguire le operazioni in maniera più rapida ed efficace.

Gli strumenti e i software da utilizzare per l'acquisizione di supporti informatici sono naturalmente variabili in funzione della tipologia di supporto: basti pensare che solo per l'acquisizione dei due supporti più classici e diffusi (hard disk e smartphone) sia le apparecchiature hardware che i software sono completamente diversi.

In generale il requisito indispensabile in ogni stazione di acquisizione è il blocco in scrittura, soluzione che può essere implementata in due modi:

[89] Sul punto, autorevoli indicazioni sono fornite dall'Ufficiale dell'Arma dei Carabinieri Marco Mattiucci sul sito personale all'url *http://www.marcomattiucci.it/lab.php*.

[90] Grillo A. (2012) Indagini digitali mediante strumenti Open Source e Freeware. *In:* Carretta P., Cilli A., Iacoviello A., Grillo A., Trocchi F. *L'acquisizione del documento informatico. Indagini penali e amministrative*. LaurusRobuffo. 107–202.

- lo strumento impedisce i tentativi di scrittura informando il sistema operativo dell'impossibilità di completare l'operazione;
- lo strumento memorizza i tentativi di scrittura per tutta la sessione, facendo credere al sistema operativo che le operazioni di scrittura si siano realmente concluse correttamente.

Per quanto concerne i supporti tipo hard disk, dischi allo stato solido, supporti ottici, floppy (nelle varie dimensioni), chiavette USB e nastri, a parte gli opportuni cavi e lettori idonei, uno strumento certamente affidabile e gratuito è il comando `dd` presente nei sistemi operativi Linux[91]; Linux consente infatti l'accesso ai device in sola lettura, non richiedendo in tal modo alcun hardware aggiuntivo che provveda ad impedire gli accessi in scrittura. Esistono numerose distribuzioni Linux che raccolgono un insieme di software specifici per la computer forensics (non solo per acquisizione, ma anche per analisi) che sono chiamate distribuzioni forensi[92].

Anche se sconsigliato in quanto non verificabile, il sistema operativo Microsoft Windows offre la possibilità di acquisire supporti informatici senza la necessità di utilizzare come intermediario un dispositivo hardware che blocchi la scrittura apportando un'opportuna voce di registro[93]. In generale, per evitare di alterare – anche accidentalmente – un reperto informatico è buona prassi utilizzare un write blocker[94]. Per l'acquisizione vera e propria sono poi disponibili diversi software che prevedono anche la compressione (uno dei più noti è EnCase ma ne esistono altri come FTK della AccessData).

---

[91] `dd` è un comando dei sistemi operativi Unix-like (tra cui Linux) che copia dei dati in blocchi, ignorando la struttura del file system e lavorando direttamente sui bit: in tal modo non è in grado di distinguere tra file in chiaro e file cancellati e tutti i bit vengono ricopiati allo stesso modo.

[92] DEFT (*http://www.deftlinux.net*), CAINE (*http://www.caine-live.net*), SIFT (*http://digital-forensics.sans.org/community/downloads*), ForLEx (*http://www.forlex.it*), NetSecL (*http://netsecl.com*), Swift Linux (*http://www.swiftlinux.org*), Matriux (*http://www.matriux.com*), BackBox Linux (*http://www.backbox.org*), Kali Linux (*http://www.kali.org*) sono le distribuzioni attive maggiormente diffuse tra gli addetti ai lavori.

[93] Per abilitare il blocco in scrittura su dispositive connessi attraverso porta usb, alla voce `WriteProtect` del registro `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies` occorre impostare il valore `1` invece che `0`.

[94] Trocchi F. (2012) Computer forensics e procedure standardizzate. *In:* Carretta P., Cilli A., Iacoviello A., Grillo A., Trocchi F. *L'acquisizione del documento informatico. Indagini penali e amministrative*. LaurusRobuffo. 69–105.

Figura 7 – Esempi di write blocker prodotti da Tableau (a sinistra) e Wiebetech (a destra)

Figura 8 – Esempio di write blocker interno (Tableau T35i)

Il write blocker è uno strumento hardware che consente di leggere i dati dal supporto impedendone la modifica. L'uso di questo tipo di strumento è certamente consigliato quando si operano acquisizioni con i sistemi operativi Windows che sono estremamente invasivi e possono portare alterazione di dati con la sola connessione del dispositivo di memorizzazione di dati digitali[95].

[95] Barrett D., Broom N., Rudolph K., Salomon M., Tittel E. (2011) *Computer forensics jumpstart*. Second edition. Sybex.

Figura 9 – Esempio di una postazione di acquisizione che fa uso di writeblocker esterno

Figura 10 – Esempio di postazione che fa uso di writeblocker usb

In alternativa all'uso di personal computer (ed eventualmente writeblocker) è possibile utilizzare dei dispositivi hardware costruiti appositamente per l'acquisizione di supporti informatici. Tali dispositivi, noti come copiatori hardware, consentono di acquisire in modalità clone o immagine – talvolta anche compressa – e di calcolare le impronte hash.

Figura 11 – Esempio di copiatore hardware per hard disk (Tableau TD3)

Nella generazione di una copia forense è d'obbligo calcolare un'impronta che contraddistingua in maniera univoca la traccia informatica oggetto dell'analisi forense al fine di ottemperare alle citate esigenze di integrità del dato. Tale sigillo di garanzia viene creato con il calcolo dell'hash e costituisce un riferimento certo alla traccia originale. Un ulteriore strumento a garanzia da utilizzare per fissare in maniera certa nel tempo le acquisizioni è la marca temporale che consente di collocare nel tempo le operazioni svolte[96].

1.9.5. Analisi forense di supporti di memorizzazione di dati digitali

L'analisi dei supporti di memorizzazione di dati digitali è estremamente variabile e dipende dall'obiettivo da perseguire. A titolo puramente esemplificativo si riportano alcune delle possibili attività:

- recupero di dati di tipo documentale;
- ricerca di dati per parola chiave, per tipologia di file, per nome, per contenuto, per intervallo temporale…;

[96] L'utilizzo della marca temporale è di fondamentale importanza soprattutto nei procedimenti civili quando l'acquisizione viene eseguita dalla parte che intende produrre una prova immediatamente dopo avere disponibilità del reperto informatico: il caso tipico è la produzione di una copia forense del computer dato in uso al dipendente che viene acquisito subito dopo la riconsegna.

- individuazione di elementi utili ad apprezzare la condotta di un dipendente infedele;
- individuazione di tracce relative a danneggiamento informatico;
- ricerca di file con contenuto pedopornografico e di elementi utili ad apprezzare il possesso consapevole (o, viceversa, il possesso inconsapevole).

1.9.5.1. Analisi forense di dispositivi mobili

In un'accezione più ampia, i dispositivi mobili comprendono tutti i dispositivi che possono essere facilmente spostati e contenuti in una tasca quali ad esempio riproduttori portatili di file multimediali, navigatori satellitari, cellulari, smartphone e tablet. L'evoluzione della tecnologia ha portato alla realizzazione di strumenti che hanno capacità computazionale paragonabile a quella dei computer: per meglio rendere l'idea, uno smartphone di oggi offre prestazioni migliori della maggior parte dei sistemi informatici commercializzati solo un decennio fa.

In generale i dispositivi mobili mantengono dati:

- nella memoria interna;
- nella memoria esterna rimovibile;
- nella scheda SIM.

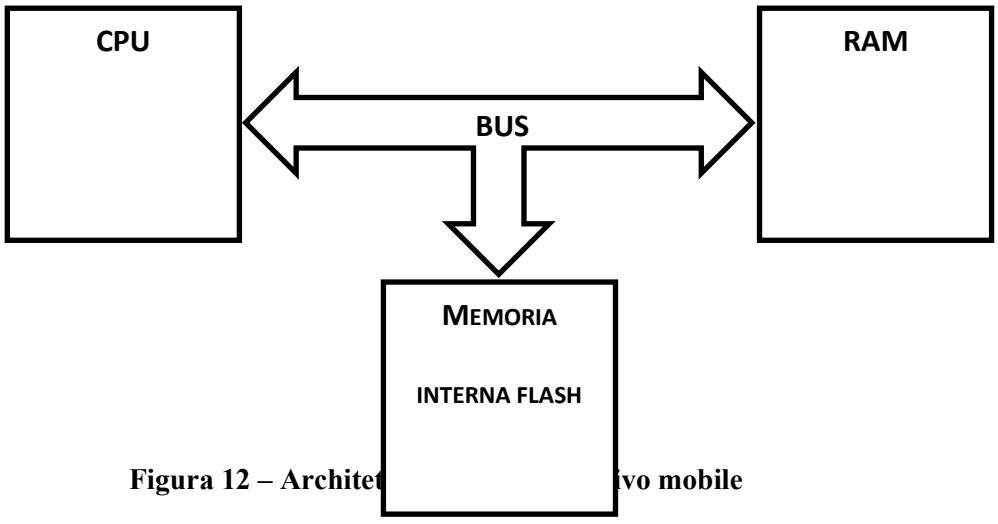


Figura 12 – Architet ivo mobile

Per l'acquisizione e l'analisi della memoria esterna rimovibile si possono utilizzare le comuni tecniche di computer forensics relative ad acquisizione ed analisi di dispositivi di memorizzazione di dati digitali, mentre per la scheda

SIM esistono ormai consolidate modalità di acquisizione ed analisi con tool quali SIMcon[97] o Paraben SIM Card Seizure[98]. L'attività è più complessa allorquando si rende necessaria l'acquisizione e l'analisi dell'hardware del dispositivo mobile (privo di SIM e memoria esterna) che tuttavia fornisce la maggiore quantità di risultati utili all'indagine[99].

Figura 13 – Esempio di dispositivo hardware per l'acquisizione di supporti tipo cellulari, smartphone, tablet e schede SIM (Cellebrite UFED Touch)

L'analisi può essere condotta in due modalità:

- invasiva: estrazione fisica del chip di memoria[100] oppure accesso come "root" al sistema, sfruttando tecniche di hacking che consentono di avere il completo controllo del dispositivo;
- non invasiva: acquisizione e ricostruzione dei dati collegando il dispositivo mobile ad una sistema informatico il quale, mediante un software specializzato, provvede al recupero dei dati rilevanti

[97] *http://www.simcon.no/*.

[98] *https://www.paraben.com/sim-card-seizure.html*.

[99] Si citano dunque alcuni dei prodotti che attualmente vanno per la maggiore in relazione all'acquisizione e l'analisi di dispositivi mobili : il più noto ed efficace è certamente l'UFED della Cellebrite (*http://www.cellebrite.com*), ma molto validi sono anche i software Oxygen Forensics Suite (*http://www.oxygen-forensic.com*), Paraben Device Seizure (*http://www.paraben.com/device-seizure.html*) e MobilEdit (*http://www.mobiledit.com*).

[100] Willassen S. (2005) Forensic Analysis of Mobile Phone Internal Memory. *In:* Pollitt M., Shenoi S. (eds.) *Advances in Digital Forensics - IFIP International Conference on Digital Forensics*, National Center for Forensic Science, 191–204.

(eventualmente anche cancellati) come SMS, lista chiamate, rubrica…; in realtà, non sapendo esattamente in che modo tali software si interfacciano con il dispositivo, sarebbe opportuno considerare anche questa tecnica come invasiva, con la conseguenza che in generale l'acquisizione di dispositivi mobili andrebbe effettuata con le garanzie previste dall'art. 360 c.p.p. in tema di accertamenti tecnici non ripetibili.

1.9.5.2. Acquisizione e analisi forense di traffico telematico

Il dato informatico può risiedere all'interno dei sistemi informatici così come può essere trasferito attraverso la rete da un sistema all'altro: in tal caso la modalità di acquisizione del dato è l'intercettazione del traffico telematico generato e ricevuto dal sistema informatico.

Le intercettazione telematiche si possono suddividere in due categorie:

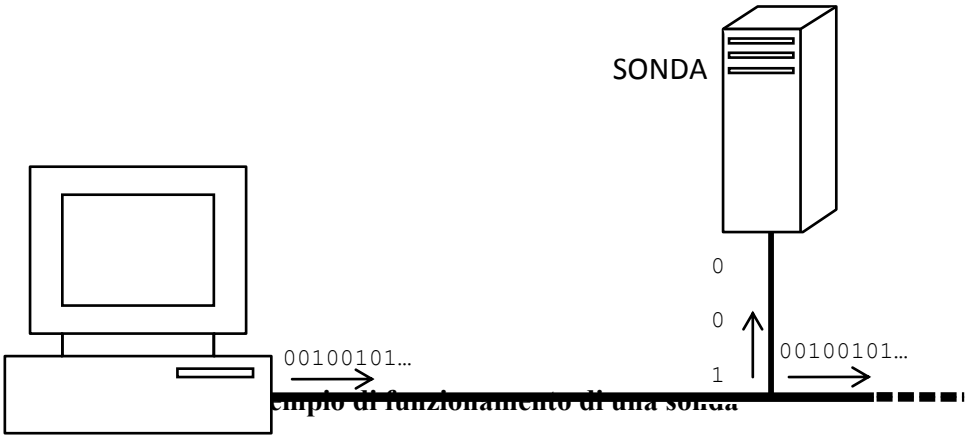
- singole: monitoraggio di tutto il traffico di uno specifico utente a prescindere dal protocollo utilizzato e dal contenuto delle comunicazioni;
- parametriche: monitoraggio del traffico che risponde a determinati requisiti, quali ad esempio la presenza di una determinata sequenza di bit nel flusso; solitamente le intercettazioni parametriche avvengono su aree geografiche molto vaste.

Dal punto di vista architetturale un sistema di intercettazione si compone di tre parti[101]:

- strumento di cattura: apparato hardware e software (sonda) capace di interfacciarsi con la rete da monitorare e di produrre una copia del traffico di interesse selezionato tramite regole di filtraggio predefinite;
- elaboratore: apparato (core) preposto alla ricostruzione ed elaborazione delle sessioni di comunicazione dalle quali vengono estratte tutte le informazioni ricercate;
- strumento di visualizzazione ed analisi: apparato (viewer) che consente l'utilizzo delle informazioni raccolte e la riproduzione dei contenuti a livello applicativo della pila dei protocolli[102].

[101] Aterno S., Cajani F., Costabile G., Mattiucci M., Mazzaraco G. (2011) *Computer forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*. Experta. Vol. II.

L'intercettazione è quindi effettivamente realizzata dalla sonda che si pone l'obiettivo di rimanere trasparente al sistema intercettato, non alterare i dati e porsi in ascolto al fine di captare passivamente (in gergo tecnico "sniffare") tutto ciò che è in transito.



Esempio di funzionamento di una sonda

La sonda memorizza tutte le comunicazioni che riguardano il sistema informatico da monitorare, ponendosi nella una zona topologicamente più prossima al sistema al fine di minimizzare la quantità di dati non rilevanti e interfacciandosi con i vari canali di comunicazione utilizzati (rete locale LAN o wireless, doppino telefonico, ponti radio…): ad esempio, se il sistema informatico oggetto di analisi è collegato ad una rete LAN, la sonda andrebbe collegata allo switch[103] di rete cui è collegato il sistema stesso, possibilmente sfruttando la span port[104], oppure posizionando la sonda tra il sistema e lo switch.

[102] L'International Organization for Standardization (ISO) nel 1979 ha definito la pila di protocolli Open Systems Interconnection (OSI), nota anche come pila ISO/OSI, con l'intenzione di creare uno standard per le telecomunicazioni da usare nelle reti di tutto il mondo. All'atto pratico però, lo standard de facto che viene comunemente usato nella maggior parte delle reti, è la pila TCP/IP, definita nella RFC 1155, che è una versione ridotta della pila ISO/OSI.

[103] Lo switch è un dispositivo di rete che si occupa di indirizzare ed instradare a livello 2 della pila ISO/OSI (*datalink*) all'interno di reti locali attraverso indirizzi MAC. Si differenzia dal router che instrada invece a livello 3 (*internetworking*) interconnettendo più reti locali attraverso il protocollo IP. Nel gergo comune tuttavia i termini switch e router vengono spesso utilizzati come sinonimi intendendo uno strumento che si occupa di instradamento di pacchetti.

[104] La span port è una porta dello switch che replica tutto il traffico scambiato con un sistema prefissato.

WireShark[105] è uno dei principali software (peraltro opensource) per il monitoraggio e l'analisi del traffico di rete[106]; in ambito di informatica forense si rende utile anche nelle acquisizioni forensi di contenuti disponibili in rete per i quali occorre anche il congelamento dell'intero traffico di rete generato nella sessione di scaricamento dei dati dalla rete.

[105] *http://www.wireshark.org*.

[106] Nelson B., Phillips A., Enfinger F., Steuart C. (2009) *Guide to computer forensics and investigation*. 4th edition. Cengage learning.

CAPITOLO 2

2. Disciplina giuridica dell'informatica forense e della pedopornografia

2.1. Disciplina giuridica sull'informatica forense

I reati informatici fanno la loro comparsa nell'ordinamento giuridico italiano alla fine del 1993 quando con la Legge 23 dicembre 1993, n. 547[107], vengono introdotti i reati di danneggiamento di sistemi informatici o telematici, falso informatico, frode informatica, accesso abusivo a sistema informatico o telematico, detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, diffusione di programmi diretti a danneggiare o interrompere un sistema informatico, intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche, installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche, falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche; inoltre, i reati relativi alla corrispondenza "analogica" vengono estesi alla corrispondenza informatica o telematica. La legge introduce altresì delle modifiche nel codice di procedura penale in relazione ad intercettazioni di comunicazioni informatiche o telematiche.

Alcuni anni dopo, la lista dei reati informatici viene estesa con la Legge 269 del 3 agosto 1998[108] che introduce nel codice penale i reati relativi alla pedopornografia.

Lo studio delle tematiche connesse all'accertamento dei reati informatici non può oggi prescindere dalla novella più importante in tema di informatica forense quale è la Legge di ratifica della Convenzione di Budapest sul

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

[108] 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".

Cybercrime[109], il testo normativo del 2001 che rappresenta il primo accordo internazionale in tema di crimini commessi attraverso sistemi informatici e telematici, Internet e altre reti informatiche.

La Convenzione sul Cybercrime si propone di armonizzare i crimini informatici, predisporre un regime rapido ed efficace di cooperazione internazionale, creare una normativa comune sovranazionale, prevedere procedure più snelle nell'ambito di sequestri, perquisizioni e intercettazioni, assegnare poteri necessari al perseguimento delle infrazioni a questo tipo di crimini nel diritto processuale nazionale.

Allo stato attuale, i crimini informatici definiti nell'ordinamento giuridico nazionale sono[110]:

- reati informatici puri:
    - accesso abusivo a sistema informatico (art. 615-ter c.p.);
    - detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.);
    - diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico (art. 615-quinquies c.p.);
    - installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche (art. 617-bis c.p.);
    - falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche (art. 617-ter c.p.);
    - intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.);
    - installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.);

[109] Legge 18 marzo 2008, n. 48. "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno".

[110] Aterno S., Cajani F., Costabile G., Mattiucci, M., Mazzaraco G. (2011) *Computer forensics e indagini digitali*. *Op. cit.*, vol. I.

- falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617-sexies c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da un altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.);
- danneggiamento di sistemi informatici e telematici (art. 635-quater c.p.);
- danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635-quinquies c.p.);
- truffa[111] (art. 640 c.p.);
- frode informatica (art. 640-ter c.p.);
- frode informatica del soggetto che presta servizi di certificazione di firma digitale (art. 640-quinquies c.p.);

- falsità in documenti informatici pubblici o privati aventi efficacia probatoria[112] (Capo III, Titolo VII c.p., in relazione alla previsione di cui all'art. 491-bis c.p.);
- diffamazione online (art. 595 comma 3 c.p., trattandosi di offesa arrecata "con altro mezzo di pubblicità"[113]);
- reati attinenti la pedopornografia online[114]
  - prostituzione minorile[115] (art. 600-bis c.p.);

[111] S'intende il caso in cui gli artifici o i raggiri consistano in condotte poste in essere con l'ausilio di strumenti informatici e/o avvalendosi della rete Internet o di piattaforme di comunicazione o commercio elettronico.

[112] Tonini P. (2009) Documento informatico e giusto processo. In *Diritto penale e processo*, 4/2009, 401–406.

[113] Sull'impossibilità di equiparare Internet alla nozione di stampa, agli effetti di incriminazione penale cfr. Zeno Zencovich V. (1998) La pretesa estensione alla telematica del regime della stampa: note critiche. In *Il diritto dell'informazione e dell'informatica*, Giuffrè, 15.

[114] Introdotti con la Legge 3 agosto 1998, n. 269 cd. "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù" e successivamente modificati con Legge 6 febbraio 2006, n. 38 cd. "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet", Legge 1 ottobre 2012, n. 172, cd. "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, nonché norme di adeguamento dell'ordinamento interno".

    - pornografia minorile (art. 600-ter c.p.);
    - detenzione di materiale pornografico (art. 600-quater c.p.);
    - pornografia virtuale (art. 600-quater.1 c.p.);
    - adescamento di minorenni (art. 609-undicies c.p.);
- tutela penale dei reati commessi con carte di credito e altri strumenti di pagamento (art. 55 comma 9 d.lgs. 21 novembre 2007, n. 231);
- tutela penale del cd. diritto d'autore online (artt. 171, 171-bis, 171-ter, 171-quater della Legge 22 aprile 1941, n. 633);
- tutela penale della cd. privacy online (art. 167 d.lgs. 30 giugno 2003, n. 196).

2.1.1. Convenzione di Budapest e Legge 18 marzo 2008, n. 48 di ratifica

L'iniziativa legislativa più importante nel settore dell'informatica forense è senza dubbio rappresentata dalla Convenzione adottata dal Consiglio d'Europa, elaborata da parte di un Comitato composto da 22 esperti provenienti da alcuni dei 41 Paesi del Consiglio e da osservatori di importanti Paesi extraeuropei (USA, Canada, Giappone, Sud Africa) e dei delegati di alcune delle maggiori organizzazioni internazionali (Interpol, Unione Europea, Unesco), aperta alla firma a Budapest il 23 novembre 2001 e sottoscritta immediatamente da ben 30 Paesi tra cui l'Italia.

[115] Cfr. Catullo F. (2004) Nota in tema di pornografia minorile e di prostituzione via Internet. *Cassazione penale*, XLIV, novembre 2004, 3577–3585. Sulla nozione di "prostituzione online" è intervenuta la Cassazione, Sez. III, 8 giugno 2004, n. 25464, di cui si riporta parzialmente e si commenta la massima: "L'elemento che caratterizza l'atto di prostituzione non è necessariamente costituito del contatto fisico tra i soggetti della prestazione, bensì dal fatto che un qualsiasi atto sessuale venga compiuto dietro pagamento di un corrispettivo e risulti finalizzato, in via diretta ed immediata, a soddisfare la libidine di colui che ha chiesto e che è destinatario della prestazione. Per l'esistenza delle condotte vietate dalla Legge. n. 75 del 1958, quindi, è irrilevante il fatto che chi si prostituisce e il fruitore della prestazione si trovino in luoghi diversi, allorché gli stessi risultino collegati, tramite internet, in videoconferenza, che consente all'utente di interagire con il minore, in modo da potergli chiedere il compimento di atti sessuali determinati". La conclusione cui è pervenuto il giudice di legittimità è consistita nel riscontrare che l'interpretazione giurisprudenziale non ha mai identificato la nozione di atto di prostituzione con quello di congiunzione carnale, pertanto va inteso come qualsiasi atto sessuale che viene compiuto per soddisfare la libido del destinatario dietro pagamento di un corrispettivo; è irrilevante poi che chi si prostituisce e il fruitore della prestazione si trovino in luoghi diversi, allorché gli stessi riescono a interagire tra loro.

La Convenzione di Budapest ha il compito di delineare definizioni comuni di reato tra i vari paesi, definire poteri comuni di indagine e predisporre mezzi di cooperazione internazionale.

Nel primo capitolo, costituito da un unico articolo, vengono preliminarmente fornite le seguenti quattro definizioni:

- per "sistema informatico" si intende 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;
- per "dati informatici" si intende qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione;
- per "service provider" si intende qualunque entità pubblica o privata che fornisce agli utenti dei propri servizi la possibilità di comunicare attraverso un sistema informatico, nonché qualunque altra entità che processa o archivia dati informatici per conto di tale servizio di comunicazione o per utenti di tale servizio;
- per "trasmissione di dati" si intende qualsiasi informazione computerizzata relativa ad una comunicazione attraverso un sistema informatico che costituisce una parte nella catena di comunicazione, indicando l'origine della comunicazione, la destinazione, il percorso, il tempo, la data, la grandezza, la durata o il tipo del servizio.

Nel secondo capitolo della Convenzione vengono enucleati i provvedimenti da adottare a livello nazionale in tema di diritto penale sostanziale – in relazione a accesso illegale, intercettazione illegale, attentato all'integrità dei dati, attentato all'integrità di un sistema, abuso di apparecchiature, falsificazione informatica, frode informatica, reati relativi alla pornografia infantile, reati contro la proprietà intellettuale e diritti collegati, tentativo e complicità, responsabilità delle persone giuridiche, sanzioni e strumenti – e procedurale – in relazione a scopo delle disposizioni procedurali, condizioni e tutele, conservazione rapida di dati informatici immagazzinati, conservazione rapida e divulgazione parziale di dati relativi al traffico, perquisizione e sequestro dei dati informatici, raccolta in tempo reale di dati sul traffico, intercettazione di dati relativi ai contenuti. In particolare, gli articoli dal 2 al 10 disciplinano una serie di fattispecie criminose che devono necessariamente essere presenti in tutti gli Stati firmatari in modo da garantire una omogeneità

delle incriminazioni: tra questi, all'art. 9, viene prende in considerazione il fenomeno della pedopornografia, dove con l'espressione "pornografia infantile" si intende il materiale che raffigura un minore coinvolto in un comportamento sessuale esplicito o un soggetto che sembra essere un minore coinvolto in un comportamento sessuale esplicito (fenomeno denominato pornografia virtuale). Gli altri articoli mirano alla regolamentazione della responsabilità delle persone giuridiche e delle sanzioni applicabili (articoli da 11 a 13) e alla definizione della disciplina processuale (articoli da 14 a 22) all'interno della quale particolare interesse rivestono le norme che concernono le modalità per garantire una tempestiva assicurazione dei dati elettronici archiviati suscettibili di essere alterati o modificati.

Nel terzo capitolo vengono definite le disposizioni in tema di cooperazione internazionale per quanto concerne la mutua assistenza relativa a misure provvisorie – conservazione e divulgazione rapida di dati informatici – nonché a poteri d'indagine – assistenza relativa all'accesso a dati informatici immagazzinati, accesso transfrontaliero a dati informatici immagazzinati con il consenso o qualora essi siano pubblicamente disponibili, mutua assistenza nella conservazione in tempo reale di dati sul traffico, mutua assistenza in materia di intercettazione di dati relativi ai contenuti – e istituzione di una rete di controllo e repressione attiva sul modello 24/7.

Il primo luglio del 2004 è stata raggiunta la condizione per l'entrata in vigore della Convenzione, che era stata stabilita al raggiungimento di cinque ratifiche, di cui almeno tre di stati del Consiglio d'Europa.

Sebbene nel nome richiami esplicitamente i crimini informatici, l'ambito di applicazione della Convenzione di Budapest sul Cybercrime è di estrema rilevanza per tutti gli operatori del diritto in quanto non comprende solo i reati informatici puri, ma anche tutti i reati "comuni" commessi attraverso un sistema informatico o le cui prove sono in formato digitale.

La Legge 18 marzo 2008, n. 48, cd. "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", apporta limitate modifiche al codice penale avendo l'Italia già provveduto ad introdurre i reati informatici nell'ordinamento nazionale negli anni precedenti[116]. Vengono introdotte nel codice di procedura penale alcune

[116] Tra le novità apportate dalla legge 48/2008 si citano la modifica dell'art. 491-bis in tema di documento informatico, la previsione di perquisizioni informatiche (art. 247 c.p.p.

norme di rilievo per quanto riguarda l'acquisizione e il recupero di dati sui quali intraprendere un'indagine informatico forense: in relazione a sistemi informatici o telematici, la nuova formulazione dell'art. 244 comma 2 c.p.p. prevede la necessità di adottare le misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedire l'alterazione; in tutti i casi in cui sussista fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, la nuova formulazione dell'art. 247 comma 1-bis c.p.p., prevede che ne venga disposta la perquisizione adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

La legge n. 48/2008 è stata sottoposta a diverse critiche[117] in ordine alle modalità e ai tempi della sua approvazione, oltre che al suo contenuto specifico ed alla correlazione ravvisabile tra la sua formulazione ed il testo della Convenzione europea cui ha dato attuazione[118]. Voci critiche hanno sostenuto l'incidenza negativa del fattore temporale, stigmatizzando il contingentamento dei lavori parlamentari che hanno portato ad una rapida approvazione della legge[119]. Gli stessi parlamentari avrebbero individuato nel testo alcune specifiche incongruenze cui tuttavia si è ritenuto di non tener conto[120] per poter

comma 1-bis e 352 c.p.p. comma 1-bis), la previsione di sequestro della corrispondenza telematica (art. 254 c.p.p.) e di dati di traffico (art. 254-bis c.p.p.), l'introduzione del concetto di sigillo elettronico o informatico e copia di dati (art. 260 c.p.p.).

[117] Sul punto, cfr. Sarzana C. (2008) La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa. In *Diritto penale e processo*, 12/2008, 1562–1577.

[118] Picotti L. (2008) Ratifica della convenzione cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo. In *Diritto penale e processo*, 5/2008, 437–448.

[119] Dopo la presentazione del disegno di legge governativo in data 19 giugno 2007 erano state tenute solo due sedute preliminari delle Commissioni Giustizia ed Affari esteri della Camera dei Deputati, che si erano svolte nei giorni del 25 settembre e del 3 ottobre 2007 senza apportare significativi contributi al testo sottoposto ad esame. Dopo il decreto di scioglimento delle Camere e con il consenso pressoché unanime di maggioranza ed opposizione, il 19 febbraio 2008 si era concluso l'esame in sede referente del testo, poi trasmesso all'aula, con emendamento unico, ove veniva tempestivamente approvato e trasmesso al Senato, portando alla definitiva approvazione del 27 febbraio 2008 ed alla pubblicazione in Gazzetta Ufficiale il 4 aprile 2008 con entrata in vigore il giorno successivo.

[120] Cfr. Picotti L. (2008) La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale. In *Diritto penale e processo*, 6/2008, pag. 700–716. L'autore evidenzia come nonostante la delicatezza della materia e l'individuazione di incongruenze normative, si fosse comunque preferito dare rapida attuazione alla legge

realizzare il primario obiettivo dell'immediato adeguamento dell'ordinamento giuridico italiano alla normativa sul cybercrime. Inoltre è stato osservato che la piena ed intera esecuzione, che ai sensi del disposto dell'art. 2 della legge è stata formalmente data alla Convenzione di Budapest, nella sostanza non corrisponderebbe all'effettivo contenuto della legge di ratifica: in particolare si ritiene che le disposizioni previste dagli articoli dal 3 al 6, nell'introdurre o modificare articoli del codice penale, spesso si discostano dai dettami della Convenzione di Budapest, rispondendo piuttosto ad autonome scelte del legislatore nazionale che ha colto l'occasione per rivedere parti controverse della disciplina già vigente in materia[121].

2.2. Disciplina giuridica della pedopornografia

La prima definizione di pedopornografia è fornita dal protocollo opzionale dell'ONU sulla vendita di bambini, la prostituzione minorile e la pedopornografia, dove per pornografia rappresentante bambini s'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 soprattutto sessuali".

Soprattutto tra i non addetti ai lavori, la Rete è considerata per molti aspetti una minaccia per l'integrità dei minori piuttosto che una risorsa per il loro sviluppo psicosociale, anche se in alcuni paesi si sta affermando la formazione nelle scuole mediante l'uso di strumenti tecnologici come i tablet a integrazione dei classici libri cartacei. La fruizione di minori sessualizzati per piacere degli adulti, già nota nell'antica Grecia, ha conosciuto uno sviluppo significativo a partire dagli anni Settanta del Novecento, durante i quali si assiste all'emergere di attività commerciali fortemente lucrative, trovando estrema diffusione grazie alle innovazioni introdotte dall'informatica. La dimensione virtuale infatti è in grado di mediare le interazioni e i rapporti fra i soggetti e può rappresentare un fattore capace di attenuare la reale percezione dei crimini, sostenuta dall'assenza di quei freni inibitori presenti nelle relazioni face-to-face. La digitalizzazione ha di fatto facilitato la diffusione di materiali audiovisivi aventi

nell'auspicio che la magistratura sarebbe stata in grado di superare le inadeguatezze in sede interpretativa.

[121] A tal proposito, emblematica tra le altre sarebbe proprio la previsione della nuova norma incriminatrice dell'art. 495-bis c.p. in tema di "falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri", estranea al contenuto della Convenzione.

come attori minori e le modalità di scambio materiale pedopornografico per quanto attiene Internet sono le seguenti:

- siti web (di solito ad accesso riservato) e in generale risorse presenti nel deep web[122];
- canali di chat che implementano anche funzionalità accessorie per l'invio di file;
- reti peer-to-peer per le attività di file sharing;
- newsgroup a tema.

Il contrasto ai crimini commessi nei confronti di minori mediante l'uso di strumenti informatici ha richiesto, come per gli altri crimini informatici, la rivisitazione delle fattispecie tradizionalmente previste che mostrano tutti i loro limiti di fronte a fenomeni sempre meno legati al contesto locale e circoscritto. Gli interventi normativi che si sono susseguiti negli anni s'inscrivono all'interno di un progetto globale di tutela dell'infanzia contro ogni forma di violenza e sfruttamento che richiede l'elaborazione di strategie, preventive e repressive, di portata mondiale. In questa prospettiva sono di fondamentale importanza i numerosi documenti internazionali che, a partire dalla Dichiarazione dei Diritti del Fanciullo[123] fino alla più recente Convenzione di

[122] Il "deep web" (noto anche come "web sommerso" o "web invisibile") è l'insieme delle risorse del World Wide Web non segnalate dai motori di ricerca. Tali risorse possono essere così catalogate: contenuti dinamici, cioè pagine web dinamiche il cui contenuto viene generato all'atto della richiesta dal server in seguito ad alcuni parametri (browser, indirizzo IP di provenienza, dati inseriti all'interno di un form, credenziali specifiche di accesso…); pagine non collegate, ossia pagine web isolate che non sono raggiungibili da link di altre pagine già note ai motori di ricerca; pagine ad accesso ristretto: pagine che richiedono l'inserimento di opportune credenziali che limitano l'accesso anche ai motori di ricerca.

[123] La Dichiarazione dei Diritti del Fanciullo, firmata a Ginevra il 24 settembre 1924 e adottata dalla Quinta Assemblea Generale della Società delle Nazioni, è il primo documento internazionale in cui si riconosce il bambino come soggetto giuridico titolare di diritti e bisognoso di particolari forme di tutela. Dopo lo scioglimento della Società delle Nazioni e la nascita dell'Organizzazione delle Nazioni Unite e del Fondo Internazionale delle Nazioni Unite per l'Infanzia (UNICEF), si fa strada il progetto di una Carta sui diritti dei bambini che integri la Dichiarazione universale dei diritti dell'uomo, con lo scopo di sottolinearne i bisogni specifici. La stesura e l'approvazione della Dichiarazione dei diritti del fanciullo da parte dell'Assemblea Generale delle Nazioni Unite avviene all'unanimità e senza astensioni il 20 novembre 1959. L'art. 34 prevede che "gli Stati parti s'impegnano a proteggere il fanciullo contro ogni forma di sfruttamento sessuale e violenza sessuale. A tal fine gli Stati parti devono prendere in particolare ogni misura adeguata su piano nazionale, bilaterale e multilaterale, per prevenire: a) l'induzione o la coercizione di un fanciullo per coinvolgerlo in attività sessuali

Lanzarote[124], hanno tracciato il quadro di riferimento entro il quale il legislatore ha predisposto le specifiche misure volte a contrastare l'abuso sessuale e le sue differenti manifestazioni.

All'interno dell'ordinamento giuridico italiano, la pornografia minorile ha trovato posto per la prima volta con 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 ha introdotto all'interno Codice Penale gli articoli che prevedono le fattispecie di reato relative alla produzione, commercio, pubblicità, diffusione e offerta di materiale pedopornografico, nonché alla detenzione del materiale in questione, anche qualora le fotografie e i video rappresentino la cosiddetta pedopornografia virtuale[125].

In generale, la normativa in materia si pone l'obiettivo di punire maggiormente chi produce e alimenta il mercato della pedopornografia rispetto a chi ne fruisce e, in secondo luogo, di salvaguardare la figura del minore punendo comunque chi produce, diffonde, fruisce di materiale con minori reali e chi crea rappresentazioni artefatte riconducibili a scene reali.

All'individuazione della naturale pedopornografica del materiale concorrono due requisiti: l'età del soggetto raffigurato, che deve essere inferiore ai diciotto anni, e la natura pornografica della rappresentazione, intesa non solo come atto sessuale ma anche come esposizione lasciva dei genitali. Tali requisiti sono esplicitamente specificati sia nelle norme in materia che in giurisprudenza di legittimità[126].

L'art. 9 della Convenzione di Budapest stabilisce che l'espressione "pornografia infantile" include il materiale che raffigura sia un minore coinvolto in un comportamento sessuale esplicito che un soggetto che sembra essere un minore coinvolto in un comportamento sessuale esplicito.

illecite; b) lo sfruttamento dei fanciulli nella prostituzione o in altre pratiche sessuali illecite; c) lo sfruttamento dei fanciulli in spettacoli e materiali pornografici".

[124] La Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e l'abuso sessuale, fatta a Lanzarote il 25 ottobre 2007, è stata ratificata in Italia con la Legge 1 ottobre 2012, n. 172.

[125] Art. 1, lett. b, sez. iii, Decisione Quadro dell'Unione Europea del 22 dicembre 2003, n. 2004/68/GAI, "immagini realistiche di un bambino inesistente".

[126] Florindi E. (2012) *Computer e diritto. L'informatica giuridica nella società dell'informazione e della conoscenza*. Giuffrè.

Secondo una definizione più recente[127] per "pornografia infantile" o materiale pedopornografico si intende:

- il materiale che ritrae visivamente un minore in atteggiamenti sessuali espliciti, reali o simulati;
- la rappresentazione degli organi sessuali di un minore per scopi prevalentemente sessuali;
- il materiale che ritrae visivamente una persona che sembra un minore in atteggiamenti sessuali espliciti, reali o simulati, oppure la rappresentazione per scopi prevalentemente sessuali degli organi sessuali di una persona che sembra un minore; oppure
- immagini realistiche di un minore in atteggiamenti sessuali espliciti o immagini realistiche degli organi sessuali di un minore, per scopi prevalentemente sessuali.

Pertanto, ai fini pratici il materiale pedopornografico è catalogabile in tre tipologie a seconda delle origini:

- produzione amatoriale: si tratta di bambini fotografati da pedofili durante attività di molestia, in famiglia, dopo adescamento in altri luoghi o semplicemente mediante foto/video realizzati in luoghi pubblici quali ad esempio spiagge o piscine;
- produzione professionale: si tratta di vere e proprie attività di organizzazioni criminali che operano prevalentemente in zone geografiche con alto tasso di povertà (Sud America, Asia, Est europeo) che collocano il materiale prodotto al fine di produrre un guadagno vendendolo direttamente on-line;
- pseudofotografie (manga): trattasi di immagini create tramite sistemi di computer graphics riproducenti bambini inesistenti (o artefatti) o personaggi infantili riconducibili a cartoni animati impegnati inequivocabilmente in atteggiamenti esplicitamente sessuali.[128]

Nel 2010 la Cassazione[129] si è pronunciata intendendo che per rappresentazione pedopornografica debba intendersi anche "il materiale che

[127] Direttiva 2011/92/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.

[128] D'Agostini D., D'Angelo S., Violino L. (2007) *Diritto penale dell'informatica: dai computer crimes alla digital forensic*. Experta.

[129] Cass. Pen., Sez. III, 4 marzo 2010, n. 10981. Nel caso di specie la Cassazione, richiamandosi all'art. 1 della Decisione Quadro del Consiglio Europeo 2004/68/GAI del 22

ritrae o rappresenta visivamente un minore degli anni diciotto implicato o coinvolto in una condotta sessualmente esplicita, quale può essere anche la semplice esibizione lasciva dei genitali o della regione pubica".

La giurisprudenza si è ormai occupata di svariate modalità tecniche di scaricamento, distribuzione, divulgazione e pubblicizzazione di materiale pornografico in rete. Il mero possesso di materiale, pur non accompagnato dall'attività di partecipazione al processo di produzione dei file stessi, avente oggetto fanciulli è qualificata dalla giurisprudenza come condotta illecita[130]. Quando l'attività di pubblicizzazione di materiale pedopornografico utilizza un sito web con materiale multimediale come foto o video oppure protocolli di rete – come i protocolli di file sharing su reti peer-to-peer – che consentono ad un numero non definito di utenti di consultare, scaricare o memorizzare file, sussiste il reato più grave definito dall'art. 600-ter c.p., comma 3[131]. Se l'invio è destinato ad un numero di persone ben determinato (ad esempio mediante invio di una e-mail) sussiste solo l'ipotesi più lieve dell'art. 600-quater c.p., comma 4[132]. Anche qualora non ci sia finalità di lucro, è punita la diffusione di materiale pedopornografico tra un pubblico indeterminato o circoscritto.[133]

2.2.1. Le prime iniziative dell'Unione Europea e del Consiglio d'Europa

Nel 1997, il Parlamento Europeo produceva una risoluzione[134] che invitava gli Stati membri a definire nei rispettivi ordinamenti giuridici norme comuni minime e forme di cooperazione amministrativa basate su orientamenti comuni; invitava, inoltre, la commissione a proporre, dopo essersi consultata con il Parlamento Europeo, un quadro comune di autoregolamentazione a livello della stessa Unione Europea. Tale quadro doveva comprendere il raggiungimento di obiettivi in termini di tutela dei minori e della dignità umana.

Successivamente con la decisione del 30 marzo 2000, relativa alla comunicazione della Commissione sull'attuazione delle misure di lotta contro il

dicembre 2003, ha escluso la configurabilità del reato nella condotta di un soggetto limitatosi a fotografare in spiaggia dei minori in costume da bagno.

[130] Cass. Pen., Sez. III, 7 giugno 2006, n. 20303.

[131] Cass. Pen., Sez. III, 16 maggio 2006, n. 23614.

[132] Cass. Pen., Sez. III, 11 dicembre 2002, n. 4900.

[133] Cass. Pen., Sez. III, 30 novembre 2006, n. 698.

[134] Risoluzione del Parlamento Europeo in merito alla Comunicazione della Commissione sul contenuto illegale o nocivo di Internet, del 24 luglio 1997.

turismo sessuale che coinvolge l'infanzia, il Parlamento europeo ribadisce che il turismo sessuale che coinvolge l'infanzia è un reato strettamente connesso ai reati di sfruttamento sessuale dei bambini e di pornografia infantile e chiede alla Commissione di presentare al Consiglio una proposta di decisione quadro che stabilisca le regole minime comuni relative agli elementi costitutivi dei suddetti atti criminosi.

La decisione del Consiglio dell'Unione Europea del 29 maggio 2000 aveva lo scopo principale di organizzare una vera e propria rete telematica per combattere la pedofilia su Internet nel modo più rapido ed efficace. Nel documento si chiedeva agli Stati membri di adottare, nell'ambito della precedente decisione 276/1999/CEE del Parlamento e del Consiglio, misure per incoraggiare gli utenti di Internet a notificare, direttamente o indirettamente, alle Autorità preposte all'applicazione della legge, il sospetto di diffusione su Internet di materiale di pornografia infantile, qualora essi avessero rinvenuto nella rete tali materiali. Il Consiglio chiedeva inoltre agli Stati membri di impegnarsi per assicurare la più ampia cooperazione possibile allo scopo di agevolare l'efficace accertamento dei reati di pornografia infantile su Internet e la relativa repressione; suggerendo anche di esaminare le misure atte a sollecitare i fornitori di servizio Internet allo scopo di:

- fornire consulenza alle Autorità competenti in ordine al materiale di pornografia infantile della cui esistenza erano stati informati o di cui erano venuti a conoscenza;
- togliere dalla circolazione il materiale pedopornografico, di cui erano stati informati o di cui erano venuti a conoscenza diffuso attraverso il servizio;
- conservare, secondo la Risoluzione del Consiglio dell'Unione Europea del 17 gennaio 1995 sulle intercettazioni legali delle telecomunicazioni, i dati relativi al traffico qualora fosse tecnicamente fattibile, soprattutto ai fini delle azioni penali allorché si sospettasse l'abuso sessuale di fanciulli nonché la produzione, il trattamento e la distribuzione di materiale di pornografia minorile: questo per il tempo eventualmente specificato nelle rispettive legislazioni nazionali;
- predisporre propri sistemi di controllo per combattere la produzione, il possesso e la diffusione di pornografia infantile.

Con l'approvazione della decisione quadro del 22 dicembre 2003[135], l'Unione Europa si è posta l'obiettivo di superare le divergenze nelle impostazioni giuridiche degli Stati membri, di adottare un metodo globale e di sviluppare una cooperazione efficace a livello giudiziario nell'applicazione delle leggi in materia di sfruttamento sessuale dei bambini e pornografia infantile. In particolare ogni Stato deve 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. Tali sanzioni devono essere sufficientemente severe da far rientrare lo sfruttamento sessuale dei minori e la pornografia infantile nell'ambito d'applicazione degli strumenti già adottati per combattere la criminalità organizzata, come l'azione comune del 3 dicembre 1998, n. 1998/699/GAI, sul riciclaggio di denaro e sull'individuazione, il rintracciamento, il congelamento o sequestro e la confisca degli strumenti e dei proventi di reato e l'azione comune del 21 dicembre 1998, n. 1998/733/GAI, relativa alla punibilità della partecipazione a un'organizzazione criminale negli Stati membri dell'Unione europea.

La direttiva è stata poi sostituita dalla direttiva 2011/93/UE[136] che si pone l'obiettivo di ravvicinare ulteriormente le legislazioni penali degli Stati membri in materia di abuso e sfruttamento sessuale dei minori, pornografia minorile e adescamento di minori per scopi sessuali, stabilendo norme minime relative alla definizione dei suddetti reati e delle relative sanzioni, nonché quello di introdurre disposizioni intese a rafforzare la prevenzione di tali reati e la protezione delle vittime minorenni: all'articolo 2 vengono fornite le varie

[135] Decisione Quadro del Consiglio Ue 22 dicembre 2003 n. 2004/68/GAI – Lotta contro lo sfruttamento sessuale dei bambini e la pornografia infantile.

[136] Direttiva del Parlamento europeo e del Consiglio 13 dicembre 2011 n. 2011/93/UE – Lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro n. 2004/68/GAI. Tale numerazione è il risultato di una rettifica (in GU L 335 del 17 dicembre 2011), in quanto la numerazione originaria era 2011/92/UE. La base giuridica della direttiva è da individuarsi nell'art. 83, primo comma del TFUE: secondo tale disposizione, "il Parlamento europeo ed il Consiglio, deliberando mediante direttive e secondo la procedura legislativa ordinaria, possono stabilire norme comuni minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente gravi che presentano una dimensione transnazionale, derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni".

definizioni già più volte fornite nel tempo[137] mentre all'articolo 5 vengono definite le pene minime per i vari reati connessi alla pedopornografia[138]:

2.2.2. Convenzione di Budapest sul Cybercrime – art. 9

La Convenzione sul Cybercrime affronta il tema della pedopornografia all'art. 9[139], nel quale si stabilisce che ciascuno degli Stati aderenti debba

[137] Per "minore" si intende la persona di età inferiore ai diciotto anni; per "età del consenso sessuale" si intende l'età al di sotto della quale è vietato compiere atti sessuali con un minore ai sensi della normativa nazionale; per "pornografia minorile" o "materiale pedopornografico" si intende il materiale che ritrae visivamente un minore in atteggiamenti sessuali espliciti, reali o simulati; la rappresentazione degli organi sessuali di un minore per scopi prevalentemente sessuali; il materiale che ritrae visivamente una persona che sembra un minore in atteggiamenti sessuali espliciti, reali o simulati, oppure la rappresentazione per scopi prevalentemente sessuali degli organi sessuali di una persona che sembra un minore; oppure immagini realistiche di un minore in atteggiamenti sessuali espliciti o immagini realistiche degli organi sessuali di un minore, per scopi prevalentemente sessuali; per "prostituzione minorile" si intende l'utilizzo di un minore per atti sessuali, dietro promessa o dazione di somme di denaro o di altri vantaggi o utilità in cambio della partecipazione a tali atti, a prescindere che il pagamento, la promessa o i vantaggi siano rivolti al minore o a terzi; per "spettacolo pornografico" si intende l'esibizione dal vivo, diretta a un pubblico, anche a mezzo di tecnologie dell'informazione e della comunicazione di un minore in atteggiamenti sessuali espliciti, reali o simulati, oppure organi sessuali di un minore, per scopi prevalentemente sessuali; per "persona giuridica" si intende un'entità che abbia personalità giuridica in forza del diritto applicabile, a eccezione degli Stati o di altre istituzioni pubbliche nell'esercizio dei pubblici poteri e delle organizzazioni internazionali pubbliche.

[138] Per l'acquisto o il possesso di materiale pedopornografico, pena detentiva massima di almeno un anno; per l'accesso consapevole, a mezzo di tecnologie dell'informazione e della comunicazione, a materiale pedopornografico, pena detentiva massima di almeno un anno; per la distribuzione, la diffusione o la trasmissione di materiale pedopornografico, pena detentiva massima di almeno due anni; per l'offerta, la fornitura o la messa a disposizione di materiale pedopornografico, pena detentiva massima di almeno due anni; per la produzione di materiale pedopornografico, pena detentiva massima di almeno tre anni. In tema di adescamento mediante tecnologie informatiche, l'articolo 6 prevede la pena detentiva massima di almeno un anno per gli adulti che propongono un incontro finalizzato al compimento di rapporto sessuale o alla produzione di materiale pedopornografico.

[139] Articolo 9 - Reati relativi alla pornografia infantile

1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commesse intenzionalmente e senza alcun diritto:

adottare le misure necessarie per rendere delitti gravi, se compiute intenzionalmente e senza diritto, le seguenti condotte:

- offerta o messa a disposizione di materiale di pornografia minorile tramite un sistema informatico, o di informazioni utili al reperimento (ad esempio, hyperlink);
- diffusione o trasmissione del materiale di cui sopra tramite un sistema informatico;
- procurarsi o procurare ad altri del materiale di pornografia infantile mediante un sistema informatico;
- produzione del materiale di cui sopra avente per scopo la sua distribuzione in un sistema informatico;
- possesso di siffatto materiale in un sistema informatico o su un supporto di dati (floppy disk, CD rom).

Il concetto di "pornografia minorile" è ben enucleato nella Convenzione, stabilendo che deve intendersi per tale "il materiale pornografico che rappresenti in maniera visuale un minore impegnato in una esplicita attività sessuale, o che rappresenti una persona che appaia essere un minore impegnato

---

a) la produzione di pornografia infantile allo scopo della sua diffusione attraverso un sistema informatico;
b) l'offerta o la messa a disposizione di pornografia infantile attraverso un sistema informatico;
c) la distribuzione o la trasmissione di pornografia infantile attraverso un sistema informatico;
d) il procurare pornografia infantile attraverso un sistema informatico per se stessi o altri;
e) il possesso di pornografia infantile attraverso un sistema informatico o uno strumento di archiviazione di dati informatici.

2. Ai fini del Paragrafo 1 di cui sopra, l'espressione " pornografia infantile " include il materiale pornografico che raffigura:
   a) un minore coinvolto in un comportamento sessuale esplicito;
   b) un soggetto che sembra essere un minore coinvolto in un comportamento sessuale esplicito;
   c) immagini realistiche raffiguranti un minore coinvolto in un comportamento sessuale esplicito;
3. Ai fini del Paragrafo 2 di cui sopra, il termine "minore" include tutte le persone sotto i 18 anni di età. Una Parte può comunque richiedere un età minore, che non potrà essere inferiore ai 16 anni.
4. Ogni Parte può riservarsi il diritto di non applicare in tutto o in parte il paragrafo 1, sottoparagrafi d ed e, e 2, sottoparagrafi b e c.

nell'attività di cui sopra, o le immagini realiste rappresentanti un minore impegnato in una attività sessualmente esplicita".

Oltre al materiale prodotto con minori impegnati realmente in atteggiamenti sessuali viene dunque criminalizzato anche il possesso, la produzione e la distribuzione di immagini realistiche (escluse quindi le semplici animazioni) che rappresentino un minore impegnato in atteggiamenti sessuali espliciti; ciò in quanto tali tipi di immagine hanno visto in momenti passati una violenza su minori, oltre a poter essere utilizzate per sedurre dei minori o per incitarli a compiere o a partecipare alle attività di cui sopra.

Nel rapporto esplicativo che accompagna il progetto di Convenzione viene precisato con la massima cura ciò che deve intendersi per atteggiamento sessuale esplicito.

Infine la Convenzione stabilisce che il termine "minori" si riferisce a soggetti di età inferiore ai 18 anni; tuttavia, per venire incontro ai Paesi che prevedono età inferiori, si è stabilito che le relative legislazioni nazionali possono prevedere una soglia diversa, purché non inferiore a 16 anni.

2.2.3. Convenzione di Lanzarote

La Convenzione di Lanzarote del 2007 ha l'obiettivo di prevenire e combattere lo sfruttamento e l'abuso sessuale di minori, nonché tutelare i diritti dei minori vittime di sfruttamento e di abuso sessuale e promuovere la cooperazione nazionale e internazionale contro lo sfruttamento e l'abuso sessuale di minori. Il vero punto di forza della Convenzione di Lanzarote è rappresentato dal fatto che si tratta del primo strumento a livello internazionale che considera reati le diverse forme di abuso sessuale commesse in danno di bambini e adolescenti con l'utilizzo della forza o delle minacce.

Rispetto alla Convenzione di Budapest sul Cybercrime, si restringe il margine di discrezionalità degli Stati membri con riguardo all'incriminazione del possesso di materiale pornografico infantile. Agli Stati membri è infatti lasciata la facoltà di escludere dall'area della punibilità il possesso di pedopornografia unicamente nei casi in cui abbia ad oggetto rappresentazioni simulate o immagini realistiche di minori non esistenti o comunque immagini prodotte dagli stessi minori con il loro consenso e per un utilizzo privato[140]. La Convenzione di Lanzarote prevede invece l'incriminazione di due atti meramente preparatori: l'accesso consapevole a siti pedopornografici effettuato

[140]Art. 20, par. 3, della Convenzione di Lanzarote.

attraverso le tecnologie dell'informazione e della comunicazione (art. 20, par. 1, lett. f) ed il c.d. child-grooming[141] (art. 23), attività a condotta libera che consiste nell'adescare il minore fingendo, ad esempio, di interessarsi alle sue vicissitudini o di prendersi cura delle sue necessità.

Vengono fornite le seguenti definizioni:

- il termine "minore" indica una persona di età inferiore a 18 anni;
- l'espressione "sfruttamento e abuso sessuale di minori" comprende i comportamenti di cui agli articoli da 18 a 23 della Convenzione;
- il termine "vittima" designa ogni minore oggetto di sfruttamento o abuso sessuale;
- il termine "pedopornografia" indica qualsiasi materiale che ritrae visivamente un minore coinvolto in una condotta sessualmente esplicita, reale o simulata, o qualsiasi rappresentazione di organi sessuali di minori a scopi principalmente sessuali.

Per gli Stati firmatari originari la Convenzione è entrata in vigore il primo luglio del 2010, quale primo giorno del mese successivo allo scadere del periodo di tre mesi dalla data in cui cinque firmatari, tra cui almeno tre Stati membri del Consiglio d'Europa, avevano consentito ad essere vincolati dalla Convenzione. Per gli Stati che invece firmeranno la Convenzione successivamente alla sua entrata in vigore, essa entrerà in vigore il primo giorno del mese successivo allo scadere di un periodo di tre mesi dalla data di deposito dello strumento di ratifica, accettazione o approvazione.

In relazione al diritto penale sostanziale, l'art. 18 descrive il reato di abuso sessuale per il quale si intende la partecipazione ad attività sessuali con un minore che non ha raggiunto l'età legale per praticare attività sessuali, nonché la partecipazione ad attività sessuali con un minore facendo uso di coercizione, forza o minaccia, abusando di una posizione riconosciuta di fiducia, autorità o influenza sul minore, anche in ambito familiare, abusando di una situazione di particolare vulnerabilità del minore, in particolare in ragione di una disabilità fisica o mentale o di una situazione di dipendenza. Non viene stabilita l'età al di sotto della quale non è consentito al minore di partecipare ad attività sessuali e si rimanda tale definizione alle singole parti, né rientra nello scopo della norma di regolare le attività sessuali consensuali tra minorenni.

[141] Sul punto, cfr. Choo R. (2009) *Online child grooming: a literature review on the misuse of social networking sites for sexual offences*. Australian Institute of Criminology. Ost S. (2009) *Child pornography and sexual grooming*. Cambridge.

L'art. 19 introduce i reati relativi alla prostituzione minorile, prevedendo che ciascuno Stato contraente punisca le condotte intenzionali finalizzate a reclutare un minore per la prostituzione o favorire l'esercizio da parte del minore della prostituzione, costringere un minore alla prostituzione, trarne profitto o sfruttare un minore in altra maniera per tali fini, e far ricorso alla prostituzione minorile.

Con l'espressione "prostituzione minorile" si indica il fatto di utilizzare un minore per attività sessuali, offrendo o promettendo denaro o qualsiasi altra forma di remunerazione, compenso o vantaggio, indipendentemente dal fatto che la promessa o il vantaggio siano rivolti al minore o a terzi.

All'articolo 20 vengono affrontati i reati relativi alla pedopornografia prevedendo che ciascuna delle Parti adotti le misure legislative o di altra natura necessarie che prevedano come reato le seguenti condotte intenzionali[142]:

- la produzione di materiale pedopornografico;
- l'offerta o la messa a disposizione di materiale pedopornografico;
- la diffusione o la trasmissione di materiale pedopornografico;
- il procurare a sé stessi o ad altri materiale pedopornografico;
- il possesso di materiale pedopornografico;
- l'accesso, con cognizione di causa e mediante l'utilizzo delle tecnologie dell'informazione e della comunicazione, a materiale pedopornografico.

Ciascuno degli Stati contraenti può riservarsi il diritto di non applicare, totalmente o in parte, la produzione e il possesso di materiale pornografico costituito esclusivamente da rappresentazioni simulate o immagini realistiche di un minore inesistente e materiale pornografico in cui sono coinvolti minori che hanno raggiunto l'età stabilita conformemente all'articolo 18, paragrafo 2, quando tali immagini sono prodotte o detenute da questi ultimi con il loro consenso e unicamente a loro uso privato. Anche l'applicazione di quanto previsto dal paragrafo 1 lettera f) viene lasciato a discrezione di ciascuna Parte.

[142] Ciascuno degli Stati contraenti può riservarsi il diritto di non applicare, totalmente o in parte, quanto previsto alle lettere a) ed e), alla produzione e al possesso di: materiale pornografico costituito esclusivamente da rappresentazioni simulate o immagini realistiche di un minore inesistente; materiale pornografico in cui sono coinvolti minori che hanno raggiunto l'età stabilita conformemente all'articolo 18, paragrafo 2, quando tali immagini sono prodotte o detenute da questi ultimi con il loro consenso e unicamente a loro uso privato. Ciascuna delle Parti può riservarsi il diritto di non applicare, totalmente o in parte, il paragrafo 1, lettera f).

All'art. 21, ciascuno Stato deve inoltre adottare le misure legislative o di altra natura necessarie per prevedere come reato le condotte relative alla partecipazione di un minore a spettacoli pornografici:

- reclutare un minore per partecipare a spettacoli pornografici o favorire la partecipazione di un minore a tali spettacoli;
- costringere un minore a partecipare a spettacoli pornografici, trarne profitto o sfruttare un minore in altra maniera per tali fini;
- assistere, con cognizione di causa, a spettacoli pornografici che comportano la partecipazione di minori.

Ciascuno Stato può riservarsi il diritto di limitare l'applicazione del paragrafo 1, lettera c), ai casi in cui i minori sono stati reclutati o costretti conformemente al paragrafo 1, lettera a) o b).

In tema di responsabilità delle persone giuridiche, l'art. 26 prevede che gli Stati contraenti adottino le misure legislative o di altra natura necessarie per garantire che una persona giuridica possa essere ritenuta responsabile dei reati previsti conformemente alla Convenzione, se commessi a vantaggio di essa da una persona fisica che agisce individualmente o in quanto parte di un organo della persona giuridica esercitando una posizione dirigenziale al suo interno sulla base di:

- un potere di rappresentanza della persona giuridica;
- un potere di prendere decisioni per conto della persona giuridica;
- un potere di esercizio del controllo in seno alla persona giuridica.

È, ad esempio, il caso di chi gestisce un sito che produce utili da pubblicità in virtù del materiale pedopornografico mostrato. In tal caso, oltre ai casi già previsti dal paragrafo 1, "ciascuna delle Parti è tenuta ad adottare le misure legislative o di altra natura necessarie per garantire che una persona giuridica possa essere ritenuta responsabile, quando la mancanza di sorveglianza o di controllo da parte di una persona fisica ha reso possibile la commissione di un reato fissato conformemente alla Convenzione a vantaggio della suddetta persona giuridica, da parte di una persona fisica che ha agito sotto la sua autorità". Sulla base dei principi giuridici dello Stato, la responsabilità di una persona giuridica può essere di natura penale, civile o amministrativa. La determinazione di tale responsabilità lascia impregiudicati i casi di responsabilità penale delle persone fisiche che hanno commesso il reato.

All'art. 28 sono definite le circostanze aggravanti tra cui, le più rilevanti ai fini dell'informatica forense sono i casi in cui il reato è stato commesso da un

familiare, da una persona che convive con il minore, da una persona che ha abusato della propria autorità, da più persone che hanno agito congiuntamente e quando il reato è stato commesso nell'ambito di un'organizzazione criminale.

In tema di indagini, azione penale e diritto processuale, la Convenzione prevede all'art. 30 che ciascuno Stato adotti le misure legislative o di altra natura necessarie per far svolgere le indagini e i procedimenti penali nell'interesse superiore e nel rispetto dei diritti del minore, nonché per consentire alle unità e ai servizi investigativi l'identificazione delle vittime dei reati fissati conformemente all'articolo 20, in particolare grazie all'analisi del materiale pedopornografico, come fotografie e registrazioni audiovisive, trasmesso o reso disponibile mediante l'utilizzo delle tecnologie dell'informazione e della comunicazione. Inoltre, all'art. 34 la Convenzione prevede che nelle indagini in materia di lotta allo sfruttamento e all'abuso sessuale di minori gli Stati contraenti impieghino personale, unità e servizi specializzati o che si provveda alla formazione di personale a tal fine: nel caso dell'Italia il compito é stato demandato alla Polizia Postale.

La Convenzione si prefigge come obiettivo la cooperazione tra le Parti nella misura più ampia possibile al fine di prevenire e combattere lo sfruttamento e l'abuso sessuale di minori, proteggere le vittime e fornire loro assistenza, e svolgere indagini o procedimenti relativi ai reati previsti dalla Convenzione medesima. In tale ottica, quando uno Stato contraente riceve una richiesta di assistenza giudiziaria o di estradizione da uno Stato con cui non ha concluso il trattato in questione, lo Stato contraente può considerare la Convenzione come base legale della mutua assistenza giudiziaria in materia penale o dell'estradizione in relazione ai reati previsti dalla Convenzione medesima.

Recependo le proposte avanzate dalla delegazione italiana, la Convenzione ha previsto nello specifico:

- la previsione del grooming, ossia della manipolazione psicologica dei minori per scopi sessuali, come nuova fattispecie di reato;
- la creazione di Unità investigative specializzate per effettuare indagini sotto copertura sulla pedopornografia online;
- il rafforzamento della cooperazione internazionale per combattere la dimensione transnazionale dei reati in oggetto;
- la creazione di un Fondo per le vittime e il trattamento dei rei;
- l'introduzione del reato di corruzione di minore, consistente nell'obbligare un minore ad assistere ad abusi sessuali o ad attività sessuali che coinvolgano uno o più adulti;

- l'allontanamento del reo dal nucleo familiare;
- l'identificazione dei minori ritratti su materiale pedopornografico;
- la creazione di osservatori nazionali per monitorare il fenomeno;
- la raccolta di dati relative alle varie forme di abuso e sfruttamento;
- apposite previsioni relative alla protezione del minore vittima nell'iter giudiziario, fra cui si segnala, in particolare, la novella previsione agli artt. 351, 362 e 391-bis c.p.p. dell'obbligo per il PM, la PG e il difensore di avvalersi dell'assistenza di un esperto in psicologia o in psichiatria infantile quando debbano interagire con un minore al fine di assumere informazioni nel corso delle indagini preliminari per i reati di sfruttamento sessuale dei minori (artt. 600-bis, 600-ter, 600-quater, 600-quater.1 e 600-quinquies c.p.), tratta di persone (artt. 600, 601 e 602 c.p.), violenza sessuale (artt. 609-bis, 609-quater, 609-quinquies, 609-octies c.p.) e adescamento di minori (art. 609-undecies c.p.). La delicatezza della materia è tale per cui anche nel caso in cui le informazioni vengano assunte dalla PG, l'esperto in psicologia o psichiatria infantile dovrà comunque essere nominato dal PM titolare dell'indagine.

2.2.4. Norme sulla pedopornografia nell'ordinamento giuridico italiano

La pornografia minorile ha acquisito rilevanza penale autonoma all'interno dell'ordinamento italiano ad opera di due leggi, intervenute nel 1998 e nel 2006[143], che sono il risultato di accordi assunti dall'Italia nell'ambito di un più ampio progetto internazionale di tutela e protezione dell'infanzia contro ogni forma di sfruttamento ed abuso sessuale[144].

[143] 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" e Legge 6 febbraio 2006, n. 38 "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet".

[144] Queste leggi sono il risultato dell'impegno assunto dall'Italia in virtù della Convenzione sui Diritti dell'Infanzia, sottoscritta a New York il 20 novembre 1989, della successiva Dichiarazione Finale della Conferenza mondiale di Stoccolma, adotta il 31 agosto 1996, e della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine transnazionale, adottati il 15 novembre 2000 e il 31 maggio 2001. La legge del 2006 rappresenta, inoltre, l'atto di recepimento della Decisione Quadro 2004/68/GAI in materia di pedopornografia online.

A livello di opinione pubblica queste leggi sono conosciute come norme contro la pedofilia, la quale, invero, è da considerarsi solo indirettamente il fenomeno incriminato[145]: si osserva, infatti, come la normativa in materia, anche con le successive modificazioni apportate dalla legge n. 38 del 2006, sia orientata primariamente a punire coloro che traggono profitto dallo sfruttamento sessuale dei minori, vale a dire chi utilizza i minori come oggetti. Coerentemente a questo obiettivo, infatti, le fattispecie in esame sono state collocate fra i delitti contro la personalità individuale[146], immediatamente dopo i reati che sanzionano la riduzione in schiavitù e la prostituzione minorile. In altre parole, il contrasto a queste realtà criminali è prevalentemente orientato verso chi trae un guadagno dall'esistenza della pedofilia e quindi dal fatto che i soggetti attratti dai bambini, al fine di soddisfare la propria perversione, devono comunque passare attraverso la condotta illecita consistente nel contatto corporeo con minori oppure nella fruizione del materiale pornografico minorile. Un'ulteriore conferma di questi rilievi deriva dalla stessa formulazione normativa, che distingue le condotte di chi alimenta il "mercato" pedopornografico secondo differenti livelli di gravità, dalla produzione sino alla cessione di contenuti illeciti, mentre qualifica in una diversa fattispecie le ipotesi legate alla ricerca e alla detenzione di questo materiale.

Si osserva come il dettato normativo preveda due requisiti per l'individuazione della natura illecita del materiale: l'età del soggetto ritratto, che deve essere chiaramente un minore degli anni diciotto, e il contenuto della rappresentazione, che deve essere ovviamente pornografico. La normativa, tuttavia, non fornisce una dettagliata definizione del concetto di "pornografia", né indica gli elementi necessari per valutare come pornografica una determinata immagine, sollevando molti dubbi fra i commentatori: una parte della dottrina, adottando una tesi restrittiva, riconosce la natura illecita nelle sole rappresentazioni che ritraggono un atto sessuale sul minore[147]; un'altra invece, propendendo per una definizione più ampia, prevede la configurabilità del reato in presenza di manifestazioni o sollecitazioni dell'istinto sessuale espresse con la riproduzione anche dei soli organi genitali. Alla qualificazione del fenomeno

[145] Helfer M. (2007) *Sulla repressione della prostituzione e pornografia minorile. Una ricerca comparatistica*. Cedam.

[146] Sorgato A., Vittorini Giuliano S. (2009) *Reati su soggetti deboli. Percorsi giurisprudenziali.* Giuffrè.

[147] Cadoppi A. (2006) *Commentario delle norme contro la violenza sessuale e contro la pedofilia*. Cedam.

in esame ha provveduto la Corte di Cassazione che ha evidenziato come tale espressione indichi "il materiale che ritrae o rappresenta visivamente un minore degli anni diciotto implicato o coinvolto in una condotta sessualmente esplicita, quale può essere anche la semplice esibizione lasciva dei genitali o della regione pubica"[148]. Tale definizione accoglie pertanto la tesi più ampia avanzata dalla dottrina, richiamando altresì la formulazione elaborata dal legislatore europeo, secondo cui non è necessaria la presenza di un atto di natura sessuale sul minore, essendo rilevanti anche i nudi suggestivi, così come tutte le rappresentazioni destinate a eccitare la sessualità altrui attraverso la natura erotica delle pose e dei movimenti del minore.

Rispetto alla formulazione normativa è opportuno esaminare le diverse figure delittuose previste:

- la condotta di distribuzione identifica un'azione di assegnazione e ripartizione dei contenuti illeciti, che richiama anche una conoscenza se non un contatto fisico tra i soggetti, destinata ad un pubblico ampio, ma non necessariamente indeterminato di persone. Si può configurare anche attraverso una serialità di atti di cessione, in cui la presenza di un numero significativo di possibili destinatari, anche se determinati, vale a distinguerla dall'ipotesi più lieve di offerta o cessione, in cui lo scambio avviene con un singolo utente identificato;
- la divulgazione e la diffusione si configurano qualora la condotta renda disponibile il materiale pedopornografico ad uno spettro di persone non predefinite. In altre parole, si tratta di una circolazione dei contenuti illeciti ad un pubblico tendenzialmente generalizzato ed indefinito[149]; tali ipotesi sono tipicamente realizzate tramite file sharing e chat line in cui, nonostante lo scambio possa avvenire anche solo tra due soggetti, la natura dello strumento rende potenzialmente disponibili i contenuti a tutti gli utenti che frequentano questi spazi virtuali;

[148] Cass. Pen. Sez. III, 4 marzo 2010, n. 10981. Nel caso di specie la Cassazione, richiamandosi alla nozione di pedopornografia fornita dall'art. 1 della decisione quadro del Consiglio europeo del 22 dicembre 2003, n. 2004/68/GAI, ha escluso la configurabilità del reato nella condotta di un soggetto limitatosi a fotografare in spiaggia dei minori in costume da bagno.

[149] Mengoni E. (2008) *Delitti sessuali e pedofilia*. Giuffrè.

- qualora il materiale venisse inviato tramite una comunicazione privata come una email, l'azione ricadrebbe nell'ipotesi di cessione.

In questa prospettiva, tuttavia, la giurisprudenza sottolinea come anche nel caso delle chat sia necessario valutare se il programma consenta a chiunque si colleghi la condivisione di cartelle, archivi e documenti contenenti le foto pornografiche minorili, in modo da potervi accedere e prelevare direttamente le foto[150]. Diversamente, se lo spazio online non risulti accessibile ad un numero indeterminato di persone o presupponga un dialogo "privilegiato", si verserà nell'ipotesi di cessione.

A prescindere dalle differenti condotte, il tratto distintivo di questa fattispecie è la potenziale indeterminatezza dei destinatari dei contenuti illeciti[151], aspetto che giustifica il trattamento sanzionatorio più elevato rispetto alle ipotesi di cessione, in cui l'occasionalità e l'identificabilità del ricevente ne comportano la più lieve sanzione.

Con riferimento al profilo soggettivo, per le diverse condotte è richiesto il dolo generico, quale coscienza e volontà di diffondere o pubblicizzare le rappresentazioni pedopornografiche. In tale prospettiva, tuttavia, sono opportune alcune precisazioni relative alle modalità e alla natura degli strumenti informatici utilizzati a tale scopo.

Infatti, se notoriamente per i servizi di file sharing non vi erano dubbi in merito alla qualificazione della condotta illecita, tale aspetto è stato recentemente messo in discussione dai giudici di legittimità. La Cassazione ha sottolineato come per la sussistenza del dolo occorra "che sia provato che il soggetto abbia avuto, non solo la volontà di procurarsi materiale pedopornografico, ma anche la specifica volontà di distribuirlo, divulgarlo, diffonderlo o pubblicizzarlo, desumibile da elementi specifici e ulteriori rispetto al mero uso di un programma di file sharing"[152]. Questi software, per loro stessa natura, determinano infatti la condivisione immediata dei contenuti nel momento in cui questi sono "scaricati", a prescindere dalla consapevolezza e dall'effettiva volontarietà in capo all'utente. Per tali motivi, al fine di integrare

[150] Cass. Pen., Sez. V, 3 febbraio 2003, n. 4900.

[151] Cass. Pen., Sez. III, 14 luglio 2000, n. 2842. La Cassazione afferma che "ai fini della configurabilità del reato di cui all'art. 600-ter, comma 3, c.p. (…) se da un parte non basta la cessione di detto materiale a singoli utenti, dall'altra è sufficiente che (…) questo venga propagato ad un numero indeterminato di destinatari".

[152] Cass. Pen., Sez. III, sentenza 28 novembre 2011, n. 44065.

la norma in esame, la giurisprudenza sottolinea come sia necessaria una valutazione fondata su ulteriori elementi e non solo sul mero utilizzo di questi specifici sistemi, seguendo pertanto la medesima modalità interpretativa già prevista per gli altri servizi della Rete, come le chat line o i forum.

Per quanto concerne il delitto di pornografia minorile, l'ultimo aspetto da esaminare attiene all'aggravante dell'ingente quantitativo introdotta con la novella del 2006, che prevede un aumento di pena fino ai due terzi nei casi in cui la diffusione e la cessione del materiale pedopornografico abbiano ad oggetto un numero cospicuo di contenuti illeciti. Quest'aggravante è stata prevista anche per le ipotesi di mera detenzione di pornografia minorile, consentendo pertanto agli operatori di polizia di poter procedere all'arresto facoltativo del soggetto qualora trovato in possesso di raccolte illecite di ampie dimensioni, ipotesi generalmente esclusa per questa fattispecie[153]. A questo intento, sicuramente lodevole, conseguono tuttavia alcuni aspetti problematici: la norma in esame, infatti, non fornisce alcuna definizione dell'espressione "ingente quantità", né indica i requisiti in presenza dei quali tale ipotesi si configura, evidenziando pertanto una lesione al principio di determinatezza che varrebbe, secondo parte della dottrina, ad escludere la costituzionalità di questa aggravante[154]. Tale aspetto, ad esempio, emerge con maggior chiarezza laddove si consideri come, nell'ambito di una medesima operazione delle forze dell'ordine, due indagati residenti in realtà territoriali differenti possano, a fronte di collezioni illecite delle stesse dimensioni, essere diversamente interessanti dall'applicazione di misure cautelari in ragione di un differente orientamento, rispetto al concetto di ingente quantitativo, da parte delle autorità giudiziarie competenti per la convalida dell'arresto[155]. È ravvisabile, pertanto,

[153] Al secondo comma dell'art. 600 quater c.p. si precisa infatti che "la pena è aumentata in misura non eccedente i due terzi ove il materiale detenuto sia di ingente quantità", a fronte di una sanzione della reclusione sino a 3 anni. In tale prospettiva, allora, dal combinato disposto con l'art. 381 c.1 c.p.p. consegue la possibilità di procedere all'arresto facoltativo anche in presenza della sola condotta di detenzione di contenuti illeciti, per la quale non è generalmente prevista la possibilità di arresto facoltativo. In particolare si ricorda che l'art. 381 c.p.p. prevede che "Gli ufficiali e gli agenti di polizia giudiziaria procedono all'arresto di chiunque è colto in flagranza di un delitto non colposo, consumato o tentato (art. 56 c.p.) per il quale la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel minimo a cinque anni e nel massimo a venti anni".

[154] Pistorelli L. (2006) Colmate le lacune della pregressa disciplina. In *Guida al diritto*, 9.

[155] Si pensi poi ad alcune problematiche prettamente tecniche quali ad esempio quelle relative all'utilizzo di archivi compressi finalizzati a contenere più file pedopornografici. Come

una disparità di trattamento legata ad un'interpretazione discrezionale della norma in esame, contraria non solo ai principi che regolano la disciplina penale, ma anche ai diritti costituzionalmente garantiti della persona.

Sul punto, si sono recentemente espressi i giudici di legittimità, evidenziando come ai fini della ricorrenza di questa ipotesi *è definibile di ingente quantità quel materiale che offra la disponibilità di un numero molto grande, rilevante o consistente di immagini pedo-pornografiche sì da contribuire concretamente ad incrementare il perverso mercato*[156]. Conformemente alla giurisprudenza elaborata in materia di stupefacenti, infatti, tale aggravante si configura qualora la fruizione di questi contenuti si discosti in termini significativi *da una condizione di detenzione di un numero contenuto di immagini quale si riscontra nella pratica giudiziaria relativa ad episodi illeciti di tal genere*[157]. Nonostante queste precisazioni, tuttavia, rimane ancora l'ambiguità di questa espressione, rispetto alla quale la dottrina sottolinea come sia auspicabile un'equilibrata interpretazione giurisprudenziale" attraverso "una lettura che contemperi la tentazione, per un verso, di imporre numeri industriali e, per altro verso, di accontentarsi di qualche decina di foto pornografiche"[158].

Nell'ambito della normativa volta al contrasto della pedopornografia, la seconda fattispecie di rilievo attiene alla repressione delle condotte di chi consapevolmente si procura o detiene questo materiale, sanzionate all'art. 600-quater c.p. con la pena della reclusione fino a 3 anni. Si tratta della norma che disciplina il comportamento dei "clienti" dei contenuti illeciti, vale a dire di quei soggetti che, richiedendo il materiale in esame, "contribuiscono significativamente ad alimentare il mercato della pornografia minorile"[159]. Per quanto concerne il dettato normativo, la prima ipotesi attiene alla ricerca e all'appropriazione del materiale illecito, mentre la seconda riguarda la compiuta acquisizione di tale contenuto[160]. Sono comprese questa fattispecie, pertanto, tutte le situazioni idonee a far rientrare le rappresentazioni pedopornografiche

si dovrebbe misurare la quantità? Un file (archivio compresso) o *n* file (il contenuto dell'archivio)? E un video da un'ora vale meno di due fotogrammi del video stesso?

[156] Cass. Pen., Sez. III, 31 marzo 2011, n. 17211.

[157] Ibidem.

[158] Mengoni E. (2008) *Delitti sessuali e pedofilia*. *Op. cit.*

[159] Sorgato A., Vittorini Giuliano S. (2009) *Reati su soggetti deboli. Percorsi giurisprudenziali*. *Op. cit.*

[160] Mengoni E. (2008) *Delitti sessuali e pedofilia*. *Op. cit.*

nella disponibilità dell'attore a prescindere dalle modalità concrete di attuazione, sia informatiche che fondate sul ricorso a supporti non digitali.

Rispetto alla previsione normativa non sono emerse particolari problematiche interpretative, con una giurisprudenza costante nell'escludere la configurabilità del reato nelle ipotesi in cui tali condotte non siano consapevoli, vale a dire non siano accompagnate da un'effettiva coscienza della natura delle rappresentazioni detenute, nonché dalla volontà di registrare tali materiali sui supporti informatici[161]. In tale prospettiva, infatti, la fruizione di contenuti pedopornografici è ravvisata laddove il materiale illecito, attraverso qualsiasi mezzo, sia nella disponibilità dell'agente, escludendo tuttavia "la configurabilità del reato in caso di mera consultazione via Internet senza registrazione su disco dei file". Pertanto non è sufficiente entrare in contatto o visionare le rappresentazioni illecite, ma occorre "appropriarsene salvandole e veicolandole o sul disco fisso del pc o su altri supporti, con esso interfacciabili, che ne consentano la visione o comunque la riproduzione". Secondo questo orientamento è quindi esclusa la configurabilità del reato nei casi di mera navigazione dei siti pedopornografici, ipotesi rispetto alla quale emergono alcuni dubbi in merito alle moderne prassi di consultazione online e in diretta dei video pedopornografici. Le pratiche conosciute con il termine streaming, infatti, non comportano una condotta attiva di registrazione o di detenzione dei file illeciti, determinando l'irrilevanza penale, se non supportata da altri riscontri, della visione dei contenuti pedopornografici realizzata attraverso questa modalità di fruizione.

Infine, l'ultimo delitto previsto dalla normativa in materia riguarda l'ipotesi in cui le condotte sanzionate nei due reati esaminati abbiano ad oggetto la "pornografia virtuale" (art. 600 quater-1 c.p.), ossia realizzata "utilizzando immagini di minori degli anni 18, o parti di esse", per la quale tuttavia la pena della reclusione diminuisce di un terzo rispetto alle sanzioni relative ai contenuti ritraenti minori "reali"[162].

[161] Cass. Pen., Sez. III, 21 settembre 2005, in Diritto dell'Internet, 2006, I, 51, nota Aterno, sentenza citata in Sorgato A., Vittorini Giuliano S. (2009) *Reati su soggetti deboli. Percorsi giurisprudenziali. Op. cit.*

[162] Art. 600 quater bis, "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 è diminuita di un terzo. Per immagini virtuali s'intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Questa fattispecie è stata introdotta sulla scia della Decisione Quadro del 2004 del Consiglio dell'Unione Europea, che qualifica come illeciti anche i materiali relativi a "immagini realistiche di un bambino inesistente"[163]. Si tratta di una norma che ha sollevato numerose perplessità tra i commentatori, poiché non coinvolgendo un minore "reale" appare difficilmente lesiva del bene giuridico protetto dalla legge in materia e, pertanto, in violazione del principio di offensività[164]. Sul punto si sono formulate differenti soluzioni in dottrina, volte in particolare ad evidenziare come la norma possa essere giustificata in virtù della tutela dell'onorabilità sessuale del minore o della protezione contro una condotta ritenuta di per sé pericolosa.

Accanto a questi dubbi interpretativi ne emergono altri strettamente legati alla nozione di contenuto "virtuale", la cui definizione normativa sembra lungi dall'essere chiara. In questo caso infatti, diversamente da quanto potrebbe far pensare il titolo giuridico della norma di reato, le rappresentazioni in esame non devono essere puramente fittizie, ma il risultato di un'elaborazione grafica che, fondandosi sull'utilizzo delle parti del corpo di un bambino reale, "fa apparire come vere situazioni non reali". Si tratta, in altre parole, di un "virtuale fatto così bene da apparire realtà; con ovvia esclusione, quindi, dell'immagine palesemente virtuale, oppure realizzata in modo grossolano […] banali collage, ma anche disegni, cartoni animati e dipinti". In questa prospettiva, pertanto, si ravvisa una formulazione ben lontana dalla previsione introdotta dalla normativa europea, la quale intende invece sanzionare anche quelle condotte relative a contenuti interamente frutto di manipolazione grafica. Le perplessità emerse in relazione alla formulazione normativa e ai comportamenti sanzionati trovano conferma anche osservando la pratica delle aule di giustizia, ove la

[163] Decisione Quadro 2004/68/GAI del Consiglio dell'Unione Europea 22 dicembre 2003 relativa alla lotta contro lo sfruttamento sessuale di bambini e la pornografia infantile. All'art. 1 la Decisione precisa la natura del materiale illecito, tanto con riferimento alla nozione di "bambino", tanto con riferimento alla nozione di "pedopornografia":

a) "bambino": una persona d'età inferiore ai diciotto anni;
b) "pornografia infantile": materiale pornografico che ritrae o rappresenta visivamente:
   i) un bambino reale implicato o coinvolto in una condotta sessualmente esplicita, fra cui l'esibizione lasciva dei genitali o dell'area pubica; o
   ii) una persona reale che sembra essere un bambino implicata o coinvolta nella suddetta condotta di cui al punto i); o
   iii) immagini realistiche di un bambino inesistente implicato o coinvolto nella suddetta condotta".

[164] Mengoni E. (2008) *Delitti sessuali e pedofilia. Op. cit.*

fattispecie in esame ha trovato finora difficile attuazione e rispetto alla quale non si osserva ancora alcuna pronuncia da parte dei giudici di legittimità[165].

Per quanto riguarda l'Italia, le norme contro lo sfruttamento sessuale dei minori sono state introdotte sin dal 1998 con la Legge n. 269 che ha previsto nuove fattispecie di reato e modificato anche alcune norme del codice di procedura penale. In particolare, l'art. 3 della citata legge ha inserito nel codice penale l'art. 600-ter c.p., intitolato Pornografia minorile, secondo cui

"1) Chiunque sfrutta minori degli anni 18 al fine di realizzare esibizioni pornografiche o di produrre materiale pornografico è punito con la reclusione da 6 a 12 anni e con la multa da 25.822 a 25.8228 euro.

2) Alla stessa pena soggiace chi fa commercio del materiale pornografico di cui al primo comma.

3) Chiunque al di fuori dell'ipotesi di cui al primo e al secondo comma, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga o pubblicizza il materiale pornografico di cui al primo comma, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto, è punito con la reclusione da 1 a 5 anni e con la multa da 2.582 a 51.645 euro.

4) Chiunque, al di fuori delle ipotesi di cui ai commi primo, secondo e terzo consapevolmente cede ad altri, anche a titolo gratuito, materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori degli anni diciotto, è punito con la reclusione fino a 3 anni o con la multa da 1.549 a 5.164 euro".

L'art. 600-quater c.p., intitolato "Detenzione di materiale pornografico", recita:

"Chiunque, al di fuori delle ipotesi previste nell'art. 600-ter, consapevolmente si procura o dispone di materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori degli anni diciotto è punito con la reclusione fino a tre anni o con la multa non inferiore a 1.549 euro".

In tema procedurale la modifica più importante è stata quella dell'art. 266 c.p.p. in tema di intercettazioni novellato nel senso di ammettere comunque la

[165] Sul punto, infatti, non si sono ancora avute pronunce da parte dei giudici di legittimità e, anche per quanto concerne quelli di merito, le sentenze che hanno affrontato quest'aspetto della pedopornografia sono rare. Si veda, in tal senso, Trib. Milano, IX Sez. Pen., Sentenza 11 novembre 2010, disponibile al sito della rivista online Penale.it. Diritto, procedura e pratica penale, consultabile al seguente indirizzo web *http://www.penale.it/page.asp?mode=1&IDPag=932*.

possibilità di intercettazione nel caso dei delitti previsti dal terzo comma dell'art. 600-ter c.p.[166].

In argomento va citata l'attività svolta in sede legislativa anzitutto dal Ministro per le Pari Opportunità che il 13 gennaio 2004, ha presentato, di concerto con i Ministri della Giustizia, dell'Interno, del Lavoro, delle Comunicazioni e delle Innovazioni, alla Camera il disegno di legge n. 4599 dal titolo "Disposizioni in materia di lotta contro lo sfruttamento sessuale di bambini e la pedopornografia anche a mezzo Internet"[167] che prevedeva, sostanzialmente, per quanto riguardava specificamente la pedopornografia informatica e telematica, le analoghe incriminazioni nel frattempo elaborate dalla Commissione Interministeriale più innanzi citata e necessarie per adattare la normativa italiana vigente al testo dell'art. 9 della Convenzione di Budapest, disegno di legge che divenne, con modificazioni, la legge 6 febbraio 2006 n. 38. Questa legge ha modificato ed integrato la normativa precedente contenuta nelle leggi 15 febbraio 2006 n. 66 e 3 agosto 1998 n. 269, introducendo, tra l'altro, all'art. 4, l'art. 600-quater il cui titolo è "pornografia virtuale" che recita nel modo seguente:

"1. Dopo l'art. 600-quater del codice penale, come sostituito dall'art. 3 della presente legge, è inserito il seguente:

Art. 600-quater. 1. (Pornografia virtuale). Le disposizioni di cui agli articolo 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 è diminuita di un terzo.

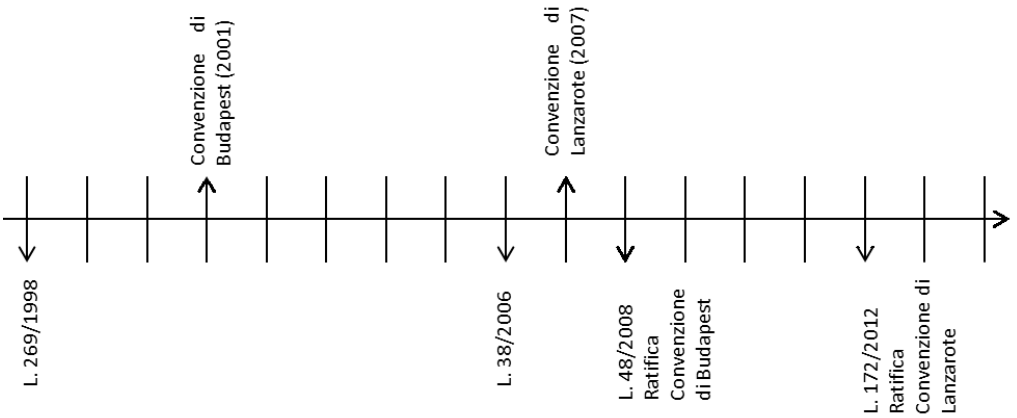
Per immagini realizzate con tecniche di elaborazione grafica non associate in arte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali".

[166] Con legge 11 marzo 2002, n. 46, il Parlamento ha disposto la ratifica e l'esecuzione dei protocolli opzionali allegati alla Convenzione dei diritti del fanciullo, il primo dei quali concerne la pornografia minorile.

[167] Nella relazione al disegno di legge sopraccitato, mentre si citava abbondantemente una Direttiva Quadro in materia che si affermava in via di approvazione da parte del Consiglio dell'Unione Europea, veniva totalmente ed inesplicabilmente, ignorata l'esistenza della Convenzione di Budapest che, come già detto prima, era stata sottoscritta dal Governo Italiano lo stesso giorno dell'apertura alla firma della Convenzione stessa (23 novembre 2001) e per la cui ratifica era stata poi costituita l'apposita Commissione Interministeriale. In realtà la Commissione aveva redatto alcuni articoli in tema di lotta alla pedopornografia già nel corso dei lavori dell'anno 2003, sempre allo scopo di adeguare la normativa vigente in materia alle prescrizioni della Convenzione.

La legge in questione ha introdotto nuove norme sostanziali e processuali, ed ha anche modificato l'art. 25-quinquies del decreto legislativo 8 giugno 2001 n. 231 in tema di responsabilità amministrativa delle persone giuridiche, inserendovi il richiamo al nuovo articolo 600-quater 1.

Il seguente diagramma riassume le varie norme che trattano di pedopornografia dal 1998 a oggi.



2.2.4.1. Legge 269/1998

Fino al 1996 il reato di abuso sessuale ai danni di un minore era previsto dall'art. 519 comma 2 del codice penale. Con la legge 66 del 15 febbraio 1996 "Norme contro la violenza sessuale" si è disposta l'abrogazione integrale della disciplina previgente e si è delineata una fattispecie ad hoc intitolata "Atti sessuali con minorenne". Tuttavia è solo dal 1998 che il fenomeno della pedopornografia ha assunto rilevanza penale. L'intervento normativo sul punto si è reso necessario in esito alla presa d'atto di aspetti gravemente degenerativi del fenomeno, tali peraltro da determinare la circolazione illecita di un'ingente quantità di danaro.

Il recupero e la cessione di materiale pedopornografico sono operazioni che ormai da diversi anni vengono quasi sempre poste in essere via Internet, sfruttando e qualità di un mezzo, di per sé neutro, che garantisce semplicità, rapidità e anonimato nello scambio del materiale anche di natura illecita. Con lo stesso strumento è possibile accedere anche ad una gran quantità di informazioni illecite in materia (luoghi dove recarsi per adescare adolescenti, soggetti da contattare, persone interessate ad acquistare e/o cedere immagini, ecc.) sfruttando siti ad accesso riservato. Orbene, proprio perché Internet è

divenuto nel corso di pochi anni un eccezionale strumento per la circolazione di materiale pedopornografico e di notizie a esso collegate, il legislatore ha dettato un'apposita disciplina contro la pedopornografia a mezzo Internet. La gravità del fenomeno deriva anche dall'elevato grado di pericolosità sociale dei soggetti che lo gestiscono: dietro la pedofilia e la pedopornografia operano spesso realtà criminali organizzate a livello internazionale.

La Legge 3 agosto 1998, n. 269[168], identifica illeciti in materia sessuale relativamente allo sfruttamento dei minori in tre diversi modi:

- induzione alla prostituzione,
- produzione, diffusione, detenzione di materiale pornografico,
- turismo sessuale all'estero.

2.2.4.2. Legge 38/2006

Successivamente, allo scopo di applicare i principi statuiti dall'Unione Europea con la decisione 2004/68/GAI del 22 dicembre 2003, il legislatore ha nuovamente regolato la materia emanando la Legge 6 febbraio 2006, n. 38[169], che apporta significative modifiche alle disposizioni alla Legge 269/1998, riservando una particolare considerazione alla commissione degli illeciti in questione tramite l'utilizzo di Internet e coinvolgendo nella lotta alla pedopornografia anche i provider.

Fra le novità introdotte dalla legge 38/2006 figurano:

- l'ampliamento della nozione di pornografia infantile e del suo ambito;
- l'estensione della protezione accordata al minore sino al compimento del diciottesimo anno di età;
- l'interdizione perpetua dall'attività nelle scuole e negli uffici o servizi in istituzioni o strutture prevalentemente frequentate da minori per le persone condannate per questo tipo di reati e l'esclusione del patteggiamento per i reati di sfruttamento sessuale;

[168] 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", emanata in adempimento a quanto sancito dalla Conferenza mondiale di Stoccolma, adottata il 31 agosto 1996.

[169] Legge 6 febbraio 2006, n. 38 "Norme contro la pedofilia e la pedopornografia anche a mezzo Internet".

- l'individuazione degli elementi costitutivi del reato di sfruttamento sessuale di minori, comuni a tutti gli Stati dell'Unione;
- la costituzione del Centro Nazionale per il Contrasto della Pedopornografia Online (CNCPO) avente il compito di raccogliere le segnalazioni, anche provenienti dall'estero, e monitorare la Rete.

La legge prevede una prima parte di disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia con aggiornamento del codice penale, del codice di procedura penale, del decreto legislativo 231/2001 e di alcune altre leggi tra cui la 269/1998.

La legge estende la protezione accordata al minore fino al compimento del diciottesimo anno di età ed amplia la nozione di pornografia infantile introducendo il concetto di pedopornografia virtuale: con tale locuzione si intendono quelle rappresentazioni realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali. Le ragioni a sostegno dell'incriminazione della pornografia virtuale, criticabili sotto il profilo giuridico e sociale, si fonderebbero, tra le altre, su esigenze probatorie legate alla difficile dimostrazione della natura reale o artificiale dell'immagine prodotta mediante le moderne tecnologie software di elaborazione grafica, con la conseguente difficoltà di risalire all'identità reale o meno del soggetto rappresentato. Inoltre, tali immagini potrebbero essere utilizzate dai pedofili per adescare i minori, senza dimenticare che comunque violano la dignità della categoria dei fanciulli.

La stessa legge inoltre inasprisce le sanzioni indicate dall'art. 600-bis c.p. ed istituisce il Centro Nazionale per il Contrasto della Pedopornografia Online presso l'organo del Ministero dell'interno con il compito di raccogliere tutte le segnalazioni, provenienti anche dagli organi di polizia stranieri e da soggetti pubblici e privati impegnati nella lotta alla pornografia minorile, riguardanti siti che diffondono materiale concernente lo sfruttamento sessuale dei minori avvalendosi della rete Internet e di altre reti di comunicazione, nonché i gestori e gli eventuali beneficiari dei relativi pagamenti. Ferme restando le iniziative e le determinazioni dell'autorità giudiziaria, in caso di riscontro positivo il sito segnalato, nonché i nominativi dei gestori e dei beneficiari dei relativi pagamenti, sono inseriti in un elenco costantemente aggiornato.

Per le operazioni di contrasto la norma prevede la collaborazione dei fornitori dei servizi resi attraverso reti di comunicazione elettronica, i quali sono obbligati a segnalare al Centro le imprese o i soggetti che diffondono,

distribuiscono o fanno commercio di materiale pedopornografico, con l'obbligo di conservare il materiale oggetto della segnalazione per almeno quarantacinque giorni. Inoltre, al fine di impedire l'accesso ai siti segnalati dal Centro, i fornitori di connettività alla rete Internet sono obbligati ad utilizzare gli strumenti di filtraggio e le relative soluzioni tecnologiche conformi ai requisiti individuati con decreto del Ministro delle comunicazioni, di concerto con il Ministro per l'innovazione e le tecnologie e sentite le associazioni maggiormente rappresentative dei fornitori di connettività della rete Internet.

Ulteriore collaborazione per il contrasto è richiesta agli intermediari finanziari che prestano servizi di pagamento, allo scopo di identificare i soggetti beneficiari di pagamenti effettuati per la commercializzazione di materiale concernente l'utilizzo sessuale dei minori sulla rete Internet e sulle altre reti di comunicazione.

Per adempiere a queste novità, la stessa legge prevede la stesura di due decreti ministeriali e di un regolamento:

- il decreto ministeriale 8 gennaio 2007[170] indica i requisiti tecnici che devono avere gli strumenti di filtraggio e le relative soluzioni tecnologiche di cui i fornitori di connettività devono dotarsi al fine di impedire l'accesso ai siti segnalati dal Centro nazionale per il monitoraggio della pornografia minorile su Internet;
- il secondo decreto definisce le procedure e le modalità da applicare per la trasmissione riservata mediante strumenti informatici e telematici delle informazioni relative al titolare delle carte di pagamento che ne abbiano fatto utilizzo per l'acquisto di materiale pedopornografico;
- infine, è emanato un regolamento[171] recante la composizione e le modalità di funzionamento dell'Osservatorio, nonché le modalità di attuazione e di organizzazione della banca dati.

[170] D.M. 8 gennaio 2007 "Requisiti tecnici degli strumenti di filtraggio che i fornitori di connettività alla rete Internet devono utilizzare, al fine di impedire, con le modalità previste dalle leggi vigenti, l'accesso ai siti segnalati dal Centro nazionale per il contrasto alla pedopornografia".

[171] D.M. 30 ottobre 2007, n. 240, "Regolamento recante Attuazione dell'articolo 17, comma 1-bis, della legge 3 agosto 1998, n. 269, in materia di coordinamento delle azioni di tutela dei minori dallo sfruttamento sessuale e dall'abuso e istituzione dell'Osservatorio per il contrasto della pedofilia e della pornografia minorile". Si riporta l'art. 1 su istituzione e compiti: "1. L'Osservatorio per il contrasto della pedofilia e della pornografia minorile, d'ora in poi denominato "Osservatorio", istituito presso la Presidenza del Consiglio dei Ministri

2.2.4.3. Legge 172/2012 di ratifica della Convenzione di Lanzarote

La legge 172 del 1 ottobre 2012 di 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, dà piena ed intera esecuzione alla Convezione in conformità all'articolo 45 della Convenzione stessa[172].

In relazione alle disposizioni previste dall'articolo 37, paragrafo 2, della Convenzione[173], l'Italia designa come autorità nazionale responsabile al fine della registrazione e conservazione dei dati nazionali sui condannati per reati sessuali il Ministero dell'Interno.

La legge di ratifica apporta inoltre modifiche al codice penale, al codice di procedura penale e ad altre norme. Per quanto attiene al codice penale, vengono apportate alcune modifiche tra cui, le più significative riguardano:

- l'introduzione degli articoli 414-bis[174], 600-septies.1[175], 600-septies.2[176], 602-quater[177], 609-undicies[178].
- la sostituzione in toto degli articoli 572[179], 600-bis[180], 600-septies[181] e 609-quinquies[182], 609-sexies[183];
- la modifica degli articoli 157[184], 416[185], 583-bis[186], 602-ter[187] con l'aggiunta di commi;

dall'articolo 17, comma 1-bis della legge 3 agosto 1998, n. 269, opera presso il Dipartimento per le pari opportunità.

2. L'Osservatorio ha il compito di acquisire e monitorare i dati e le informazioni relativi alle attività, svolte da tutte le pubbliche amministrazioni, per la prevenzione e la repressione dell'abuso e dello sfruttamento sessuale dei minori."

[172] Capitolo XIII - Clausole finali - Articolo 45 - Firma ed entrata in vigore.

[173] Capitolo VIII - Registrazione e conservazione di dati - Articolo 37 - Registrazione e conservazione dei dati nazionali sui condannati per i reati sessuali.

[174] Art. 414-bis - Istigazione a pratiche di pedofilia e di pedopornografia.

[175] Art. 600-septies.1 - Circostanza attenuante.

[176] Art. 600-septies.2 – Pene accessorie.

[177] Art. 602-quater – Ignoranza dell'età della persona offesa

[178] Art. 609-undecies – Adescamento di minorenni.

[179] Art. 572 – Maltrattamenti contro familiari e conviventi.

[180] Art. 600-bis – Prostituzione minorile.

[181] Art. 600-septies – Confisca.

[182] Art. 609-quinquies – Corruzione di minorenne.

[183] Art. 609-sexies – Ignoranza dell'età della persona offesa.

[184] Art. 157 – Prescrizione. Tempo necessario a prescrivere.

[185] Comma 7 dell'art. 416 - Associazione per delinquere.

- la modifica di un comma degli articoli 576[188], 600-ter[189], 604[190], 609-quater[191], 609-nonies[192], 609-decies[193];
- l'abrogazione degli articoli 600-sexies, 602-bis.

Le modifiche di maggior rilievo riguardano dunque l'introduzione dei reati di istigazione a pratiche di pedofilia e pedopornografia, di adescamento di minore.

Nell'ambito dell'esame parlamentare del disegno di legge di ratifica della Convenzione, che è stato approvato all'unanimità dalla Camera, sono stati recepiti i punti salienti della Convenzione di Lanzarote e più precisamente sono state introdotte nuove fattispecie di reato:

- il reato di pedofilia culturale o ideologica che era una fattispecie che mancava e che impediva talvolta alle forze dell'ordine di intervenire. La nuova fattispecie di reato è individuata nella condotta di chi, con qualsiasi mezzo, anche telematico, e con qualsiasi forma di espressione, pubblicamente istiga a commettere, in danno di minorenni, delitti a sfondo sessuale ed è punito con la reclusione da tre a cinque anni. La stessa pena si applica a chi pubblicamente fa l'apologia di uno o più dei delitti indicati;
- l'introduzione del grooming (adescamento in rete), poiché nella Convenzione di Lanzarote si prevede la finalità dell'adescamento solo al momento dell'incontro, che invece molto spesso non c'è, in quanto avverrebbe il cosiddetto peer-to-peer, ovvero uno scambio di dati e immagini attraverso gli utenti del web allorquando il minore viene costretto a compiere dei fatti illeciti. Viene individuato, infatti, il nuovo delitto di adescamento di minorenni, reato a condotta libera che consiste nel compimento di atti volti a carpire la fiducia del minore di età inferiore a sedici anni, attraverso artifici, lusinghe o minacce posti in essere anche mediante internet o altre reti o mezzi di comunicazione; il soggetto agente deve avere agito al fine di

[186] Art. 583-bis – Pratiche di mutilazione degli organi genitali femminili
[187] Art. 602-ter – Circostanze aggravanti.
[188] Art. 576 – Circostanze aggravanti. Ergastolo.
[189] Art. 600-ter – Pornografia minorile.
[190] Art. 604 – Fatto commesso all'estero.
[191] Art. 609-quater – Atti sessuali con minorenne
[192] Art. 609-nonies – Pene accessorie ed altri effetti penali.
[193] Art. 609-decies – Comunicazione dal tribunale per i minorenni.

commettere delitti di sfruttamento sessuale di minore o delitti di violenza sessuale: in questi casi si applica la pena della reclusione da uno a tre anni;

- è previsto altresì che i minori persone offese da delitti di sfruttamento sessuale e di tratta di persone possano essere ammessi al gratuito patrocinio, anche in deroga ai limiti di reddito.

Dal confronto tra i principi enunciati nella Convenzione di Lanzarote e l'approvazione degli emendamenti approvati alla Camera vengono individuate le fattispecie di reato, ma non viene presa in considerazione un'attività di prevenzione volta ad impedire il perpetrarsi del fenomeno stesso. Si rende infatti opportuno sottolineare come, in un'ottica di reale contrasto del fenomeno, appaia assolutamente necessario intervenire anche nello specifico ambito della prevenzione e della formazione, valorizzando gli interventi di sensibilizzazione sui principali fattori di rischio e sui comportamenti più appropriati per far fronte ad eventuali situazioni di pericolo. Può, dunque, affermarsi che il fenomeno della pedofilia non può combattersi solo con nuove leggi, senza prevedere anche azioni preventive e formative che coinvolgano una pluralità di soggetti pubblici e privati: accanto alle Forze dell'Ordine e all'Autorità giudiziaria, le famiglie, la scuola, le agenzie educative, i servizi del territorio, gli esperti di salute mentale.

2.2.4.4. La pornografia minorile nel codice penale: stato attuale

Dopo aver ripercorso il processo di produzione normativa in tema di pedopornografia, si riassumono gli articoli del codice penale allo stato attuale che trovano collocazione nel Libro secondo, Titolo XII, Capo III Dei delitti contro la libertà personale, Sezione 1 Dei delitti contro la persona.

L'art. 600-bis c.p. prevede che la reclusione da sei a dodici anni e una multa da euro 15.000 a euro 150.000 per chiunque recluti o induca alla prostituzione una persona di età inferiore agli anni diciotto, nonché favorisca, sfrutti, gestisca, organizzi o controlli la prostituzione di una persona di età inferiore agli anni diciotto, ovvero altrimenti ne tragga profitto. Salvo che il fatto costituisca più grave reato, chiunque compie atti sessuali con un minore di età compresa tra i quattordici e i diciotto anni, in cambio di un corrispettivo in denaro o altra utilità, anche solo promessi, è punito con la reclusione da uno a sei anni e con la multa da euro 1.500 a euro 6.000.

L'articolo 600-bis c.p. non è dunque particolarmente rilevante ai fini dell'informatica, anche se sul tema è intervenuta Cassazione[194] rilevando che l'elemento che caratterizza l'atto di prostituzione non è necessariamente costituito del contatto fisico tra i soggetti della prestazione, bensì dal fatto che un qualsiasi atto sessuale venga compiuto dietro pagamento di un corrispettivo; quindi è irrilevante il fatto che chi si prostituisce e il fruitore della prestazione si trovino in luoghi diversi, allorché gli stessi risultino collegati, tramite Internet, in videoconferenza, che consente all'utente di interagire con il minore, in modo da potergli chiedere il compimento di atti sessuali determinati.

L'art. 600-ter c.p. introduce la definizione di pornografia minorile e fornisce una prima lista di atti illeciti ad essa connessi. In coda viene offerta la definizione di pornografia minorile, intendendo "*ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali*".

Per quanto riguarda la definizione dei reati e delle pene, l'articolo prevede la reclusione da sei a dodici anni e con la multa da euro 24.000 a euro 240.000 per chiunque, utilizzando minori di anni diciotto, realizza esibizioni o spettacoli pornografici ovvero produce o fa commercio di materiale pornografico, nonché recluta o induce minori di anni diciotto a partecipare a esibizioni o spettacoli pornografici ovvero dai suddetti spettacoli trae altrimenti profitto. Con esplicito riferimento anche al mezzo informatico e telematico, è prevista la reclusione da uno a cinque anni e la multa da euro 2.582 a euro 51.645 per chiunque distribuisce, divulga, diffonde o pubblicizza il materiale pornografico di cui al primo comma, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto. Sono inoltre puniti con la reclusione fino a tre anni e con la multa da euro 1.549 a euro 5.164 coloro che offrono o cedono ad altri, anche a titolo gratuito, materiale pornografico. La pena è aumentata fino a due terzi ove il materiale sia di ingente quantità, senza tuttavia esplicitare quale sia la soglia che faccia scattare questo genere di valutazione. L'articolo prevede anche la reclusione fino a tre anni, con la multa da euro 1.500 a euro 6.000, per chiunque assiste a esibizioni o spettacoli pornografici in cui siano coinvolti minori di anni diciotto.

L'art. 600-quater c.p. si focalizza sulla detenzione del materiale pedopornografico così come definito dall'articolo precedente. Per cui,

[194] Cass. Pen., Sez. III, 8 giugno 2004, n. 25464.

chiunque, al di fuori delle ipotesi previste dall'articolo 600-ter, consapevolmente si procura o detiene materiale pornografico realizzato utilizzando minori degli anni diciotto, è punito con la reclusione fino a tre anni e con la multa non inferiore a euro 1.549. La pena è aumentata in misura non eccedente i due terzi ove il materiale detenuto sia di ingente quantità. In tema di consapevolezza, è rilevante la sentenza del Tribunale di Brescia del 22 aprile 2004, n. 1619, che ha assolto l'imputato che aveva sul proprio computer un file compresso che si presentava con il nome di un videogioco mentre al suo interno conteneva 11 file pedopornografici[195].

[195] Tribunale di Brescia, sentenza 22 aprile 2004, n. 1619. Si contestava all'imputato di essersi consapevolmente procurato materiale a contenuto "pedopornografico"; in particolare, si contesta la detenzione sul proprio pc di undici immagini "contenute in un file compresso protetto da password". La norma di cui all'art. 600 quater c.p. punisce chi, consapevolmente, si procura "materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori degli anni diciotto". Occorre chiarire, con riferimento ai materiali informatici, e, segnatamente, a quelli connessi a navigazione nel web, che la norma, punendo chi "si procura o dispone" di materiale illecito, e non chi, semplicemente, lo visiona, consente lo svolgimento della pretesa punitiva non nei confronti di tutti coloro che, navigando in internet, "entrino in contatto", semplicemente, con immagini aventi quel contenuto, ma coloro che "se ne approprino", "salvandole" e veicolandole o sul disco fisso del pc o su altri supporti, con esso interfacciabili, che ne consentano la visione o comunque la riproduzione. Lo "scaricamento" dei materiali, ovviamente, deve essere consapevole e volontario, dovendosi escludere profili di responsabilità penale nei casi in cui il materiale rinvenuto sul pc costituisca la mera traccia di una trascorsa consultazione del web, creata dai sistemi di salvataggio automatico del personal computer. Fatte tali brevi premesse di carattere generale, snodo centrale della vicenda è la verifica del carattere "consapevole" e "volontario" della memorizzazione sui (due) hard disc del pc detenuto da Tizio delle immagini di carattere pornografico ivi rinvenute: dato, questo, che può darsi per assodato, sulla scorta di quanto rilevato dal C.T. del Pubblico Ministero, e in alcun modo contestato dalla difesa, all'interno dei predetti hard disk si rinveniva un file (denominato "(...)desktop\Pendrive\Downloads\XP.zip") che conteneva, come da contestazione, n. 11 immagini a contenuto illecito. L'utilizzo del p.c. da parte di Tizio è dato a sua volta assolutamente pacifico e giudizialmente incontestato. Il consulente tecnico della difesa, nella sua relazione, esaminato il pc in sequestro, affermava in sintesi che: 1) il file xr.zip poteva essere scaricato dal web scambiandolo per un aggiornamento al gioco GTA3 che, come dimostravano gli accertamenti svolti, veniva assiduamente utilizzato da Tizio; 2) il file in questione poteva essere aperto solo previo utilizzo di una password, probabilmente non conosciuta da Tizio posto che alcun software di decriptazione era stato reperito sul suo pc; 3) le immagini illecite ivi contenute non erano state salvate in nessun altro file o directory del computer. Simili rilievi, all'evidenza intesi a sostenere l'assoluta non volontarietà del salvataggio di immagini pedopornografiche sul computer di Tizio, sono in linea con quanto dallo stesso affermato in sede di dichiarazioni spontanee, laddove egli adduceva di essere assolutamente sicuro di avere scaricato quel file quale aggiornamento del gioco GTA e di non essere mai riuscito ad aprirlo (evidentemente, per mancanza della password), dimenticandolo

Anche in questo caso, non è stabilita la soglia per la quale scatti l'ingente quantità; a differenza dell'articolo 600-ter è invece presente una clausola di consapevolezza per la quale la persona è da ritenersi colpevole solo se detiene il materiale in maniera consapevole.

Infine, l'art. 600-quater.1 affronta il tema della pornografia virtuale: per immagini virtuali si intendono "*immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali*". Dunque, le disposizioni previste agli articoli 600-ter e 600-quater si applicano anche quando il materiale pornografico rappresenta immagini virtuali realizzate

nella memoria del pc. Il C.T. della difesa concludeva che: 1) il file xr.zip è un file che può effettivamente contenere anche l'aggiornamento di un gioco elettronico, protetto da password; 2) sul pc di Tizio era installato un programma di decriptazione delle password, pur non essendo chiaro, alla stregua di quanto affermato dai consulenti, se esso possa essere utilizzato anche per file non in formato Word o Excel (ma in formato zip, come quello in questione); 3) non c'era traccia delle immagini illecite contenute in quel file ne nella cartella "file recenti", né nella cartella "file temporanei" (quest'ultima è una cartella dove si "appoggiano" i file zip decompressi, e dove rimane traccia, per un periodo variabile, dell'apertura di quei file). Alla luce della loro complessiva valutazione non ritiene questo Giudice che si possa affermare in modo persuasivo e tranquillizzante che Tizio abbia consapevolmente "scaricato" da Internet le immagini illecite che sono state reperite dal C.T. del Pubblico Ministero. In primo luogo, l'ipotesi che egli possa avere scaricato il file nella convinzione che contenesse l'aggiornamento di un videogame appare seriamente sostenibile, in quanto convalidata anche dal consulente del Pubblico Ministero. Ancor di più essa prende corpo una volta che si consideri la totale assenza di prove circa la consultazione e la visione, da parte di Tizio delle immagini ivi contenute, come dimostra, nella misura che può essere processualmente somministrata alla stregua di quanto osservato, la ricognizione delle cartelle "file recenti" e "temporanei", nonché la circostanza che non risulta alcun trasferimento delle immagini in altre ripartizioni della memoria del pc. Non possono poi trascurarsi, sempre su questa linea, ulteriori elementi di valutazione. Le immagini captate nella disponibilità di Tizio sono solo undici, e sono allocate in un unico file, oggetto, per quanto risulta, di un solo, originario download; ciò rende ancora maggiormente plausibile l'ipotesi, coonestata dalla difesa, che esse possano derivare da un'erronea operazione di salvataggio dal web, non essendovi elementi ulteriori che suffraghino l'idea di un interesse dell'imputato per i materiali a contenuto pedopornografico. Ne basta a contrastare quest'ipotesi il dato della permanenza del file nella memoria del computer, dato che può essere agevolmente spiegato con una dimenticanza dell'imputato. In definitiva, secondo un sorvegliato e prudente criterio di valutazione, condotto alla stregua dei principi di cui all'art. 192, II comma c.p.p. e 530, II comma c.p.p., non ritiene il Decidente che gli elementi raccolti consentano di sostenere, in termini sufficientemente persuasivi, l'ipotesi che Tizio si sia procurato consapevolmente le immagini illecite rinvenute nel suo pc, apparendo l'alternativa lettura della vicenda prospettata dalla difesa plausibile e compatibile con gli elementi raccolti.

utilizzando immagini di minori degli anni diciotto o parti di esse, ma la pena è diminuita di un terzo.

Vengono poi definiti degli articoli con circostanze attenuanti (art. 600-septies.1 c.p.), pene accessorie (art. 600-septies.2 c.p.) e confisca (art. 600-septies c.p.).

2.2.5. La disciplina giuridica sul possesso di materiale pedopornografico negli altri Paesi

In linea con le indicazioni di fonte sovranazionale, la maggior parte degli Stati europei punisce oggi il possesso o la detenzione di materiale pornografico minorile[196]. Lo Strafgesetzbuch, il codice penale tedesco, sanziona il possesso e l'attività di procacciamento di materiale pedopornografico. Il possesso consiste nel mantenere un rapporto di effettiva signoria sul materiale posseduto, ovvero la possibilità da parte del possessore di accedere e disporre del menzionato materiale. Nel diritto penale tedesco, con la nozione di possesso non si intende solo la disponibilità immediata, ma anche il possesso mediato purché il possessore abbia la possibilità di disporre del materiale[197]. Anche la sola possibilità di controllare temporaneamente il materiale archiviato in un sistema informatico sarebbe sufficiente ad integrare, secondo parte della dottrina, la fattispecie di possesso di materiale pornografico.

Il legislatore francese, in linea con le raccomandazioni di fonte sovranazionale, ha sanzionato la mera detenzione di materiale pedopornografico. L'art. 227-23-5, introdotto nel Code Pénal con la legge 305/2002, punisce, con la pena della reclusione fino a 2 anni e l'ammenda, la detenzione di immagini o rappresentazioni pedopornografiche[198]. Nel diritto

[196] Salvadori I. (2010) Possesso di pornografia infantile, accesso a siti pedopornografici, child-grooming e tecniche di anticipazione della tutela penale. *In:* Ruggieri F., Picotti L., eds. *Nuove tendenze della giustizia penale di fronte alla criminalità informatica*. Giappichelli, 20–31. Salvadori I. (2010) Legal problems of possession and viewing child pornography in the Internet. *In:* Herczeg J., Hilgendorf E., Grivna T., eds. *Internet kriminalität und die neuen Herausforderungen der Informationsgesellschaft des 21*. Jahrunderts.

[197] Si pensi per esempio al soggetto che possieda le chiavi di una cassaforte nella quale sono conservate immagini pornografiche minorili. Lo stesso dicasi nel caso in cui un soggetto possieda una password che gli permetta di accedere ad un computer che contiene file di analogo contenuto.

[198] Art. 227-23-5 Code Pénal: "*Le fait de consulter habituellement un service de communication au public en ligne mettant à disposition une telle image ou représentation ou de*

penale francese vengono ricondotti al concetto di detenzione anche i casi in cui il materiale è custodito presso un terzo e il soggetto ne mantiene comunque la disponibilità: ad esempio, la condotta dell'utente che salva delle immagini o dei video pedopornografici su server remoto, mantenendo la possibilità di accedervi, è penalmente rilevante[199].

Alla luce delle varie Convenzioni internazionali, il possesso di materiale pornografico minorile viene ormai punito in molti Stati, anche extra-Europei: in Spagna (art. 189.2 CP), in Belgio (art. 383-bis, par. 2, Code Penal), in Austria (§ 207a, par. 3, StGB), in Romania (art. 51, L. 161/2003), in Messico (artt. 202, 202-bis CP), in Colombia (art. 218 CP), in Argentina (art. 128. 2 CP), in Canada (Section 163.1(4) Criminal Code) e negli Stati Uniti d'America, dove è previsto sia a livello di legge federale (§ 2252A US Code) che nel *tort law* dei singoli stati[200].

L'orientamento giurisprudenziale prevalente in molti Stati europei sostiene che la mera visualizzazione di materiale pedopornografico disponibile in Internet, senza la consapevolezza che a seguito della navigazione in rete una copia delle immagini visualizzate venga automaticamente salvata dal browser nella memoria temporanea del sistema informatico (c.d. copie cache), non integri gli estremi del delitto di possesso di materiale pedopornografico. Come si è correttamente sostenuto, il possesso si configura soltanto nei casi in cui l'utente sia in grado di accedere al materiale e ne sia consapevole: questa impostazione, seppur corretta, porta naturalmente ad una disparità di trattamento tra gli utenti, con conseguenze diverse per quelli privi di una minima alfabetizzazione informatica rispetto a quelli più esperti; lo stesso dicasi con riguardo alle condotte di quei soggetti che accedono ai siti pedopornografici utilizzando computer di terzi soggetti o da postazioni pubbliche (ad esempio Internet Point o biblioteche), dal momento che non potrebbero rispondere del reato di possesso di materiale pedopornografico non avendo disponibilità per un tempo apprezzabile e neanche la possibilità di accedere al materiale temporaneamente salvato sul sistema informatico altrui.

détenir une telle image ou représentation par quelque moyen que ce soit est puni de deux ans d'emprisonnement et 30000 euros d'amende".

[199] Tirelli L.A. (2008) *La répression pénale des consommateurs de pédopornographie á l'heure de l'Internet*. Schulthess.

[200] Salvadori I. (2010) *Possesso di pornografia infantile, accesso a siti pedopornografici, child-grooming e tecniche di anticipazione della tutela penale. Op. cit.*

Non rientrano in questa casistica coloro che accedono consapevolmente a siti pedopornografici: ad esempio l'art. 227-23-5 Code Pénal francese punisce dal 2007 "chiunque consulta abitualmente pagine web che mettono a disposizione materiale pedopornografico". Lo stesso Consiglio d'Europa ha recentemente affermato l'obbligo di sanzionare la condotta di mero accesso a materiale pornografico minorile: l'art. 20, par. 1, lett. f) della Convenzione di Lanzarote limita la rilevanza penale alle sole condotte di accesso intenzionale a siti pedopornografici. Come si sostiene nel rapporto esplicativo della Convenzione, il carattere intenzionale dell'accesso può dedursi, per esempio, dalla frequenza con cui il soggetto consulta in rete il materiale o dal ricorso a servizi a pagamento, onde escludere la rilevanza penale del mero accesso fortuito o inconsapevole. La ratio della norma è quella di punire gli internauti che si limitano a visionare il materiale illecito disponibile in rete, senza salvarne una copia sul proprio computer.

CAPITOLO 3

3. Aspetti tecnici del peer-to-peer e del file sharing

I protocolli, e le relative applicazioni, di file sharing in reti peer-to-peer consentono agli utenti di scambiare allo stesso livello di complessità – o forse sarebbe meglio dire semplicità – non solo contenuti leciti ma anche materiale protetto da copyright e pedopornografia[201]. Tra i primi protocolli di file sharing progettati per il trasferimento efficiente di file di grandi dimensioni, e certamente il più utilizzato a livello globale tanto da renderlo ancora oggi uno dei principali per volume di traffico generato[202], BitTorrent è il protocollo più popolare a livello globale. Tuttavia in ambito europeo, e in particolare tra i sistemi di utenti italiani, lo scambio di file avviene per buona parte utilizzando eDonkey, il protocollo sul quale è implementato il software eMule, il secondo software più scaricato di tutti i tempi dal sito di progetti opensource *sourceforge.net*[203].

Un report contenente uno studio del 2013 condotto da Sandvine[204], azienda statunitense produttrice di apparati di rete, evidenzia come oltre il 50% del traffico di rete generato in upstream dagli utenti collegati in rete da punti d'accesso fissi è frutto di attività di file sharing, percentuale che si riduce a circa il 15% se si considerano solo gli accessi da punti mobili.

I due grafici seguenti illustrano la distribuzione di banda tra categorie di traffico[205].

---

[201] Layton R., Watters P. (2010) *Investigation into the extent of infringing content on BitTorrent networks*. Internet Commerce Security Laboratory.

[202] *https://www.sandvine.com/downloads/general/global-internet-phenomena/2013/sandvine-global-internet-phenomena-report-1h-2013.pdf*

[203] *http://sourceforge.net/top*

[204] *http://www.sandvine.com*

[205] Categorie di traffico:

- Comunicazioni: applicazioni, servizi e protocolli che permettono di ricevere e trasmettere messaggi di posta elettronica, chat, voce e video, nonché lo scambio di informazioni di contatto tra gli utenti. Esempi: Skype, WhatsApp, iMessage, FaceTime.

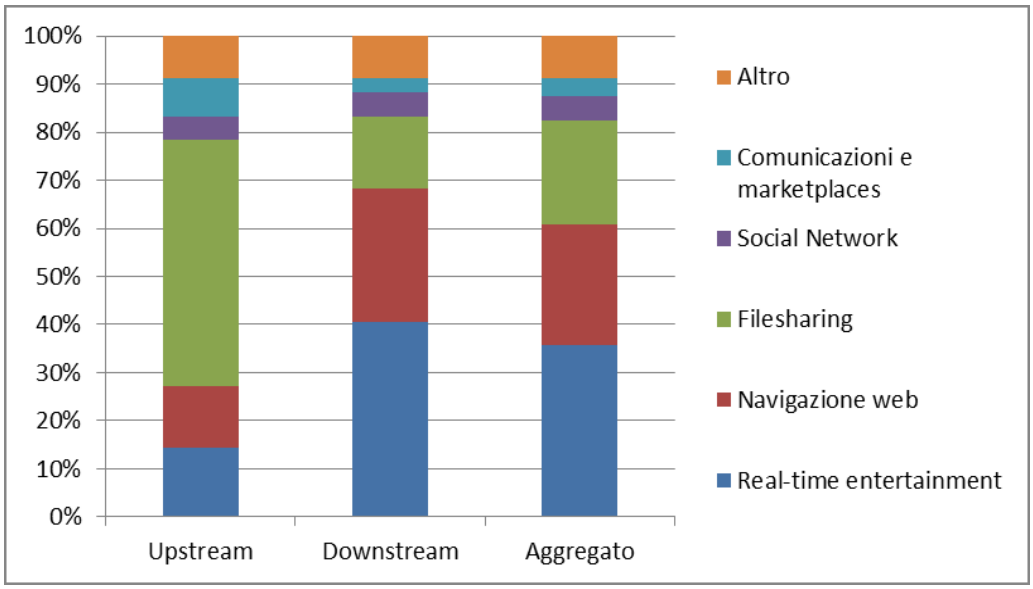


Figura 15 - Stima di distribuzione di traffico di rete generato da un punto di accesso fisso in Europa. Fonte Global Internet Phenomena Report, Sandvine, 2013.

- Filesharing: applicazioni per lo scambio di file che usano protocolli peer-to-peer o newsgroup. Esempi: BitTorrent, eDonkey, eMule, Gnutella, Ares.
- Marketplaces: sistemi dove gli utenti possono acquistare e scaricare software, libri, musica… Esempi: Google Android Marketplace, Apple iTunes, Windows Update.
- Real-Time entertainment: applicazioni e protocolli che consentono la fruizione di intrattenimento in streaming- Esempi: YouTube, Netflix, PPStream, Hulu, Pandora, MPEG, RTSP, RTMP, Flash Video.
- Social network: siti e servizi finalizzati all'interazione sociale e condivisione di informazioni (foto, status…) tra utenti. Esempi: Facebook, Twitter, Google+, LinkedIn.
- Tunneling: protocolli e servizi che consentono l'accesso remoto a risorse di rete, mascherando l'identità o fornendo incapsulamento. Esempio: VNC, SSL, SSH, Desktop remoto.
- Navigazione web: applicazioni e protocolli che consentono la fruizione di siti web. Esempio: HTTP, WAP.

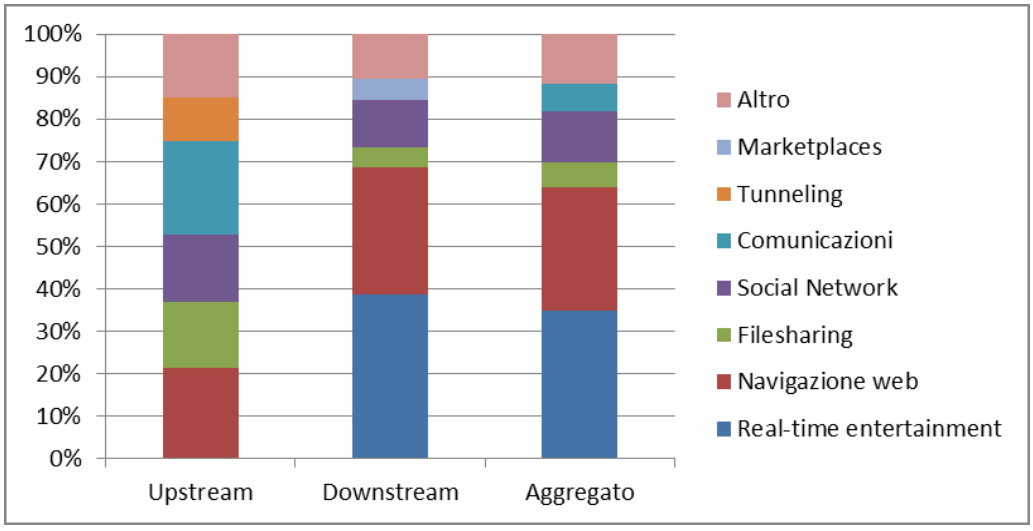


Figura 16 - Stima di distribuzione di traffico di rete generato da un punto di accesso mobile in Europa. Fonte Global Internet Phenomena Report, Sandvine, 2013

Mentre in quasi tutto il mondo BitTorrent è il protocollo di file sharing prevalente, in Europa circa il 6% del traffico in upload, e 2,5% se si considera il dato aggregato (upstream e downstream), è generato nell'ambito del protocollo eDonkey.

Le due tabelle successive illustrano la distribuzione di banda tra i programmi e protocolli specifici.

	Upstream		Downstream		Aggregato	
Rank	Applicazione	Percentuale	Applicazione	Percentuale	Applicazione	Percentuale
1	**BitTorrent**	**40,63%**	HTTP	26,15%	HTTP	23,34%
2	HTTP	10,70%	YouTube	24,25%	YouTube	21,27%
3	YouTube	7,79%	**BitTorrent**	**12,22%**	**BitTorrent**	**17,36%**
4	**eDonkey**	**6,45%**	RTMP	4,16%	Facebook	3,95%
5	Skype	5,86%	MPEG	4,03%	RTMP	3,67%
6	Facebook	3,79%	Facebook	3,94%	MPEG	3,48%
7	SSL	2,20%	Flash Video	2,98%	**eDonkey**	**2,59%**
8	RTMP	1,21%	**eDonkey**	**1,74%**	Flash Video	2,59%
9	MPEG	1,11%	Skype	1,65%	Skype	2,41%
10	Flash Video	0,94%	iTunes	1,54%	SSL	1,47%

Tabella 1 – Distribuzione del consumo di banda di rete tra le varie applicazioni (top 10) in Europa. Fonte Global Internet Phenomena Report, Sandvine, 2013

	Upstream		Downstream		Aggregato	
Rank	Applicazione	Percentuale	Applicazione	Percentuale	Applicazione	Percentuale
1	HTTP	17,77%	HTTP	27,61%	HTTP	26,38%
2	Skype	14,59%	YouTube	21,85%	YouTube	19,71%
3	Facebook	13,78%	Facebook	10,13%	Facebook	10,59%
4	**BitTorrent**	**12,34%**	Flash Video	5,22%	**BitTorrent**	**4,99%**
5	SSL	6,64%	MPEG	4,14%	Flash Video	4,66%
6	YouTube	4,65%	**BitTorrent**	**3,94%**	Skype	3,88%
7	Hotmail	1,25%	SSL	2,94%	MPEG	3,70%
8	Dropbox	1,21%	RTMP	2,90%	SSL	3,40%
9	**Ares**	**1,18%**	Skype	2,37%	RTMP	2,65%
10	SPDY	1,07%	Windows Update	1,81%	Windows Update	1,63%

Tabella 2 – Distribuzione del consumo di banda di rete tra le varie applicazioni (top 10) in Europa. Fonte Global Internet Phenomena Report, Sandvine, 2013

3.1. Definizioni

3.1.1. Peer-to-peer

Con il termine peer-to-peer (spesso abbreviato in p2p) si definisce un'infrastruttura di scambio informazioni tra nodi alla pari in cui due entità oggetto dello scambio possono indifferentemente scambiarsi i ruoli di fornitore e di cliente di un determinato servizio, solitamente non in maniera isolata ma costituendo un gruppo più ampio di sistemi al quale partecipano diversi nodi.

Il modello peer-to-peer è in antitesi con il paradigma client-server nel quale i ruoli dei due attori sono ben definiti (il server fornisce servizi e/o contenuti, il client li richiede)[206].

Una rete peer-to-peer può essere pura (detta anche decentralizzata pura), centralizzata o ibrida:

- in un'architettura decentralizzata pura tutti i nodi (peer) sono alla pari e non esiste alcun coordinatore centralizzato per cui ogni nodo può fungere da servente o da richiedente e l'uscita di un nodo non provoca alcun problema al funzionamento della rete, ad eccezione delle prime eventuali fasi di ricostruzione di connessioni tra nodi;

[206] Non si confonda la definizione di peer-to-peer con la rete peer-to-peer come viene intesa nell'ambiente del sistema operativo Windows, dove si fa riferimento ad una tipologia di rete in antitesi al dominio. Cfr. Microsoft, *Introduction to Windows Peer-to-Peer Networking* disponibile all'url *http://technet.microsoft.com/en-us/library/bb457079.aspx*.

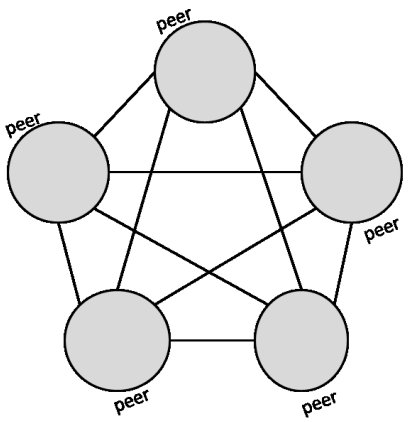


Figura 17 – Esemplificazione di un'architettura peer-to-peer decentralizzata pura

- in un'architettura centralizzata esiste un server (o cluster di server) che è in possesso di un indice e svolge ruolo di coordinamento tra i nodi;
- in un'architettura ibrida alcuni nodi assurgono a compiti superiori e vengono pertanto battezzati supernodi (superpeer oppure ultrapeer), a differenza degli altri nodi detti leaf-peer: in una prima fase, i nodi contattano i superpeer che provvedono a mettere in contatto i nodi tra loro, non interferendo successivamente nei processi di comunicazione.

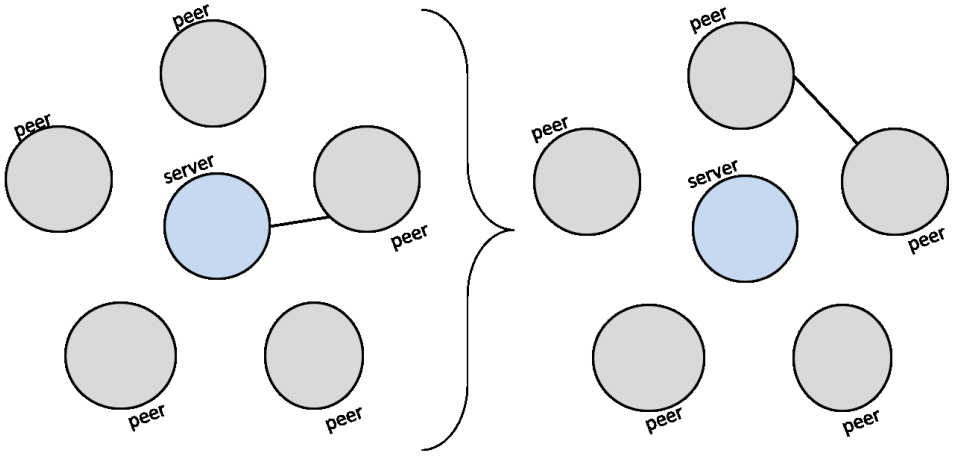


Figura 18 – Esemplificazione di un'architettura peer-to-peer centralizzata: il server ha un ruolo vitale per la rete, consentendo ai vari nodi di conoscersi (a sinistra) e poter poi comunicare direttamente senza alcuna ulteriore attività di intermediazione (a destra)

Nei sistemi centralizzati, il nodo (directory server) possiede un indice con le associazioni tra risorse e nodi, fornendo un servizio di individuazione di nodi e risorse. Napster utilizzava un sistema di questo genere che presenta i seguenti limiti: gestione costosa della directory centralizzata; collo di bottiglia costituito dal nodo centrale, con scalabilità limitata; singolo punto di vulnerabilità (point of failure), con conseguenza che il funzionamento dell'intero sistema è dipendente dal funzionamento del sistema centrale.

Nei sistemi puri invece, l'assenza di coordinamento centralizzato pone il problema della gestione dell'ingresso di un nodo alla rete in quanto per accedere alla rete peer-to-peer occorre conoscere l'indirizzo di almeno un nodo (problema del bootstrap): il problema si risolve prevedendo un bootstrap server, che può essere un web server che memorizza una lista di nodi attivi, oppure tramite peer cache, cioè una lista di nodi noti in precedenti sessioni, oppure tramite host noti, quindi solo i nodi che conoscono almeno uno degli altri partecipanti possono prendere parte alle rete.

Infine, nei sistemi ibridi non tutti i peer sono uguali: i nodi meglio connessi e con buona capacità computazionale possono avere funzioni speciali e vengono identificati dinamicamente tramite un algoritmo di elezione[207]. I superpeer indicizzano le risorse disponibili nei leaf-peer che gestiscono e, rispetto ai sistemi decentralizzati puri si riduce il tempo di discovery, rispetto ai sistemi centralizzati si elimina il singolo punto di vulnerabilità.

[207] Quando i sistemi distribuiti non hanno dei nodi predefiniti per le attività di coordinamento si rende necessario avere un sistema automatico di elezione del leader detto "Leader Election". Tale meccanismo consente, nel caso in cui il leader in carica subisca un guasto, di eleggere in corso un nuovo leader per ovviare al problema e consentire alla rete di funzionare. Il primo algoritmo di Leader Election è quello descritto da Gerard LeLann nel 1977 per reti ad anello, la cui complessità di gestione è certamente bassa. Nel caso delle reti peer-to-peer si è in presenza di una struttura a grafo fortemente connessa e quindi occorrono delle tecniche più sofisticate per l'elezione del leader. Un esempio di algoritmo, detto FloodMax, sfrutta un valore numero identificativo univoco associato ad ogni nodo mediante il quale viene eletto leader il nodo con il valore identificativo maggiore (oppure minore), mediante l'invio di messaggi tra i vari nodi proporzionale al diametro del grafo.

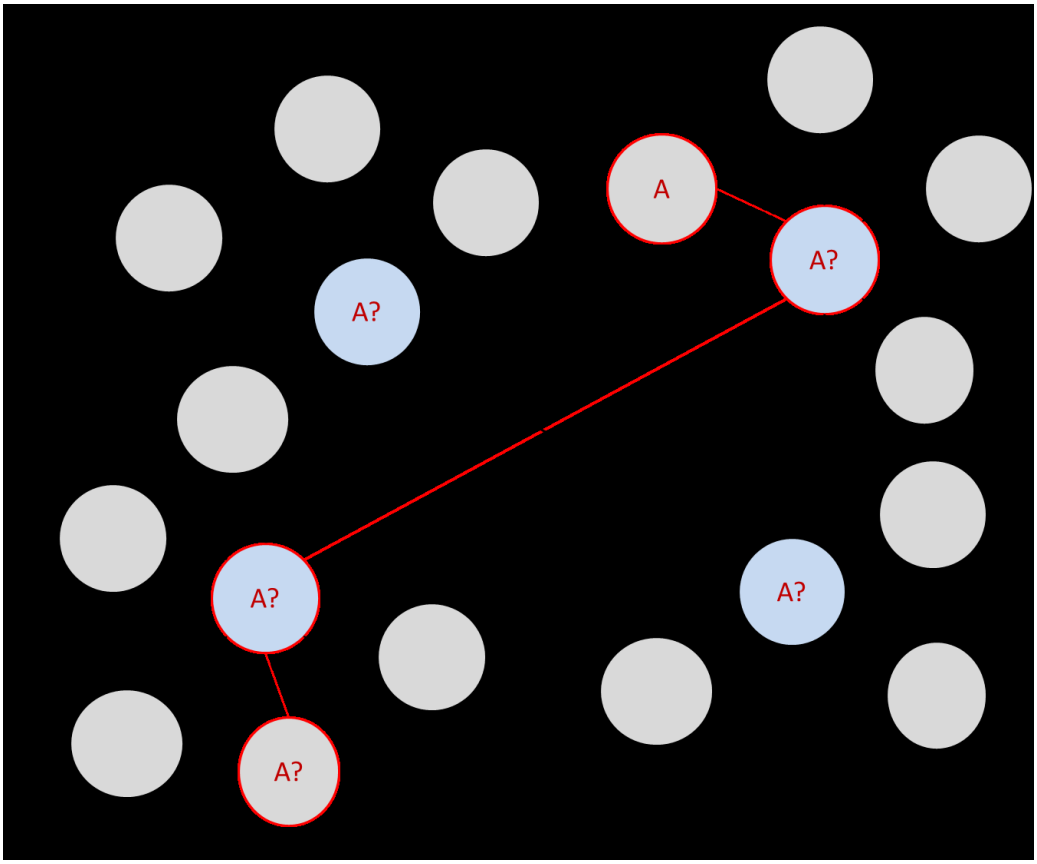


Figura 19 – Esemplificazione del processo di ricerca dei nodi (o delle risorse da essi forniti) nelle reti peer-to-peer ibride: il nodo in basso a sinistra cerca la risorsa (o il nodo) A, inoltra la richiesta al superpeer che fa lo stesso ai nodi a lui noti e agli altri superpeer, finché la richiesta non viene soddisfatta con l'individuazione della risorsa (o del nodo) richiesto

É doveroso chiarire che quando si tratta di protocolli e applicazioni peer-to-peer non necessariamente si fa riferimento al file sharing, né si può considerare sempre vera l'equazione che vede il peer-to-peer accostato a comportamenti o pratiche illegali. Tuttavia è vero, da qui anche la motivazione principale che ha dato origine al presente lavoro, che le reti peer-to-peer sono utilizzate principalmente per lo scambio di file, dei quali una percentuale massiccia è coperta da copyright o è costituita da materiale pedopornografico. Un'architettura peer-to-peer molto nota utilizzata su larga scala che non ha come obiettivo lo scambio di file è Skype[208], il noto software di VoIP di

[208] *http://www.skype.com*

Microsoft che si basa su una rete ibrida a due livelli con server di login e dei super-peer che si occupano dell'inoltro dei pacchetti.

3.1.2. File sharing

Le applicazioni più note che fanno uso della tecnologia peer-to-peer sono senza dubbio quelle dedite al file sharing: gli utenti hanno la possibilità di scambiare i file sulla rete Internet in maniera semplice ed efficiente anche con interlocutori sconosciuti, chiunque può svolgere il ruolo di fornitore del servizio (fornitura di file) e evitando così di utilizzare un unico server centralizzato che potrebbe facilmente essere oggetto di attività di indagine.

In realtà, lo scambio di file non è di per sé attività illecita se oggetto dello scambio non è materiale protetto da qualche diritto (materiale protetto da diritto d'autore, materiale protetto da segreto industriale, materiale a contenuto pedopornografico[209]…): esempi di file liberamente scaricabili sono i programmi distribuiti sotto licenze aperte (GPL, LGPL, Creative Commons…), tra le quali immagini di distribuzioni Linux, brani musicali liberamente scaricabili, opere dell'ingegno su cui non si possono più vantare diritti economici.

Di norma, l'approvvigionamento di file disponibili su reti peer-to-peer viene realizzato tramite appositi software che comunicano tra loro mediante specifici protocolli di rete di livello applicativo. Alcuni esempi sono i seguenti:

- eMule, basato sul protocollo KAD ed eDonkey;
- BitTorrent;
- Gnutella;
- KaZaA.

Sin dal 2004[210], quando ancora la banda larga non era diffusa con la capillarità che conosciamo oggi, si stimava il traffico generato da applicazioni di file sharing su reti peer-to-peer in circa il 60% del traffico di rete degli Stati Uniti e in circa 80% del traffico di rete dell'Asia, anche se negli ultimi anni questo dato è certamente ridotto in favore del classico HTTP utilizzato per l'accesso ai siti che forniscono la consultazione immediata dei contenuti audiovisivi in modalità streaming.

[209] United States General Accounting Office (2003) *File-sharing programs - peer-to-peer networks provide ready access to child pornography*. Online *http://www.gao.gov/new.items/d03351.pdf*.

[210] CacheLogic Research: The True Picture of P2P File Sharing, *http://www.readwriteweb.com/archives/p2p_growth_trend_watch.php*.

3.1.2.1. Tecniche di contrasto allo scambio di materiale illecito tramite protocolli di file sharing su reti peer-to-peer

Certamente i sistemi di file sharing su reti peer-to-peer vengono utilizzati principalmente per lo scambio di materiale che viola il diritto d'autore e di natura pedopornografica[211]. La difficoltà di arginare lo scambio di file è dovuta dall'impossibilità di imporre limiti allo scambio di file tra utenti di piattaforme di file sharing su reti peer-to-peer.

Per proteggere i file dalla massiccia attività di condivisione in rete, la letteratura scientifica propone di interferire con il processo di scaricamento di file. Una classificazione[212] di queste tecniche è la seguente:

- decoy[213]: l'idea è quella di pubblicare falsi file con nome, dimensione, tipo di file compatibile con quello del file da proteggere. Gli utenti che effettuano la ricerca per parola chiave vengono confusi nella scelta del file da scaricare. L'unico modo per poter comprendere se il file corrisponde ai propri interessi è quello di scaricare (spesso completamente) il file per verificare l'aderenza al materiale da ricercare. Alcune aziende[214] forniscono questo genere di servizio.
- Index poisoning[215]: l'idea è quella di comunicare agli utenti un falso indirizzo dal quale ottenere il file, generando notevoli perdite di tempo dovuto allo scambio degli indici tra i vari nodi della rete peer-

[211] Dazeley R., Layton R., Watters P. (2011) How much material on BitTorrent is infringing content? A case study. *Information Security Technical Report*, 16(2), 79–87.

[212] Wang C., Chiu C. (2011) Copyright protection in p2p networks by false pieces pollution. In *Lecture Notes in Computer Science*, 6906, 2011, 215–227.

[213] Kumar R., Liang J., Xi Y., Ross K. (2005) Pollution in P2P file sharing systems. In *IEEE INFOCOM 2005*. Christin N., Chuang J., Weigend A. (2005) Content Availability, Pollution and Poisoning in Peer-to-Peer File Sharing Networks. In *ACM E-Commerce Conference (EC'05)*, June 2005.

[214] Viralg, a digital copyrights protecting company (February 2009) *http://www.viralg.com/* e MediaDefender (February 2009) *http://www.mediadefender.com/*.

[215] Liang J., Naoumov N., Ross K. (2006) The Index Poisoning Attack in P2P File Sharing Systems. In *Proceedings INFOCOM 2006 25th IEEE International Conference on Computer Communications*, April 2006. Locher T., Moor P., Schmid S., Wattenhofer R. (2006) *Free Riding in BitTorrent is Cheap. In Fifth Workshop on Hot Topics in Networks*. ACM, 2006. Rao S., Sun X., Torres R. (2007) DDoS Attacks by Subverting Membership Management in P2P Systems. In *Third IEEE Workshop on Secure Network Protocols*, Beijing, China, October 2007.

to-peer che invece si scambiano le corrette informazioni sul materiale disponibile.

- Unauthenticated false blocks[216]: in questo caso, l'idea è quella di provare ad impedire lo scaricamento del file fornendo agli utenti blocchi di file che, accorpati ai vari blocchi costituenti l'intero file, rendono lo stesso inconsistente e quindi inutilizzabile. Tale meccanismo è possibile in alcuni sistemi (tra i quali BitTorrent) nei quali il file viene condiviso non come un'unica sequenza di bit ma come un insieme di blocchi, ognuno condiviso senza la verifica di integrità per mezzo di algoritmi di hash.

Napster è stato il primo servizio peer-to-peer di file sharing a riscuotere notorietà: rilasciato nel giugno 1999, permetteva agli utenti di mettere in condivisione file presenti nel proprio disco con gli altri partecipanti alla rete di scambio. In realtà Napster non era un sistema di peer-to-peer puro in quanto si basava su una serie di server centrali che mantenevano informazioni sugli utenti connessi e ai file condivisi da essi. Vi sono dunque due unità fondamentali:

- l'applicazione utente, che svolge ruolo di client per quanto la ricerca e la richiesta di file, e di server per quanto riguarda la condivisione e l'invio di file;
- metaserver, che hanno il ruolo di mantenere un indice dei file e degli utenti partecipanti.

Una volta connessi, i client utilizzavano i server per ottenere informazioni riguardo gli altri nodi in possesso del file desiderato, quindi lo scambio avveniva direttamente tra i nodi servente e ricevente.

3.2. I principali protocolli di file sharing su reti peer-to-peer

Nel settembre del 1999, Shawn Fanning pubblicò in rete un software gratuito per la condivisione di file musicali via Internet chiamato Napster. Da allora, il fenomeno sociale della condivisione di file sulla rete peer-to-peer non si è mai fermata. I motivi di questo successo sono molteplici: i software di file sharing su reti peer-to-peer sono sempre molto leggeri (pochi megabyte), non

[216] Kohler E., Liogkas N., Nelson R., Zhang L. (2006) Exploiting BitTorrent For Fun (But Not Profit). In *Proceedings 5th International Workshop on Peer-to-Peer Systems (IPTPS)*, Santa Barbara, USA, 2006. Dhungel P., Ross K. Schonhorst B., Wu D. (2008) A Measurement Study of Attacks on Bit-Torrent Leechers. In *Proceedings of Seventh International Workshop on Peer-to-Peer Systems (IPTPS)*, Tampa Bay, USA, 2008.

richiedono risorse computazionali elevate, si installano facilmente, non richiedono particolari competenze da parte degli utilizzatori. Per cercare un file è sufficiente indicare una parola chiave (ad esempio, il titolo e/o l'autore), ottenendo la lista dei file disponibili, quindi con un clic è possibile procedere allo scaricamento. In pratica, la rete diventa un immenso deposito di file di qualsiasi natura distribuito su milioni di computer.

Da allora, le reti peer-to-peer si sono evolute (come già illustrato nei paragrafi precedenti) e dunque anche i protocolli di file sharing ne hanno seguito le orme. Vengono di seguito proposti i principali protocolli di file sharing su reti peer-to-peer, alcuni dei quali ormai in disuso, ripercorrendo anche le vicissitudini giudiziarie che hanno portato allo sviluppo di versioni differenti.

3.2.1. Napster

Il meccanismo su cui si basava il funzionamento di Napster era estremamente semplice: la rete peer-to-peer alla base era di tipo centralizzato, dunque il server si limitava a tenere traccia degli utenti connessi e dei file che hanno a disposizione, senza disporre al suo interno di alcun file.

Quando un utente chiedeva di scaricare un file, il server lo metteva direttamente in contatto con il nodo che ne era effettivamente in possesso. Con questa nuova innovativa modalità di connessione si superava il problema del sovraffollamento dei server in quanto i tempi di connessione ad esso erano limitati alla sola ricerca dei file, mentre la parte più onerosa dell'operazione (da un punto di vista di occupazione di banda[217]) relativa all'effettivo invio da una parte e scaricamento dall'altra risultava completamente delocalizzata. Il successo di Napster ha indotto le case discografiche ad additarlo come il pericolo pubblico numero uno, mentre l'autore del software sosteneva la neutralità dello strumento, la cui unica funzione è permettere lo scambio di file la cui legittimità è di esclusiva responsabilità dell'utilizzatore finale. Questa tesi difensiva tuttavia non è stata accolta dalla giustizia americana che ha condannato alla chiusura Napster per le accuse di violazione del diritto d'autore.

[217] Si tenga presente che nel 1999 le connessioni ad Interne non avevano le prestazioni attuali e lo scaricamento di un file di pochi megabyte (ad esempio, un brano musicale) poteva richiedere diversi minuti.

Intanto alcuni hacker avevano iniziato un'attività di reverse engineering finalizzata all'analisi del protocollo alla base di Napster che culminò con la nascita del protocollo OpenNap. I primi server OpenNap apparvero nel 1999 in maniera analoga a Napster: il programma client si connetteva ad un server centralizzato OpenNap, quindi cercava, condivideva e scaricava file; il server OpenNap si occupava di tenere traccia di tutti i file disponibili, fornendo ai client la possibilità di cercare l'indice dei file disponibili e per poi avviare il trasferimento diretto tra i clienti dal momento che i file rimanevano unicamente sui client senza mai transitare dai server. Nel 2000 fu creato un servizio di indicizzazione per tutti i server OpenNap, chiamato Napigator. Mentre l'Associazione Americana dell'Industria Discografica cominciò a smantellare Napster, la popolazione di OpenNap cominciò inizialmente ad aumentare, perdendo comunque utenti nel corso degli anni a causa dell'utilizzo di server centralizzati.

Attualmente anche OpenNap, a causa della necessità di coordinamento centralizzato predefinito, è praticamente in disuso.

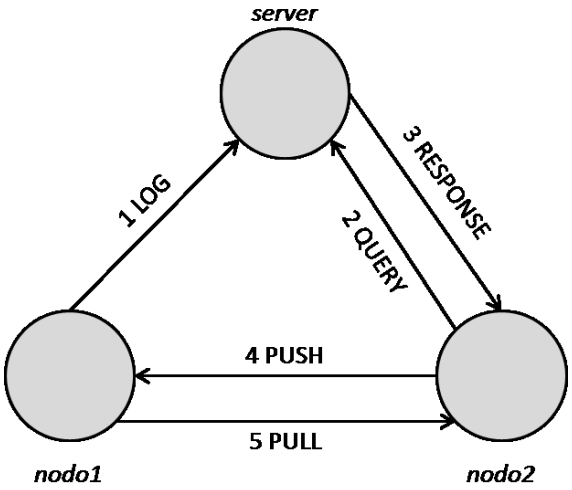


Figura 20 - Funzionamento delle reti peer-to-peer centralizzate nei casi di file sharing

L'immagine precedente mostra il funzionamento delle reti peer-to-peer centralizzate utilizzate da protocolli di file sharing come Napster e OpenNap. Posto che nodo2 intende scaricare un certo file, nodo1 è uno degli altri nodi che compone la rete e server è il sistema di coordinamento centralizzato, l'ordine delle operazioni è il seguente:

1. LOG: nella prima fase, nodo1 (ma anche nodo2) si connette alla rete p2p autenticandosi sul server centrale, al quale trasmette l'elenco dei file che intende condividere;
2. QUERY: nodo2 esegue la ricerca di una risorsa mediante l'utilizzo di opportune parole chiave, inoltrandola al server;
3. RESPONSE: il server risponde al nodo2 fornendo la lista dei nodi che dispongono della risorsa richiesta;
4. PUSH: nodo2 contatta direttamente uno dei nodi risultanti dalla ricerca, richiedendo la risorsa cercata;
5. PULL: nodo1 accetta la richiesta e invia al risorsa.

3.2.1. Gnutella

Gnutella è un protocollo peer-to-peer completamente distribuito per la condivisione di file rilasciato nel 2000 da Nullsoft: ogni nodo conosce alcuni vicini e le richieste vengono propagate ad altri nodi, sempre sfruttando la relazione di vicinanza. L'assenza di server centralizzati supera dunque il problema di un eventuale obbligo di chiusura del punto di coordinamento.

Scottate dall'esperienza Napster, le case discografiche non hanno aspettato la diffusione del programma per attaccarlo, ma poche ore prima che diventasse esecutiva la disposizione di non pubblicazione di Gnutella, alcuni tecnici della Nullsoft ne resero pubblici i sorgenti annullando in tal modo la sentenza di morte già pronunciata dalle case discografiche. Gnutella diventò quindi un progetto open source, inducendo programmatori di tutto il mondo allo sviluppo di client per questa tipologia di rete.

La partecipazione alla rete (bootstrap) è gestita da un apposito nodo che assolve ai compiti che nella rete centralizzata erano demandati al server. Il nodo esplora la rete provando a connettersi con alcuni degli altri nodi noti e, a seconda della velocità di connessione, il nodo prova a mantenere da 3 a 8 connessioni; se una connessione viene persa, il nodo cerca di connettersi ad un altro peer della lista che viene continuamente aggiornata. La fase di installazione procede secondo il seguente processo:

1. ALIVE: il nodo comunica la propria partecipazione agli utenti nella propria cache list, una lista di nodi noti;
2. FORWARD: i nodi contattati provvedono a loro volta alla comunicazione verso altri nodi noti della partecipazione alla rete del nuovo nodo; la comunicazione viene reiterata secondo lo stesso schema per un numero finito di volte, secondo il valore previsto dal

TTL (time to live), ovvero un numero massimo di passaggi dopo i quali i nodi smettono di propagare l'informazione;

3. QUERY: il nodo può eseguire ricerche e scambi con gli utenti conosciuti nelle fasi precedenti.

La ricerca di risorse avviene inoltrando la richiesta ai nodi vicini i quali, qualora non fossero in grado di soddisfare la richiesta, provvedono ad inoltrarla ai nodi a loro vicini fino ad un certo livello di profondità per evitare di far girare richieste all'infinito. Una volta che il peer che detiene la risorsa è stato individuato, il nodo richiede il trasferimento del file.

Tutti i nodi sono trattati allo stesso modo, indipendentemente dalla banda e dal numero di file condivisi, ed ognuno di essi si occupa di fornire e ricevere file, rispondere ed inoltrare richieste di routing provenienti dagli altri nodi[218].

Con questo metodo la rete è fortemente stabile, l'ingresso e l'uscita di nodi dalla rete non modifica le prestazioni della rete ma per ogni ricerca effettuata viene generato molto traffico di rete sui vari nodi.

Le applicazioni più popolari che fanno uso di questa rete sono Shareaza[219], LimeWire[220], FrostWire[221] e BearShare[222]. Dal progetto Gnutella sono nati diversi protocolli, tra cui il più famoso è FastTrack, la cui caratteristica principale è stata l'introduzione del resume dei download, ovvero della possibilità di riprendere uno scaricamento di un file lasciato a metà dal punto in cui era arrivato, e della possibilità di scaricare simultaneamente segmenti di file da peer multipli. I principali software che ne fanno uso sono KaZaA, Grokster, iMesh e FastTracker.

3.2.2. BitTorrent

BitTorrent è il protocollo di rete più popolare a livello mondiale per la distribuzione di contenuti con un traffico stimato intorno al 40% dell'intero traffico Internet in upload e del 12% in download[223].

[218] In una rete non completamente distribuita (ad esempio Napster) questo compito invece è riservato a dei server.

[219] *http://shareaza.sourceforge.net*

[220] *http://www.limewire.com*

[221] *http://www.frostwire.com*

[222] *http://www.bearshare.com*

[223] Dati da distribuzione del consumo di banda di rete tra le varie applicazioni (top 10) in Europa. Fonte Global Internet Phenomena Report, Sandvine, 2013.

Il protocollo si basa su un'architettura centralizzata che prevede l'utilizzo di un piccolo file che funge da indice con estensione .torrent, all'interno del quale sono contenute varie informazioni tra le quali la descrizione di tutti i pacchetti in cui il file originale è stato suddiviso e le chiavi hash che garantiscono l'integrità delle varie parti. La segmentazione del file consente di ridurre il carico di ogni sorgente, di ridurre la dipendenza dal gestore originale e di fornire ridondanza, consentendo peraltro la possibilità di procedere a download paralleli.

La condivisione di un file in BitTorrent funziona nel seguente modo:

1. sia X il file da condividere;
2. viene creato un file torrent che agisce come un indice dei frammenti che compongono il file X; il file torrent contiene i nomi attesi dei file condivisi, il numero di frammenti in file, l'hash di ogni frammento in modo che il cliente possa verificare che il file è stato ricostruito correttamente, una lista di tracker preferenziali e alternativi; il tracker è un sistema informatico che coordina le operazioni;
3. un tracker viene informato che il file di origine è pronto per la condivisione;
4. il nodo sorgente è impegnato nella distribuzione finché non ci sono abbastanza copie disponibili sui client che hanno scaricato il file di origine;
5. gli utenti che intendono scaricare il file X devono procedere prima all'individuazione del file torrent; la ricerca dei torrent può essere realizzata in diversi modi: dalla ricerca su siti appositi che fungono da motore di ricerca (ad esempio, The Pirate Bay[224] o Isohunt[225]), all'invio del torrent per posta elettronica;
6. una volta completato il download, il client riassembla il materiale e ne controlla l'integrità.

Il trasferimento è completamente gestito fra i peer con il tracker che è l'unico punto di coordinamento. Quando un peer si connette, il tracker invia una lista casuale di peer ai quali connettersi[226].

[224] *http://thepiratebay.se*.

[225] *http://isohunt.to*

[226] Erdely R., Kerle T., Levine B., Liberatore M., Shields C. (2010) Forensic investigation of peer-to-peer file sharing networks. In *Digital investigation*, 7, 95–103.

3.2.3. eDonkey

Il protocollo di file sharing su reti peer-to-peer sviluppato da Kulbak e Bickson[227] denominato eDonkey, noto anche come eDonkey2000 o eD2K, prevede dei server che mantengono in memoria le liste dei file condivisi dai client e assolvono alla funzione di indice del materiale condiviso. I client inviano ai server una sequenza di parole chiave e ottengono in risposta una lista di file nel cui nome c'è una corrispondenza con le keyword utilizzate; per maggior precisione, i server inviano ai client una lista di nodi remoti che nel momento della richiesta stanno condividendo quei file. La chiave univoca di indicizzazione dei file è la coppia formata dall'hash in formato MD4 e dalla dimensione del file. Utilizzando i dati presenti in queste liste, i client dispongono di tutte le informazioni necessarie a procedere allo scaricamento dei file da diversi client in parallelo[228].

Le comunicazioni che si verificano nel protocollo sono di tre tipi: server to server, client to server e client to client. Le prime non sono rilevanti ai fini di questo studio in quanto si tratta di attività di sincronizzazione per scambiare informazioni sugli indici e statistiche di utilizzo, le seconde riguardano l'attività di interrogazione, le terze rappresentano gli scambi di file veri e propri.

L'indicizzazione dei file avviene una lista di file che il ruolo di indice permette la condivisione di file di qualsiasi tipo in una rete peer-to-peer utilizzando dei server che fungono da centro di presentazione dei client[229] e permettono di localizzare i file all'interno della rete.

Nella rete eDonkey i file condivisi sono identificati mediante l'impronta hash MD4 calcolata sul contenuto dei file: in questo modo è possibile accomunare file identici con nomi diversi e distinguere file dissimili aventi lo stesso nome ma non il medesimo contenuto. Un identificativo a 128 bit è altresì utilizzato per identificare in modo univoco e permanente gli utenti della rete ma esso non ha alcuna relazione con l'algoritmo di hash. I server quindi detengono una tavola di hash contenente un elenco dei file e dei relativi utenti da cui sono scaricabili.

---

[227] Bickson D., Kulbak Y. (2005) *The emule protocol specification*. Online *http://leibniz.cs.huji.ac.il/tr/731.pdf*.

[228] Latapy M., Magnien C., Valadon G. (2009) Measurement of paedophile activities in eDonkey. *In:* Seifi M., ed. *Proceeding of International Conference Advances in the Analysis of Online Paedophile Activity*, 7–8.

[229] I client più diffusi che fanno uso della rete eD2K sono eMule (*http://www.emule-project.net/*) – e sue sottoversioni (dette "mod") – e Shareaza (*http://shareaza.sourceforge.net/*).

Un'altra caratteristica di eDonkey sta nel fatto che i file più grandi di 9,8 MB vengono divisi in parti, ognuna delle quali, appena scaricata, viene direttamente messa in condivisione al fine di accelerare il processo di distribuzione dei file molto grandi.

La ricerca dei file da scaricare può avvenire tramite il motore di ricerca interno al client oppure tramite liste di checksum di file presenti su siti web che possono essere messi in scaricamento tramite i link eD2K.[230]

Un punto debole della rete eDonkey è rappresentato dalla presenza dei server che devono rimanere attivi in maniera permanente al fine di fornire servizi ai client: questo genere di server è sottoposto ad un pesante carico di traffico e il loro blocco può compromettere il funzionamento della rete.

3.2.4. KAD

La rete Kademlia (o KAD) è una rete peer-to-peer priva di server utilizzata principalmente all'interno del progetto eMule al fine di sopperire ai problemi indotti dalla necessità di server centralizzati tipica della rete eDonkey[231].

Kad permette ai client di comunicare in modo diretto tra loro nella fase di ricerca delle fonti, senza la necessità di interpellare dei server custodi di indici – più o meno secondo lo schema di funzionamento di Gnutella – con lo svantaggio di dover attendere alcune ore prima che il protocollo sia operativo a pieno regime. Anche qualora un intero insieme di nodi fosse preso di mira da un attacco di tipo DoS[232], si avranno effetti molto limitati sulla rete che sarà in grado di superare automaticamente il problema isolando la rete intorno ai nodi problematici.

[230] I link eD2K permettono di identificare in modo univoco i file condivisi della rete peer-to-peer eDonkey, non indicano in modo esplicito un indirizzo dal quale poter prelevare il file ma contengono tutte le informazioni necessarie per poter eseguire una ricerca del file nella rete condivisa. Un link eD2K ha una struttura di questo tipo:
`ed2k://|file|nomefile.iso|129086478|9CD6AC211C43A83AE3F01E6AA2A120B0|/`
Il link eD2K potrebbe anche contenere un riferimento ad un client ben preciso: in questo caso l'indirizzo IP dell'utente di riferimento e posto alla fine:
`ed2k://|file|nomefile.iso|129086478|9CD6AC211C43A83AE3F01E6AA2A120B0|/|sources,209.189.53.26:4662|/`

[231] La prima versione di eMule che supportava la rete Kademlia è la 0.40.

[232] Il Denial of Service (DoS) è una tipologia di attacco informatico che impedisce agli utenti di utilizzare un servizio (ad esempio, raggiungere un sito web), esaurendo le risorse di un sistema informatico che lo fornisce fino a renderlo non più in grado di erogarlo.

A causa dell'assenza di server centralizzati, la fase di bootstrap di KAD può avvenire in due modalità: la prima mediante la funzionalità del software (ad esempio eMule) che all'atto dello scaricamento di un file provvede a individuare a contattare i nodi che dispongono del file; la seconda recuperando una lista di nodi noti dal sito http://www.nodes-dat.com.

Kademlia si basa sulla tecnologia del Distributed Hash Table (DHT): la rete definisce un concetto di distanza che permette di stabilire la prossimità tra due nodi cosicché, dato un nodo $nodo_1$ è sempre possibile determinare se un nodo $nodo_2$ risulta più vicino di un nodo $nodo_3$. Ogni nodo ha una conoscenza della rete Kademlia che diminuisce all'aumentare della distanza dal nodo stesso.

CAPITOLO 4

4. Investigazioni sulla pedofilia online e tecniche di contrasto

4.1. Statistiche e classificazioni di materiale e fruitori

Da fenomeno di nicchia relegato ai retrobottega di negozi compiacenti o ai ristretti circoli delle comunità pedofile, la pedopornografia si è oggi trasformata in una realtà che non conosce confini e dagli sviluppi senza precedenti[233]. La diffusione di Internet ha consentito un nuovo canale di espressione per la pedofilia, centrato principalmente sullo scambio di pedopornografia, sulla connessione tra pedofili e sui tentativi di adescamento dei bambini nelle chat, che sembra essere in fase di incremento e che si affianca alle forme tradizionali di abuso sui minori. La rete mette infatti in connessione pedofili di tutto il mondo consentendo a molti di essi di soddisfare la loro parafilia dalla propria postazione telematica, limitando (talvolta solo apparentemente) i rischi di essere scoperti ed arrestati[234].

L'influenza e il ruolo della dimensione virtuale sono testimoniati ormai da numerose ricerche[235], che concordano nel rilevare come il Web abbia aumentato la gamma, il volume e l'accessibilità delle immagini sessualmente oscene, ivi comprese quelle di pornografia infantile[236]. L'incontro fra perversioni pedofile e cyberspazio ha, in sostanza, inciso sul crimine in esame ampliandone l'eco a

[233] Per una genesi sull'evoluzione del fenomeno della pedopornografia, cfr. Tate T. (1990) *Child pornography: An Investigation*, Methuen; e Milner C., O'Donnel O. (2007) *Child pornography. Crime, computers and society*. Cullompton.

[234] De Marco F., Mattiucci M., Rossi A., Strano M. (2006) Le investigazioni sulla pedofilia on-line. *In:* Strano M., ed. *Abusi sui minori: manuale investigativo*. Nuovo Studio Tecna, 86–94.

[235] Jenkins P. (2003) *Beyond Tolerance: Child Pornography on the Internet*. NYU Press; Davidson J., Gottschalk P. (2011) *Internet child abuse. Current research and policy*. Routledge; Davidson J., Martellozzo E. (2008) Protecting children in cyberspace. *In:* Legherby G., Birch P., Cain M., Willimas K., eds. *Sex Crime*. Willan Publishers; Akdeniz Y. (2008) *Internet Child Pornography and the Law*. Ashgate.

[236] Krone T. (2005) International Police Operations Against Online Child Pornography. In *Australian Institute of Criminology, Trends and Issues in Crime and Criminal Justice*, 296.

livello globale e rendendone i contenuti accessibili ad un pubblico potenzialmente illimitato di persone, attraverso le più svariate modalità e i più differenti ambiti di diffusione.

Nello stereotipo culturale il pedofilo è uomo, tipicamente di mezza età. Nella realtà, anche le donne sono parte attiva del fenomeno con una percentuale attualmente stimata tra l'8 e il 12% del totale[237]. Di pedofilia femminile si comincia a discutere in America intorno agli anni '70 e soprattutto in relazione al fenomeno del turismo sessuale. La constatazione che la pedofilia è anche donna rompe alcuni tabù, credenze e certezze, presenti nell'immaginario collettivo: cade il dogma della maternità buona ad ogni costo, il principio per cui in ogni femmina c'è l'istinto a proteggere, o almeno a non colpire, un cucciolo della sua specie[238].

Nel report annuale del 2013[239], la Internet Watch Foundation (IWF)[240] riporta di aver individuato 13.182 siti web contenenti immagini di pornografia

[237] Sul punto, cfr. Petrone L., Troiano M. (2005) *E se l'orco fosse lei? Strumenti per l'analisi, la valutazione e la prevenzione dell'abuso al femminile*. Franco Angeli. Gli autori forniscono sei profili specifici: pedofilia latente, dove la donna nutre una morbosa attrazione nei confronti dei minori, ha fantasie ma non agisce per la consapevolezza del fatto che tali pulsioni non sono socialmente accettate; pedofilia occasionale, dove la donna tipicamente single o divorziata di mezza età si lascia andare in particolari situazioni tipo viaggi in paesi esteri con forte tasso di turismo sessuale; pedofilia immatura, dove la donna non è riuscita a sviluppare normali capacità di rapporto interpersonale con coetanei e quindi si rivolge ai minori da cui non si sente minacciata; pedofilia regressiva, dove la donna ad un certo punto della sua vita avverte un senso di inadeguatezza a convivere con gli stress quotidiani e regredisce nella fase infantile sentendosi essa stessa una bambina; pedofilia sadico-aggressiva, dove la donna manifesta un comportamento schivo e antisociale, trae piacere nel provocare dolore; pedofilia omosex, dove la donna trasferisce su una bambina l'amore che non ha ricevuta dalla mamma, identificandosi essa stessa nella sua vittima per colmare le carenze affettive subite.

[238] Bellissimo L., Crisafi M., Trunfio E. (2010) *Pedofilia. Disciplina, tutele e strategie di contrasto*. Giuffrè.

[239] *https://www.iwf.org.uk/assets/media/annual-reports/annual_report_2013.pdf.pdf*.

[240] La Internet Watch Foundation è un organismo indipendente finanziato dall'Unione europea e dall'industria ICT che dal 1996 fornisce un servizio di segnalazione dei contenuti illeciti online in maniera sicura e riservata, anche in forma anonima. La fondazione collabora con gli organismi istituzionale (forze dell'ordine, governo e altri partner internazionali) per combattere la diffusione online di contenuti relativi ad abusi sessuali su minori, procedendo in maniera attiva alle richieste di rimozione dei contenuti che in genere avvengono entro 60 minuti se è all'interno del Regno Unito o 10 giorni se fuori. In 16 anni di attività sono state valutate 400.000 pagine web, di cui 100.000 rimosse. Tra i finanziatori della IWF ci sono Internet Service Provider, operatori mobili, fornitori di contenuti e di hosting, società di filtraggio, provider di ricerca, associazioni di categoria e del settore finanziario. *https://www.iwf.org.uk/*.

minorile: 76% di sesso femminile, 10% di sesso maschile e 9% con minori di entrambi i sessi; il 3% dei minori è di età inferiore a 2 anni e 81% inferiore ai 10; il 51% delle immagine mostra violenze o torture nei confronti delle vittime. In relazione alla geografia dei fatti individuati, meno dell'1% dei file è stato individuato nel Regno Unito, a fronte del 54% nel Nord America, il 43% in Europa e Russia e il 3% in Asia. Tra i siti individuati, 392 sono risultati violati al fine di poterci caricare del materiale pedopornografico. All'interno del report è riportato anche lo schema che mostra come i video e le immagini pedopornografiche vengono individuate per poi procedere alla rimozione.

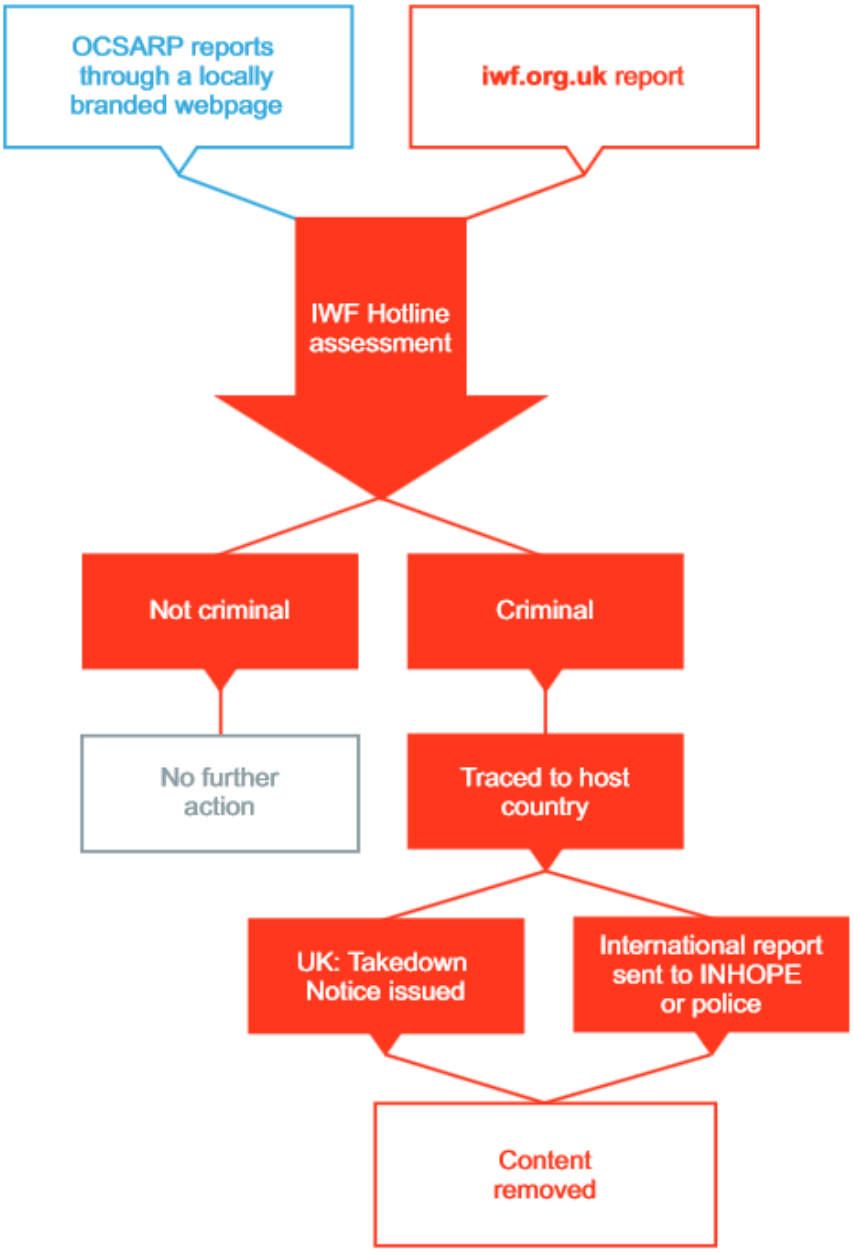


Figura 21 – Come i video e le immagini pedopornografiche vengono valutate e rimosse attraverso il portale sviluppato da IWF[241]

Con tale protocollo è stato possibile identificare oltre 10.000 domini in 8 anni.

[241] *https://www.iwf.org.uk/assets/media/annual-reports/annual_report_2013.pdf.pdf. Op. cit.*

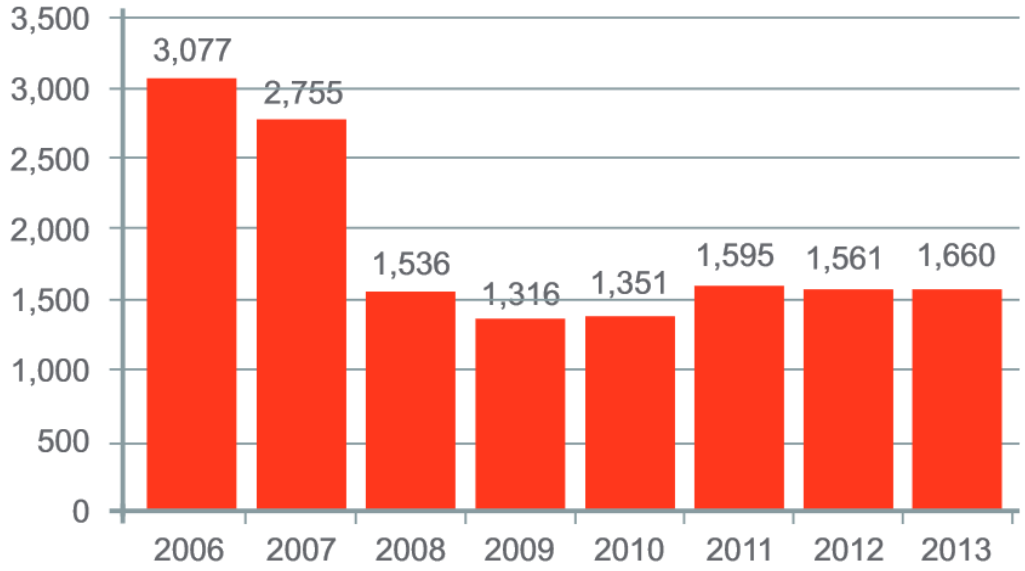


Figura 22 – Numero di domini contenenti materiale pedopornografico dal 2006 al 2013 individuati da IWF[242]

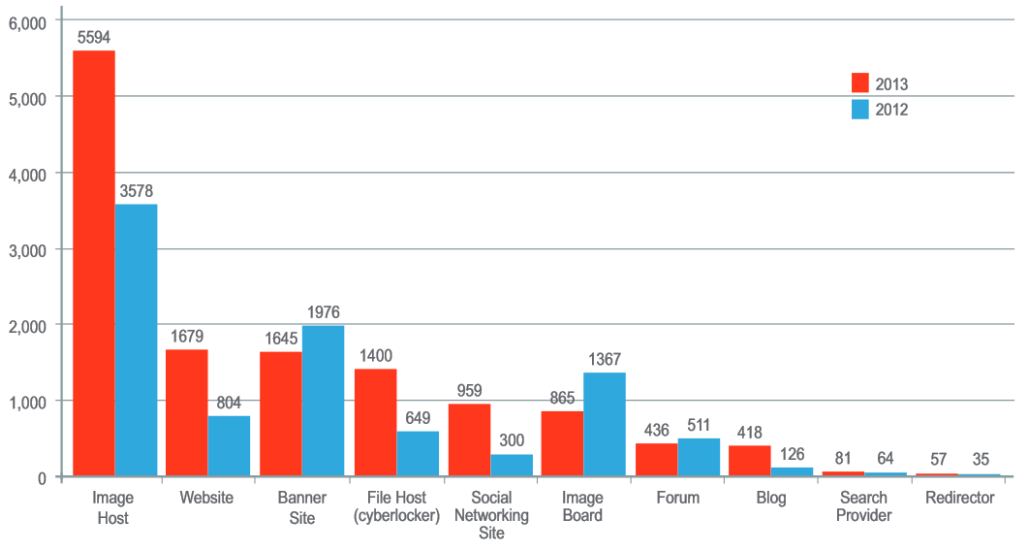


Figura 23 – Top 10 tipi di servizi Internet contenenti materiale pedopornografico: comparazione tra 2013 e 2012[243]

I trend mostrati nel report citato trovano conforto anche nelle stringhe di ricerca sui motori di ricerca. Si presentano i dati relativi ai trend di ricerca di

[242] Ibidem.
[243] Ibidem.

alcune parole chiave relative alla pedopornografia ricavate da Google[244]. Tale grafico mostra quanto spesso viene inserito un particolare termine di ricerca rispetto all'intero volume di ricerca in un'area geografica (o a livello mondiale). L'asse orizzontale del grafico rappresenta il tempo, l'asse verticale la frequenza di ricerca di un termine rispetto al numero totale di ricerche. Le lettere mostrate nel grafico sono utilizzate da Google per segnalare un evento che probabilmente ha scatenato una maggiore ricerca della parola chiave.

Figura 24 – Trend di ricerca della parola chiave "child pornography"

In generale, tutti i trend mostrati evidenziano un calo tra l'inizio del 2004 e la fine del 2007, con un andamento che è proseguito poi in maniera piuttosto costante. La chiave di ricerca generica "child pornography" evidenzia come il termine subisce un elevato numero di ricerche in corrispondenza di fatti di cronaca (ad esempio, il picco in segnalato dalla lettera A di Figura 24 segue l'arresto di dieci minori tra i 13 e i 15 anni a Montereal accusati di condividere materiale pedopornografico).

Oltre al grafico principale, viene offerta la popolarità del termine per nazione, regione, città e lingua. Prendendo sempre in esame la chiave di ricerca "child pornography" si riscontra un picco nelle Filippine.

[244] *https://www.google.it/trends*.

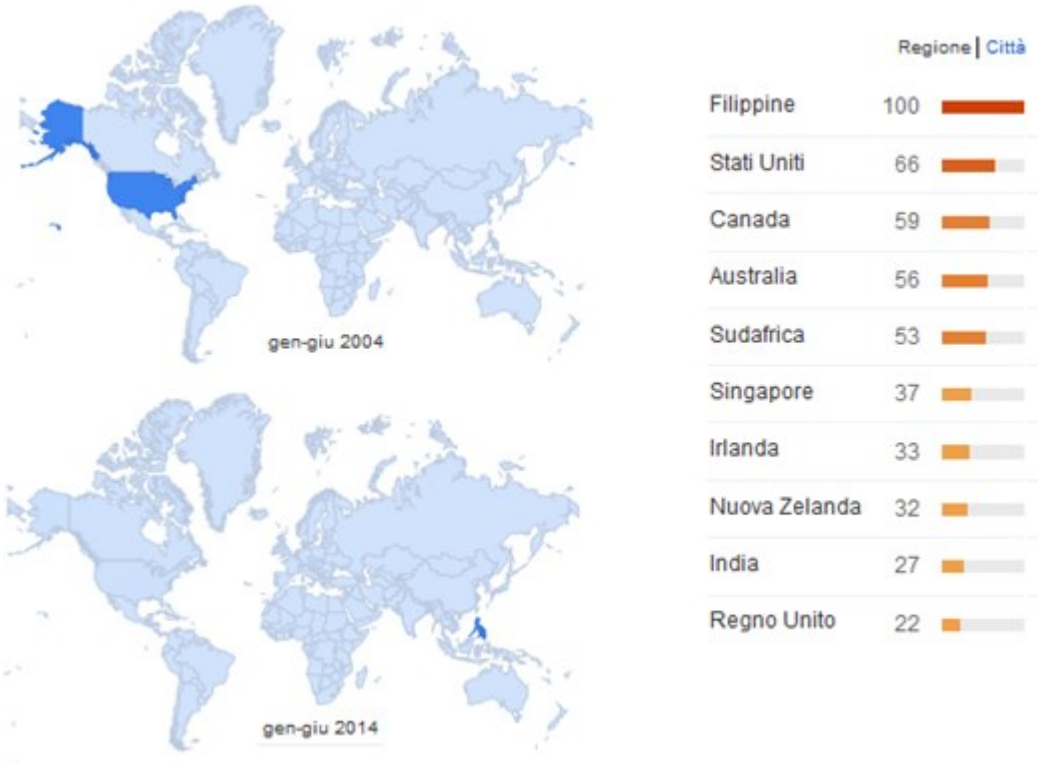


Figura 25 – Trend di ricerca della parola chiave "child pornography" con geolocalizzazione per paese

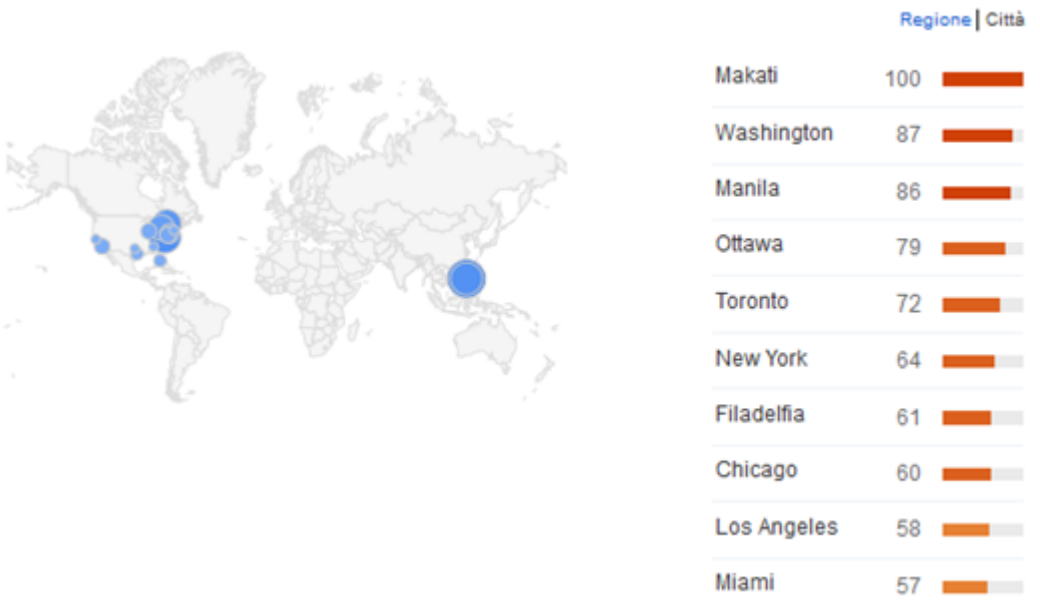


Figura 26 – Trend di ricerca della parola chiave "child pornography" con geolocalizzazione per città

Per quanto riguarda la chiave di ricerca italiana "pedopornografia" si ottiene un risultato analogo in termini di valutazione dei picchi, riscontrando comunque un andamento piuttosto regolare nel tempo anche come prospettiva.

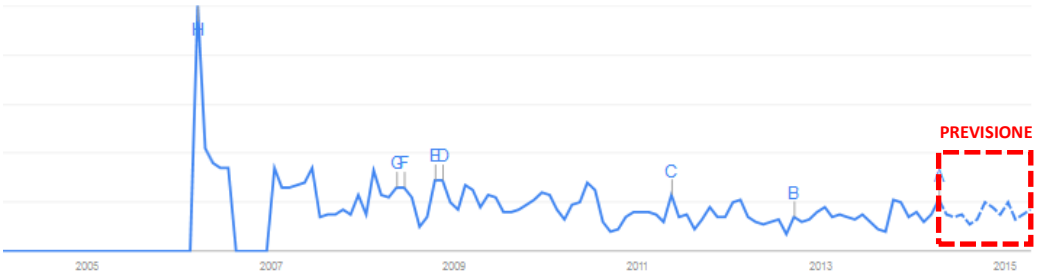


Figura 27 – Trend di ricerca della parola chiave "pedopornografia"

Tra le ricerche correlata a "pedopornografia", Google segnala una chiave probabilmente utilizzata dagli utenti per individuare il materiale illecito ("video pedopornografia") e altre due più generiche ("la pedopornografia" e "reato pedopornografia") utilizzate probabilmente a scopo informativo.

Risultati interessanti si ottengono analizzando i dati relativi a termini di ricerca molto più specifici, potenzialmente utilizzati da utenti alla ricerca di materiale illecito: in questo caso infatti si osserva che l'andamento rimane piuttosto costante nel tempo per chiavi di ricerca di tipo descrittivo quali "child sex" o "child having sex". Gli utenti – provenienti in larga parte da Sri Lanka, Bangladesh, Pakistan, Nepal, India, Nigeria, Filippine, Kenya, Siria, Sudafrica, India, Stati Uniti, Australia, Regno Unito e Canada – utilizzano probabilmente queste chiavi per cercare il materiale da scaricare e per documentarsi sulle modalità di fruizione.

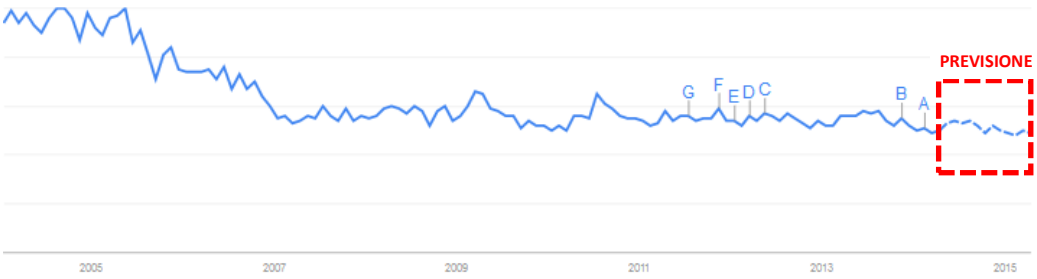


Figura 28 – Trend di ricerca della parola chiave "child sex"

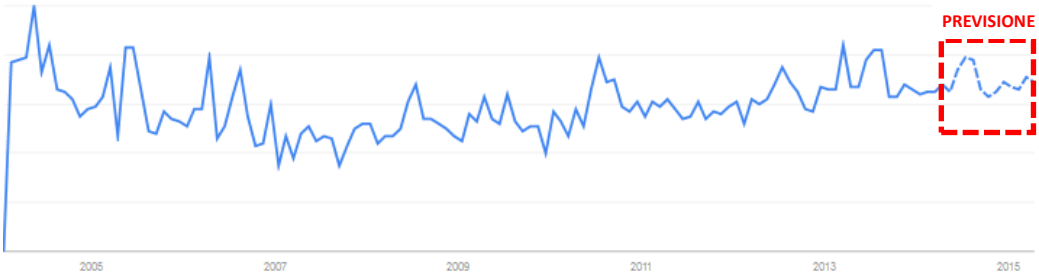


Figura 29 – Trend di ricerca della parola chiave "child having sex"

Accanto alle due chiavi di ricerca sopra identificate infatti Google segnala le seguenti chiavi correlate, con il relativo indice di crescita.

	Parola chiave	Più cercati	In crescita
child sex	child porn sex	100	
	porn child	100	
	sex with child	60	180%
	child sex video	55	450%
	free child sex	50	
	child sex videos	40	400%
	young sex	35	
	children sex	35	
	child sex abuse	30	
	nude child	30	
	indian child sex		200%
	sex offender		90%
	child sex offender		80%
	child having sex		40%
child having sex	sex with child	100	250%
	child porn	75	60%
	children sex	40	
	children having sex	40	
	child sex videos	35	
	kids having sex	35	Impennata
	child sex video	35	Impennata
	young child sex	30	Impennata
	free child sex	20	
	child porn videos	20	Impennata
	child fucking		Impennata
	child sex videos		Impennata

Utilizzando due delle parole chiave "riservate" ai fruitori di materiale pedopornografico si osserva invece come l'andamento di ricerca sia in discesa, probabilmente in ragione del fatto che tali ricerche vengono attualmente condotte direttamente mediante altri canali quali ad esempio il peer-to-peer.

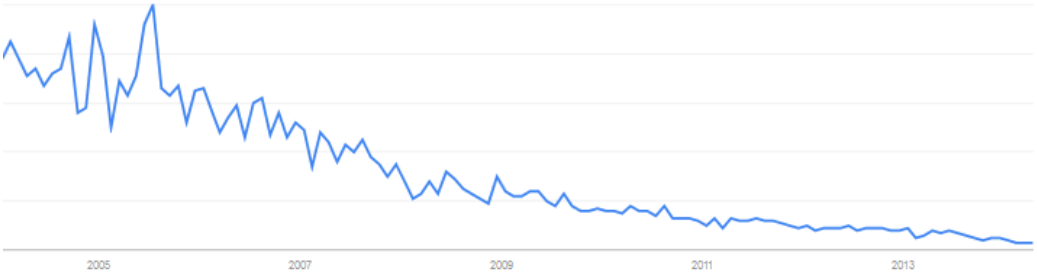


Figura 30 – Trend di ricerca della parola chiave "raygold"

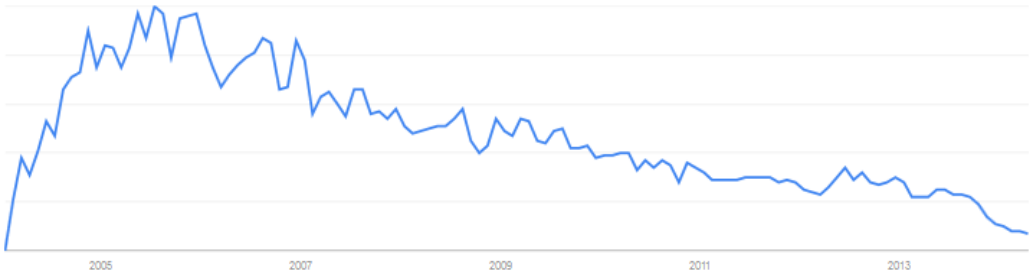


Figura 31 – Trend di ricerca della parola chiave "hussyfan"

Diversamente dal caso delle parole chiave "child sex" e "child having sex", queste ricerche sono prevalentemente condotte da utenti localizzati in Messico, Germania, Canada, Francia, Regno Unito, Stati Uniti e Brasile, ovvero paesi di utilizzatori finali e non di produttori. La diffusione della pedopornografia in questi paesi è documentata anche in un lavoro prodotto nell'ambito del progetto europeo Measurement and Analysis of P2P Activity Against Paedophile Content[245].

4.1.1. Classificazione del materiale pedopornografico

A seconda delle pose assunte dai minori, dal livello di partecipazione, dalle parti del corpo esposte e altri fattori, si fornisce una classificazione del materiale pedopornografico come riportato nella seguente tabella[246].

[245] Fournier R., Latapy M., Magnien C., Seifi M. (2010) *Maps of paedophile activity. http://antipaedo.lip6.fr.*

[246] Quayle E., Taylor M. (2003) *Child pornography: an Internet crime*. Routledge.

Descrizione	Tipologia
Immagini che ritraggono in nudo o in posa erotica, senza alcuna attività sessuale	Nudismo (nudo o seminudo in contesto non illegale); Erotica (fotografie clandestine che mostrano la biancheria intima o nudità); In posa (posa deliberata suggerendo contenuto sessuale); In posa erotica (accento sulla zona genitale); In posa erotica esplicita (accento sulla zona genitale)
Attività sessuale tra i bambini, o masturbazione di un bambino	Attività sessuale esplicita che non prevede la partecipazione di un adulto
Attività sessuale senza penetrazione tra adulto(i) e bambino(i)	Aggressione (violenza sessuale nei confronti di un minore che coinvolge un adulto)
Attività sessuale con penetrazione tra adulto(i) e bambino(i)	Aggressione più evidente (violenza sessuale nei confronti di un minore che coinvolge un adulto)
Sadismo o bestialità	Sadismo o bestialità (immagini sessuali con dolore o animali)

Tabella 3 - Categorie di materiale pedopornografico

4.1.2. Classificazione del fruitore di pedopornografia

Utilizzando alcuni parametri legati alle modalità di accesso e alle conoscenze tecniche personali, si fornisce una classificazione di fruitori di materiale pedopornografico[247]:

- Navigatore accidentale: un utente che naviga in rete può imbattersi involontariamente in materiale pedopornografico (ad esempio, cliccando su un link contenuto in una email ricevuta), decidendo comunque di salvare il materiale. Questo comportamento è illecito se è possibile dimostrare l'intenzione di possedere il materiale. In caso di assenza di confessione da parte della persona, questo può essere dimostrato in presenza di alcune circostanze quali, ad esempio, una ripetuta consultazione del sito contenente il materiale pedopornografico.

[247] Krone T. (2004) A typology of online child pornography offending. In *Australian Institute of Criminology, Trends and Issues in Crime and Criminal Justice*, 279.

- Curioso: non esiste alcun reato qualora una persona avesse una fantasia privata relativa a sesso con minori. Se tuttavia la fantasia trova applicazione, ad esempio mediante rappresentazione in formato digitale, il reato viene posto in essere anche in caso di assenza di attività di divulgazione. Per la persona che commette un reato di questo tipo, il rischio di esposizione è molto basso dal momento che solo lui stesso è a conoscenza del possesso di tale materiale; tuttavia la scoperta può avvenire in vari modi: ad esempio, può essere segnalato da qualcuno che utilizza il sistema informatico che contiene il materiale, da chi ricerca materiale utile per altri reati, da chi è intento ad effettuare una riparazione del sistema.
- Consumatore di pornografia: in questa categoria è possibile raggruppare tre casi: l'utente sessualmente "onnivoro", alla ricerca generica di materiale pornografico nell'ambito del la pornografia infantile è semplicemente una parte e non la parte predominante; l'utente sessualmente curioso che ha sperimentato il materiale pedopornografico, ma non ne ha particolare interesse; il libertario che è spinto a far valere diritti a essere liberi di accedere a qualsiasi genere di materiale si possa desiderare.
- Collezionista non protetto: il collezionista non protetto acquista, scarica o scambia materiale pedopornografico da risorse disponibili liberamente in Internet (siti, chat room, reti peer-to-peer…) senza utilizzare barriere che elevino la propria sicurezza quali ad esempio password, cifratura o numero massimo di immagini possedute. Questa tipologia di utente ha certamente un buon livello di informatizzazione superiore a quella degli utenti dei livelli precedenti, ma non a sufficienza da comprendere la necessità di aumentare il proprio livello di sicurezza.
- Collezionista protetto: rispetto all'utente della categoria precedente, questa tipologia di utente innalza barriere di sicurezza (ad esempio, cifratura) che possono essere impiegata a diversi livelli di efficienza. In aggiunta, alcuni gruppi di utenti hanno requisiti di accesso alla cerchia quali ad esempio la presentazione da parte di altri membri o il caricamento di un certo numero di file nuova produzione.
- Adescatore in rete: l'adescatore in rete (groomer) è una persona che ha iniziato a contattare minori online con l'intenzione di stabilire una relazione sessuale con essi che può andare dal sesso virtuale al sesso

fisico. Il materiale pedopornografico è utilizzato per stabilire un contatto con il minore ed abbassarne le inibizioni. L'adescamento di minori in rete è stato definito di recente nella Convenzione di Lanzarote.

- Abusatore fisico: l'abusatore fisico è attivamente impegnato ad abusare di minori e la pornografia minorile è solo uno strumento supplementare al soddisfacimento del desiderio sessuale personale. L'abuso sessuale può essere registrato per uso personale futuro ma non è finalizzato alla distribuzione. In casi di questo tipo, il reato di detenzione di pedopornografia non è il capo d'accusa principale, essendo legato alla violenza sessuale sul minore.
- Produttore: il produttore di materiale pedopornografico è impegnato ad abusare sessualmente di minori al fine di produrre materiale pedopornografico destinato ad altri utenti.
- Distributore: il distributore di materiale pedopornografico può avere interesse sessuale nella pedopornografia o anche non averne, assumendo in questo secondo caso il ruolo di "imprenditore" disinteressato in prima persone del bene commercializzato.

Le categorie appena definite vengono riportate in una tabella riassuntiva dove, per ogni tipologia di utente, si riprendono le caratteristiche identificative principali, la valutazione del livello di partecipazione alla rete, la valutazione delle misure di sicurezza informatica adottate, la natura dell'abuso sul minore inteso come contatto con la vittima.

Tipologia di utente	Caratteristiche	Livello di partecipazione in rete	Sicurezza informatica	Natura dell'abuso
Navigatore accidentale	Accesso al materiale in maniera accidentale (da spam, popup…) tuttavia, il materiale viene salvato consapevolmente	Zero	Zero	Indiretto
Curioso	Creazione consapevole di testo o di immagini digitali online per uso privato	Zero	Zero	Indiretto
Consumatore di pornografia	Attivamente in cerca di pornografia infantile utilizzando i browser apertamente disponibili	Basso	Zero	Indiretto
Collezionista non protetto	Attivamente in cerca di materiale spesso attraverso reti peer-to-peer	Alto	Zero	Indiretto
Collezionista protetto	Attivamente in cerca di materiale, ma solo attraverso reti sicure . La sindrome di raccolta e di scambio come una barriera all'entrata	Alto	Sicuro	Indiretto
Adescatore in rete	Coltivare un rapporto online con uno o più bambini. L'autore del reato può o non può cercare materiale in qualsiasi dei modi di cui sopra. La pornografia può essere utilizzato per facilitare abusi	Varia. Contatto online con i singoli bambini	Sicurezza dipende da bambino	Diretto
Abusatore fisico	Abusare di un bambino che potrebbe essere stato introdotto al trasgressore online. L'autore del reato può o non può cercare materiale in qualsiasi dei modi di cui sopra. La pornografia può essere utilizzato per facilitare abusi	Varia. Contatto online con i singoli bambini	Sicurezza dipende da bambino	Diretto
Produttore	Registra i propri abusi o quelli degli altri (o induce i bambini ad inviare le immagini di sé stessi)	Varia. Dipende se anche distributore	Sicurezza dipende da bambino	Diretto
Distributore	Può distribuire ad un soggetto qualificato nei livelli precedenti	Vari	Tende ad essere sicuro	Indiretto

Tabella 4 - Categorie di fruitori di materiale pedopornografico

4.2. L'attività d'indagine della polizia giudiziaria

Correva l'anno 1994 quando si realizzò l'operazione Fidobust[248], la prima corposa indagine su scala nazionale basata sulla normativa sul diritto d'autore da poco modificata (D. Lgs. 518/1992), nonché sulla disciplina introdotta, allora di recente, sui crimini informatici (L. 547/1993).

La vicenda era stata presa molto sul serio dall'autorità giudiziaria procedente che aveva ipotizzato quasi tutti i reati relativi ai fenomeni informatici penalmente rilevanti: duplicazione abusiva di software, frode informatica, contrabbando[249] e associazione a delinquere che consentiva l'unitarietà dell'indagine. L'aspetto associativo era stato individuato mediante l'osservazione di un fenomeno vero ed il suo totale travisamento in fatto. La maggior parte degli indagati gestiva dei BBS[250] della rete Fidonet[251], a quel tempo uno dei pochi strumenti disponibile per chiunque per comunicare a distanza. Nella totale inconsapevolezza di cosa fosse la rete Fidonet, le telefonate, prevalentemente notturne, tra i computer furono scambiate per i collegamenti tra i vari associati dove taluno fu indagato per una connessione tra due modem di 23 secondi.

L'inesperienza totale degli inquirenti diede luogo a situazioni che oggi si potrebbero giudicare esilaranti, pur essendo anche drammatici per chi li subì[252].

---

[248] Gubitosa C. (1999) *Italian Crackdown*. Apogeo.

[249] Per giustificare il contrabbando, la giustificazione "ci sono dei programmi in inglese e quindi di provenienza straniera".

[250] Un BBS (*Bulletin Board System*) è un computer che utilizza un software per permettere a utenti esterni di connettersi a esso attraverso la linea telefonica, dando la possibilità di utilizzare funzioni di messaggistica e file sharing centralizzato. Il sistema è stato sviluppato negli anni settanta del XX secolo, e ha costituito il fulcro delle prime comunicazioni telematiche amatoriali, dando vita alla telematica di base. Nell'uso moderno (soprattutto in giapponese) il termine viene usato anche per indicare i forum, i guestbook e i newsgroup su Internet.

[251] Fidonet è una rete informatica creata nel 1984 e utilizzata dalle BBS per lo scambio ed il trasporto file e messaggi che ha preceduto la creazione del World Wide Web. Dato che le connessioni utilizzano la stessa linea telefonica dell'utente della BBS, Fidonet effettuava i trasferimenti solo in precise ore del giorno (Zone Mail Hour, tipicamente alle 4:00 del mattino). Pur avendo perso importanza a causa del WWW, è ancora in uso come rete amatoriale in alcune aree del mondo.

[252] In alcuni casi si sono verificati sequestro di mouse con relativo tappetino e di ciabatte di prese multiple, fino a sigilli alla camera da letto nella quale era posizionato il computer. Il

Ciò che stupì allora, e lascia perplessi ancora oggi, fu l'utilizzazione di ragionamenti logici vecchi per fenomeni nuovi, senza un'analisi approfondita dell'oggetto di indagine: ad esempio, nessuno si domandò per quale motivo ci fossero tante telefonate, brevi e secondo pattern ben precisi, di notte o come si potesse trasmettere software per via telematica con modem a velocità molto basse, rischiando di pagare più di connessione che per il software originale.

Da allora certamente l'attività di indagine della polizia giudiziaria è notevolmente migliorata in tema di crimini informatici, anche se continuano a verificarsi sequestri massivi di materiali accessori (ad esempio, tastiere) o alterazioni di reperti, principalmente a causa di accessi privi di blocchi in scrittura ai supporti informatici.

Ogni investigatore dovrebbe godere delle seguenti qualità: intuito, tempestività, tenacia, buonsenso, freddezza, equilibrio, fantasia, curiosità, amore per la verità[253]. Quando l'investigatore si interfaccia con la materia informatica deve seguire rigorosamente le varie fasi di conservazione, acquisizione, analisi, valutazione e presentazione[254], che significa raccogliere informazioni sul tipo di reato, reperire i log del sistema, stimare i danni e le modifiche al sistema, elaborare le informazioni, procedere alle richieste di risoluzione di indirizzi IP all'Internet Service Provider, acquisire i vari supporti informatici e analizzare tutti i dati complessivamente acquisiti.

L'attività della polizia giudiziaria è sia preventiva, dunque focalizzata al monitoraggio, alla partecipazione, all'iscrizione ad eventuali aree riservate e all'informazione, che repressiva, mediante intercettazioni telematiche, attività sotto copertura e analisi dei dati ottenuti.

Tuttavia, le indagini informatiche si scontrano sempre più spesso con problematiche di natura tecnica che impediscono di individuare l'autore di un reato o, peggio, portano all'individuazione di una persona che è invece estranea ai fatti. Problemi tipici nelle indagini si riscontrano nei seguenti casi:

- anonymous remailer: si tratta di un server che riceve messaggi di posta elettronica e li rinvia seguendo apposite istruzioni incluse nei messaggi stessi, senza rivelare la loro provenienza originaria;

tribunale del riesame revocò poi il sequestro sull'hardware, mantenendolo invece sui supporti di memorizzazione di dati digitali.

[253] Intini A., Picozzi M. (2009) *Scienze Forensi. Teoria e prassi dell'investigazione scientifica*. Utet.

[254] Carrier B. (2006) *A hypothesis-based approach to digital forensic investigations*. PhD thesis, Purdue University.

l'utilizzo di sistemi di invio di messaggi di posta elettronica in maniera anonima impedisce di risalire all'utente che aveva inviato originariamente l'email, dal momento che l'indirizzo IP di partenza del messaggio non consente di risalire al mittente reale;

- reti anonime: come nel caso precedente, la navigazione all'interno di reti anonime come TOR[255] vanifica i tentativi di individuazione dell'autore di una condotta illecita;
- assenza di log: quando non vengono utilizzati sistemi di anonimizzazione, i dati relativi ad una condotta illecita possono essere individuati all'interno dei file di log; tuttavia, quando il meccanismo di registrazione degli eventi è assente, insufficiente (mancano alcuni dati) o rimosso (ad esempio, quando è trascorso un certo periodo temporale dai fatti), risulta comunque impossibile risalire all'utente al pari dei due casi precedentemente esposti;
- utilizzo di reti wireless: nelle situazioni in cui il punto di accesso alla rete si estende oltre ai confini fisici dei muri perimetrali, la platea dei potenziali autori del reato aumenta, soprattutto nei casi in cui la rete fosse sprovvista di meccanismi di autenticazione (password WPA, credenziali di accesso, identificazione mediante MAC address del sistema informatico…);
- controllo di sistemi informatici altrui: qualora il reati risultasse commesso da un sistema informatico che si rivela compromesso ed utilizzato da remoto da altri utenti, si perde il legame con la persona che realmente ha commesso il fatto illecito.

Si osservi come in generale l'identificazione del potenziale autore del reato avviene risolvendo l'indirizzo IP: ovvero, partendo dal sistema informatico in cui vi è traccia della commissione del reato e dell'indirizzo IP di partenza identificato, si contatta l'Internet Service Provider per richiedere l'utenza telefonica alla quale era associato l'indirizzo IP ad un certo orario e quindi al soggetto intestatario del contratto di telefonia. In questo modo, soprattutto per gli ultimi due punti presentati, è frequente che una persona totalmente estranea

[255] TOR (The Onion Router) è un sistema di comunicazione anonima per Internet basato sul protocollo di onion routing che ha lo scopo di rendere difficile l'analisi del traffico e proteggere così la privacy e la riservatezza delle comunicazioni: i dati che appartengono ad una qualsiasi comunicazione non transitano direttamente dal client al server, ma passano attraverso i server Tor che agiscono da router costruendo un circuito virtuale crittografato a strati.

ai fatti si ritrovi indagata solo in quanto intestataria di un contratto di connettività alla rete.

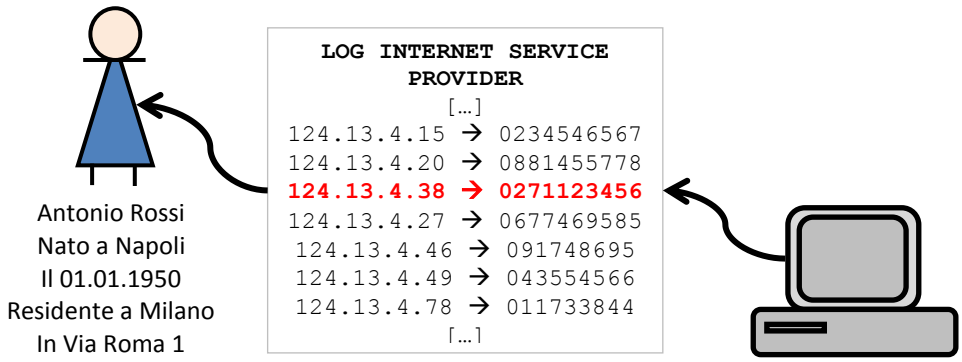


Figura 32 – Esemplificazione dello schema di risoluzione di un indirizzo IP nella persona titolare del contratto di connettività: l'immagine va letta da destra verso sinistra

Alla luce di queste problematiche di indagine, soprattutto in contesti dove ad un utenza telefonica corrispondono più utilizzatori, sarebbe di fondamentale importanza per le indagini disporre di meccanismi per una corretta e funzionale gestione delle credenziali di accesso e dei log di sistema. Infatti, in caso di incidente informatico, per collaborare al meglio alle indagini occorre fornire log degli accessi (con indicazione di data e ora, durata, utilizzatore e sistema informatico utilizzato), avendo cura di avere sempre sincronizzati e correttamente impostati gli orologi di tutti i sistemi, il tipo e la versione dei sistemi in uso (sia hardware che software), i nominativi delle figure professionali di riferimento tecnico e una descrizione particolareggiata del tipo di operazioni illecite e dei danni accertati.

In Italia, il RACIS per i Carabinieri, il Nucleo Speciale Investigazioni telematiche (ex GAT) per la Guardia di Finanza e la Polizia Postale per la Polizia di Stato sono i corpi specializzati in tema di indagini informatiche:

- il RACIS (Raggruppamento Carabinieri Investigazioni Scientifiche), nato nel 1955, ha sede a Roma ed è presente sul territorio nazionale con quattro Reparti Investigazione Scientifica (Cagliari per la

Sardegna; Messina per Sicilia e Calabria; Roma per Italia centrale e meridionale; Parma per Italia settentrionale)[256];

- il Nucleo speciale frodi tecnologiche, precedentemente noto come Nucleo speciale frodi telematiche e prima ancora Gruppo anticrimine tecnologico (GAT), è la sezione della Guardia di Finanza italiana nata nel 2001 che si occupa di frodi telematiche ed informatiche;
- il Servizio di Polizia Postale e delle Comunicazione è definito con il Decreto del Ministero dell'Interno del 30 marzo 1998 secondo il quale a tale organismo spetta il compito di coordinamento operativo dei compartimenti, sicurezza delle comunicazioni, analisi ed elaborazione di strategie, rapporti internazionali;
- presso la Polizia di Stato è istituita altresì l'unità di analisi sul crimine informatico (Computer Crime Analysis Unit), composta da personale tecnico e investigativo che si occupa di affiancare gli investigatori della Polizia Postale e delle Comunicazioni nelle indagini sui crimini ad alta tecnologia, progettando nuove tecniche investigative e tracciando profili psicologici e comportamentali degli autori di tali crimini. Tra le attività della struttura si individuano:
    - ricerche e studi sul fenomeno della criminalità informatica in collaborazione con Università, Aziende ed Istituzioni;
    - sperimentazione di nuove tecniche investigative in materia di computer crime;
    - progettazione di percorsi di formazione sulla sicurezza informatica e computer crime in collaborazione con Università e aziende;
    - divulgazione di informazioni e risultati di ricerche in contesti scientifici;
    - assistenza psicologica degli investigatori che si occupano di computer crime (pedofilia).

A livello sovranazionale, per soddisfare le esigenze di cooperazione internazionale si identificano il Comitato per la politica dell'informatica e delle comunicazioni (ICCP) dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE), l'High Technology Crime Investigation Association

[256] Autorevoli sono gli interventi dell'Ufficiale dei Carabinieri Marco Mattiucci che gestisce anche un sito web preciso e aggiornato su temi di informatica forense disponibile all'url *http://www.marcomattiucci.it*.

(HTCIA) del G8[257], il Child Pornography Group che è parte del network di polizie denominato Virtual Global Task force (VGT)[258], l'European Working Party on information technology crime che si riunisce periodicamente presso il segretariato generale interpol di lione, nel comitato high tech crime dell'Europol e del Police Cooperation Working Group (PCWG) della Commissione Europea.

4.2.1. Contrasto alla pedopornografia online: la censura di siti web e la black list del CNCPO

In tema di pedopornografia, la legge 38/2006 ha istituito presso la Presidenza del Consiglio dei ministro l'Osservatorio per il contrasto della pedofilia e della pornografia minorile ed ha affidato al Centro Nazionale per il Contrasto della pedopornografia sulla rete Internet della Polizia Postale la funzione di raccogliere tutte le segnalazioni provenienti anche da organi di polizia stranieri e da soggetti pubblici e privati impegnati nella lotta alla pornografia minorile riguardanti ambiti di rete che diffondono materiale relativo all'utilizzo sessuale dei minori a mezzo Internet[259].

In materia ha assunto particolare rilevanza il Decreto[260] dell'allora Ministero delle Comunicazioni Gentiloni che in materia di oscuramento dei siti pedopornografici ha previsto dei requisiti tecnici di strumenti di filtraggio che i fornitori di connettività alla rete internet devono utilizzare al fine di impedire, con le modalità previste dalle leggi vigenti, l'accesso ai siti segnalati dal CNCPO: pertanto i provider ricevono periodicamente delle liste nere di indirizzi e provvedono ad applicare filtri al fine di impedirne l'accesso[261],

[257] *http://www.htcia.org*.

[258] *http://www.virtualglobaltaskforce.com*.

[259] Macilotti G. (2011) Il contrasto alla pedopornografia online: esperienze italiane e francesi a confronto. *Rivista di Criminologia, Vittimologia e Sicurezza*, V(1), 81–107.

[260] Ministero delle comunicazioni, decreto 8 gennaio 2007: Requisiti tecnici degli strumenti di filtraggio che i fornitori di connettività alla rete Internet devono utilizzare, al fine di impedire, con le modalità previste dalle leggi vigenti, l'accesso ai siti segnalati dal Centro nazionale per il contrasto alla pedopornografia, G.U. n. 23 del 29 gennaio 2007.

[261] Agli articoli 3, 4 e 5 del Decreto del Ministero delle comunicazione del 8 gennaio 2007 viene indicato il meccanismo con il quale il CNCPO comunica ai fornitori di connettività la lista dei siti da filtrare. C'è tuttavia da evidenziare che tale filtro è facilmente aggirabile da un qualsiasi utente con una discreta competenza nell'uso di un sistema informatico: infatti il filtro prevede la modifica della tabella DNS con la quale i provider associano un url (ad esempio, www.sito.it) ad un indirizzo IP (ad esempio 100.120.140.160). Quando l'url fa riferimento ad un sito da oscurare, viene modificata l'associazione ed impostato un indirizzo IP di una pagina

proponendo al visitatore una pagina di servizio come quella mostrata in Figura 33.

Figura 33 – Pagina di servizio utilizzata per i siti oscurati

Tale indicazione necessita di un'osservazione critica di natura tecnica: per aggirare un problema di questo genere è sufficiente che l'utente modifichi i

di servizio che informa dell'oscuramento (ad esempio 200.240.70.80), pertanto da quel momento in poi gli utenti che digiteranno nella barra degli indirizzi l'url (nell'esempio, www.sito.it) vedranno comparire la pagina di servizio disponibile al nuovo indirizzo IP (nell'esempio, 200.240.70.80). Tuttavia, tale sistema è facilmente aggirabile utilizzabile un Server DNS diverso da quello del provider che ha provveduto al filtro. Il CNCPO infatti riesce ad ottenere la modifica del database dei DNS dei fornitori di servizi di connettività italiani, non potendo invece alterare server neutrali (tipo OpenDNS) o privati. Peraltro, tale modalità di oscuramente provoca effetti collaterali per i domini di terzo livello, come il caso (non ufficialmente confermato dal momento che la lista nera è segreta e accessibile solo ai vari provider accreditati) del dominio tumblr.com del febbraio 2013 quando il CNCPO ha inserito, e poco dopo rimosso, uno dei domini che contengono le immagini caricate sulla piattaforma di microblogging. Il dominio *25.media.tumblr.com* è dunque risultato irraggiungibile agli utenti italiani a seguito dell'inserimento dell'url nella lista nera. Qualcuno ha subito sottolineato come la blacklist del CNCPO ordini di bloccare una singola immagine, con la possibilità di estendere il blocco ad un intero dominio in mancanza di tecniche censorie più mirate. In sostanza, gli utenti italiani della piattaforma di blogging non sono più riusciti a visualizzare molta parte delle immagini caricate online.

DNS[262] utilizzati rendendo di fatto inutile lo strumento di filtraggio impostato dal provider. Altro problema riguarda i siti che utilizzano indirizzi IP dinamici in virtù del fatto che il sito può cambiare indirizzo molto rapidamente, bloccando invece eventuali utenze successivamente assegnatarie di detto indirizzo IP.

4.2.2. Il monitoraggio sulle reti peer-to-peer

La pedopornografia è offerta – e richiesta – online su praticamente tutti i canali disponibili: siti web (sia aperti che ad accesso riservato), social network, chat, email, file sharing. Alla luce di questa diffusione, le investigazioni da parte della polizia giudiziaria richiedono la copertura integrale della rete mediante attività di intercettazione sotto copertura, monitoraggio di siti web e chat, partecipazione a forum e community, iscrizione a maling list.

Il monitoraggio delle reti peer-to-peer[263] è più complesso e può seguire due metodi: indiretto e diretto[264]. Con il monitoraggio indiretto le autorità di controllo si basano su indizi indiretti quali ad esempio la presenza dell'indirizzo IP del nodo all'interno di un gruppo di possessori di un file. Tale metodo tuttavia rende un elevato tasso di falsi positivi. Con il monitoraggio diretto, forze dell'ordine raccolgono prove direttamente dal nodo, ricevendo (modalità passiva) o trasmettendo (modalità attiva) il materiale illecito. Chiaramente, tecniche di monitoraggio diretto consentono di raccogliere potenziali prove digitali più conclusive che presentano meno falsi positivi, ma l'attività risulta più costosa in termini di larghezza di banda, risorse computazionali e costo di personale[265].

[262] Il Domain Name System (DNS) è un sistema utilizzato per la risoluzione di nomi dei nodi della rete (in inglese host) in indirizzi IP e viceversa. Il servizio è realizzato tramite un database distribuito costituito dai server DNS. Tale meccanismo si occupa della conversione della risorsa richiesta (ad esempio, *http://www.google.it*) nell'indirizzo IP della macchina che ospita fisicamente la risorsa (ad esempio, *173.194.35.31*).

[263] Chothia T., Cova M., González C., Novakovic C. (2013) The Unbearable Lightness of Monitoring: Direct Monitoring in BitTorrent. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, 106, 185–202.

[264] Kohno T., Krishnamurthy A., Piatek M. (2008) Challenges and Directions for Monitoring P2P File Sharing Networks - or - Why My Printer Received a DMCA Takedown Notice. In *Proceedings of the USENIX Workshop on Hot Topics in Security*, San Jose, USA.

[265] Bauer K., Grunwald D., McCoy D., Sicker D. (2009) Bitstalker: Accurately and efficiently monitoring bittorrent traffic. *Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS)*, London, UK, 2009.

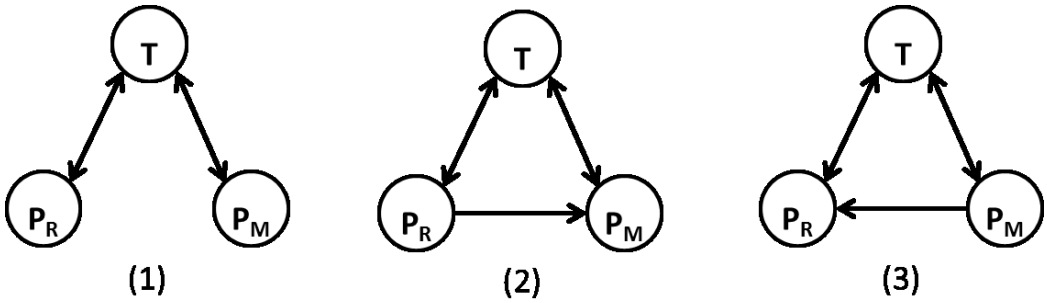


Figura 34 – Differenti metodologie per il monitoraggio da parte del nodo P_M (Peer monitoring) nei confronti di un nodo (P_R) attraverso il tracker (T): 1 indiretto; 2 diretto passivo; 3 diretto attivo

4.2.3. Keyword utilizzate per la ricerca di materiale pedopornografico su reti peer-to-peer

In molti sistemi peer-to-peer, incluso eDonkey, gli utenti cercano file utilizzando query basate su parole chiave. Il sistema cerca e fornisce quindi i file che contengono all'interno del nome le parole chiave indicate e l'utente può scegliere di scaricare il file sulla base di altre informazioni quali il nome complessivo del file, la dimensione, il tipo di file, il numero di utenti remoti che lo forniscono e così via. Di conseguenza, le keyword giocano un ruolo chiave nella funzionalità e nell'uso di questi sistemi: preso atto che normalmente i nomi dei file ne descrivono il contenuto, che file uguali possono essere identificati da nomi diversi e che file diversi possono essere caratterizzati dallo stesso nome, affinché il sistema sia affidabile occorre che i nomi dei file rispecchino il reale contenuto al fine di rendere efficace questo genere di ricerca.

In eDonkey, quando un utente effettua una ricerca basata su keyword il server cerca tra i nomi di file che contengono tali parole, restituendo in output i file corredati da tutte le informazioni accessorie (filename, dimensione…): ad esempio, l'utente che cerca con la keyword "Lady Gaga" esprime evidentemente interesse per contenuti relativi alla cantante Lady Gaga, quali file musicali o video. La presenza delle parole chiave "Lady" e "Gaga" in un nome di file indicate che tale file probabilmente è relativo alla cantante Lady Gaga (video di un concerto, promo di un nuovo brano, brano dell'ultimo

singolo...); il resto del nome del file, inclusa l'estensione, fornisce dettagli aggiuntivi sul contenuto[266].

Alcuni articoli[267] di ricerca su temi di misurazione di file pedopornografici all'interno della rete eDonkey a cura del LIP6[268] hanno affrontato il tema dell'analisi delle parole chiave utilizzate per indicizzare i file contenenti materiale pedopornografico.

Una valutazione delle keyword si è basata sull'analisi dei messaggi inviati e ricevuti da un server di eDonkey in un periodo di 10 settimane: con circa 9 miliardi di messaggi scambiati sono transitate informazioni su circa 90 milioni di utenti e su oltre 275 milioni di file distinti.

Per quanto concerne il materiale di natura pedopornografica, l'analisi dei dati osservati[269] evidenzia i pedofili tendono a evitare il rilevamento utilizzando le parole chiave segrete, pertanto accade che si trovano file con parole di pedopornografia che tuttavia non hanno contenuto pedofilo, mentre alcuni file con nome "innocente" contengono materiale di pornografia minorile.

I termini maggiormente utilizzati per identificare file a contenuto pedopornografico sono "lolita", "ptsc", "hussyfan", "raygold", "r.gold", "r@aygold", "babyj", "babyshivid", "kidzilla", "phtc", "*n*y", "*n*yo", "*n*yr"[270].

[266] Ad esempio, in molti file nel nome del file viene riportata una sigla che indica la lingua dell'audio: nel caso di file in lingua italiana solitamente è qualcosa tipo [ITA].

[267] Magnien C., Latapy M., Guillaume J., Le Grand B. (2008) *First Report on Paedophile Keywords Observed in eDonkey*. Belbèze C., Chavalarias D., Denoyer L., Fournier R., Guillaume J., Latapy M., Magnien C., Valadon G., Vehovar V., Žiberna A. (2010) *Technical report on Automatic Identification of Paedophile Keywords*. Gli articoli precedenti sono disponibili all'url *http://antipaedo.lip6.fr* del progetto europeo Measurement and Analysis of P2P Activity Against Paedophile Content. Si segnalano inoltre Aidouni F., Latapy M., Magnien C. (2009) Ten weeks in the life of an eDonkey server. In *Sixth International Workshop on Hot Topics in Peer-to-Peer System (Hot-P2P 2009*). Roma, Maggio 2009. Fournier R., Latapy M., Magnien C., Valadon G. (2009) Tracing paedophile eDonkey users through keyword-based query. In: Seifi M., ed. *Proceeding of International Conference Advances in the Analysis of Online Paedophile Activity*. Belbèze C., Latapy M. (2009) Detecting keywords used by paedophiles. In: Seifi M., ed. *Proceeding of International Conference Advances in the Analysis of Online Paedophile Activity*, 93–96.

[268] Il LIP6 (Laboratoire d'informatique de Paris 6) è un laboratorio di ricerca dell'Università Pierre e Marie Curie e del CNRS.

[269] Magnien C., Latapy M., Guillaume J., Le Grand B. (2008) First Report on Paedophile Keywords Observed in eDonkey.

[270] Nei termini *ny*, *n*yo e *n*yr, *n* è un numero minore di 18 che viene utilizzato per identificare l'età dei protagonisti delle scene rappresentate all'interno del file, *y* e *yr* sono

La natura pedopornografica di diversi dei termini presentati è confermata da Urban Dictionary[271], un dizionario di slang.

Analizzando i dati individuati nelle reti peer-to-peer e confrontando tali risultati anche con valutazioni di soggetti impegnati nel contrasto della pedopornografia, emerge che le keyword che appaiono maggiormente nei file di natura pedopornografica sono le seguenti: 1man, 2005new, 349, 4yo, 5yo, 7yo, 7o, 8yo, 9yo, 10y, 10yo, 11yo , 12y, 12yo, abt, amateurz, arina, ass, baby, babyj, babyshivid, babyshvid, bambina, bbx, bella, boy, boylover, cambodian, cbaby, child, childfugga, childlover, childs, childsex, ck, cries, cum, cs, dad, daddy, daughter, diaper, doggyfuck, doughter, eurololita, furs, girl, girls, gostosinha, harier, hussyfa, hussyfan, hussyfun, hyman, illegal, inces, incest, infant, inga, inna, island, island03, jackie, jailbait, janniefer, jenny, jho, kdquality, kdv, kiddy, kids, kidzilla, kinderficker, kindergarden, kingpass, kleuterkutje, kurahashi, laika, liluplanet, little, lolalover, lolifuck, lolita, lolita2, lolitaguy, lordofthering, ls, lsbar, lsm, lsn, lso, lsp, lsw, lucie, luto, mafiasex, maryanne, mellony, model, moscow, mylola, nablot, newcaps, newstar, nimbus, nimphets, nn, novinhas, nude, nude01, nudis, olds, pae, pedo, pedofilia, peepee, petersburg, phantom, phtc, playtoy, porn, pre, preteen, preteenz, pretten, ptivate, prt, pt, ptff, ptsc, pussy, qqaazz, rape, raygold, r@aygold, r.gold, reallola, rizmaster, sandra, sex, sofie, spam, spreading, stasia, st, teen, tochter, tori, torture, ul5, underage, valya, vater, vdbest, vicky, xlola, yamad, ye, yelitza, yg, ygold, young.

L'utente che intende condividere e/o scaricare materiale pedopornografico utilizza dunque sia termini che hanno un senso (ad esempio "child porn"), sia termini specifici del settore (ad esempio "qqaazz"). Tali keyword possono essere sconosciute agli altri utenti (comprese forze dell'ordine, consulenti tecnici e giuristi che si occupano di questi casi) e mantenuti segreti all'interno di queste comunità: nuove keyword infatti potrebbero apparire nel tempo.

La conoscenza delle parole chiave di riferimento è dunque un elemento determinante sia per accertare la consapevolezza nella ricerca e nell'ottenimento di questo genere di materiale, sia per le attività di contrasto da parte delle forze dell'ordine: monitoraggio della rete, investigazioni online,

abbreviazioni di *years* e *yo* di *years old*; ad esempio, 7y, 7yr o 7yo indicano soggetti di 7 anni (7 years old).

[271] *http://www.urbandictionary.com/*.

analisi forense dei sistemi informatici coinvolti richiedono la piena conoscenza di questo insieme di dati.

4.3. Il problema dei file fake e della consapevolezza

Come verrà nel seguito definito, i file sulle reti peer-to-peer sono identificati mediante un hash. Tuttavia, ogni file è anche caratterizzato da altri elementi non identificativi univoci ma comunque rilevanti quali dimensione e, soprattutto, nome del file: il nome del file è infatti visto come una sequenza di parole chiave che vengono utilizzate all'atto della ricerca.

Uno dei problemi maggiori dello scambio di file nelle reti peer-to-peer è dato dalla difficoltà di arginare lo scambio di file cosiddetti *fake*, file che si presentano sotto un certo nome e una certa estensione che in realtà possono contenere al loro interno materiale di tipo e contenuto completamente diverso[272]. Esistono due categorie di file fake:

1. file con nome riferibile alla pedopornografia che tuttavia contengono materiale non pedopornografico;
2. file con nome non alludono alla pedopornografia che invece contengono materiale pedopornografico.

Il fenomeno dei file fake nelle reti peer-to-peer non riguarda solo la pedopornografia ma anche qualsiasi genere di contenuto (ad esempio, file video con nomi di cartoni animati che invece contengono film pornografici o di altro tipo) e per comprendere quanto è diffuso è sufficiente prendere in esame un qualsiasi file osservando che con estrema probabilità lo stesso è disponibile in rete con nomi diversi. Ad esempio, il file con hash 561a069cac2a4ff5d6bd14c747145c9f è stato individuato in rete con almeno tre nomi diversi.

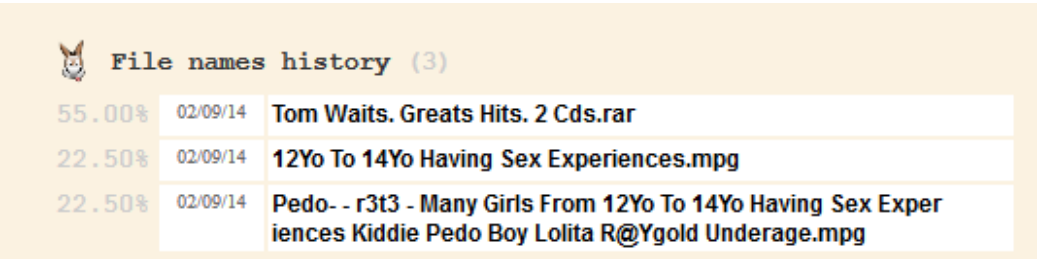


Figura 35 – Esempio di file fake presente in rete eDonkey con tre nomi differenti

[272] Guillaume J., Latapy M., Magnien C., Valadon G. (2008) *Content rating and fake detection system. http://antipaedo.lip6.fr.*

Ad essere rigorosi, la problematica dei file fake esiste anche con lo scaricamento di file da siti internet tuttavia, mentre nel caso del peer-to-peer risulta impossibile risalire alla persona che ha inviato il file, nel caso di scaricamento da siti internet il rischio è pressoché nullo dal momento che il gestore potrebbe essere facilmente identificato e la correttezza dei contenuti messi a disposizione rappresenta un forte elemento di valutazione della reputazione nel web.

Il nome del file non è dunque in alcun modo collegato al reale contenuto dello stesso, pertanto un film animato della Walt Disney potrebbe essere contenuto all'interno di un file il cui nome lascia pensare ad un brano musicale di un noto artista italiano. La scoperta del reale contenuto può avvenire solo in alcuni casi attraverso un'anteprima del file (e ciò è possibile solo per alcune tipologie di formato di dati); solitamente l'utente tende a scaricare numerosi file che danno riscontri positivi ad una ricerca per parola chiave, rimandando l'attività di verifica a momenti successivi al termine dello scaricamento.

Tale circostanza, associata al relativo comportamento dell'utente, crea rilevanti problematiche in tema di consapevolezza. Per comprendere questo fenomeno si rende efficace la seguente metafora.

ACQUISTO DI SCATOLA CON OGGETTI USATI DA UNA SVENDITA	SCARICAMENTO DI FILE DALLA RETE
il venditore scrive sulla scatola il contenuto (ad esempio, "giocattoli") e sigilla la scatola	il venditore è un utente che partecipa alla rete peer-to-peer; la scatola è il file scambiato; "giocattoli" è il nome che l'utente che cede assegna al file
il compratore che cerca giocattoli usati compra la scatola e la porta a casa	il compratore è l'utente che cerca file in rete; "giocattoli" è la parola chiave utilizzata per cercare il file di interesse; il file si chiama come lo ha chiamato chi lo ha ceduto
il compratore sarà inconsapevole di cosa ha acquistato, o meglio sarà convinto di aver acquistato giocattoli; il tutto finché non apre la scatola e guarda uno per uno gli oggetti contenuto nella scatola	l'utente che ha scaricato il file è inconsapevole finché non apre il file e non ne visiona il contenuto
il compratore potrebbe avere per anni la scatola in casa, nella cameretta dei figli così come in cantina, ma finché non apre la scatola continua ad essere inconsapevole circa il suo contenuto	il file può rimanere nella cartella dei file scaricati, può essere copiato sul Desktop così come su un hard disk esterno destinato ad archiviazione, ma finché il file non viene aperto il problema della consapevolezza del contenuto rimane
il compratore un certo giorno potrebbe decidere di aprire la scatola, accorgendosi che non contiene "giocattoli per bambini" ma "giocattoli sessuali per adulti" (perché il venditore con il termine giocattoli intendeva far riferimento a quest'ultima categoria); oppure che la scatola contiene "barattoli di alimenti ormai scaduti" (il venditore si era sbagliato a nominare la scatola o	l'utente che aveva scaricato il file scopre che il file "sesso.avi" non contiene scene di sesso tra adulti ma tra minori; oppure il file denominato "Biancaneve e i sette nani.avi" non è un cartone animato ma un file pedopornografico; oppure il file "Vasco Rossi – discografia.zip" non è un album musicale, ma ancora un file pedopornografico ribattezzato in maniera differente; oppure, il file

voleva prendere in giro i compratori)	"Agenzia entrate.pdf" non è un documento relativo all'agenzia delle entrate ma un file a contenuto pedopornografico
se il compratore risulta comunque interessato al contenuto può decidere di trattenere la scatola, **questa volta (e solo da questo momento) conscio del contenuto**; sui vari oggetti la presenza delle sue impronte digitali saranno a dimostrare che ha avuto occasione di verificarne il contenuto.	se l'utente conserva il file allora si può considerare consapevole; se il file è stato visionato avrà data di ultima lettura successivo alla data di scaricamento, oltre a numerosi altri elementi che verranno poi illustrati

Anche prima di completare lo scaricamento, addirittura prima ancora di avviarlo, sarebbe possibile utilizzare degli strumenti disponibili in rete per cercare di capire il reale contenuto dei file. Il sito *http://peerates.net* consente di eseguire una verifica (check) di hash: digitando un hash da verificare, ottenuto ad esempio dall'utente a seguito di una ricerca, è possibile verificare l'elenco dei file presenti nella rete caratterizzati dallo stesso identificativo, verificando la distribuzione geografica e il nome utilizzato da altri utenti all'interno delle rete.

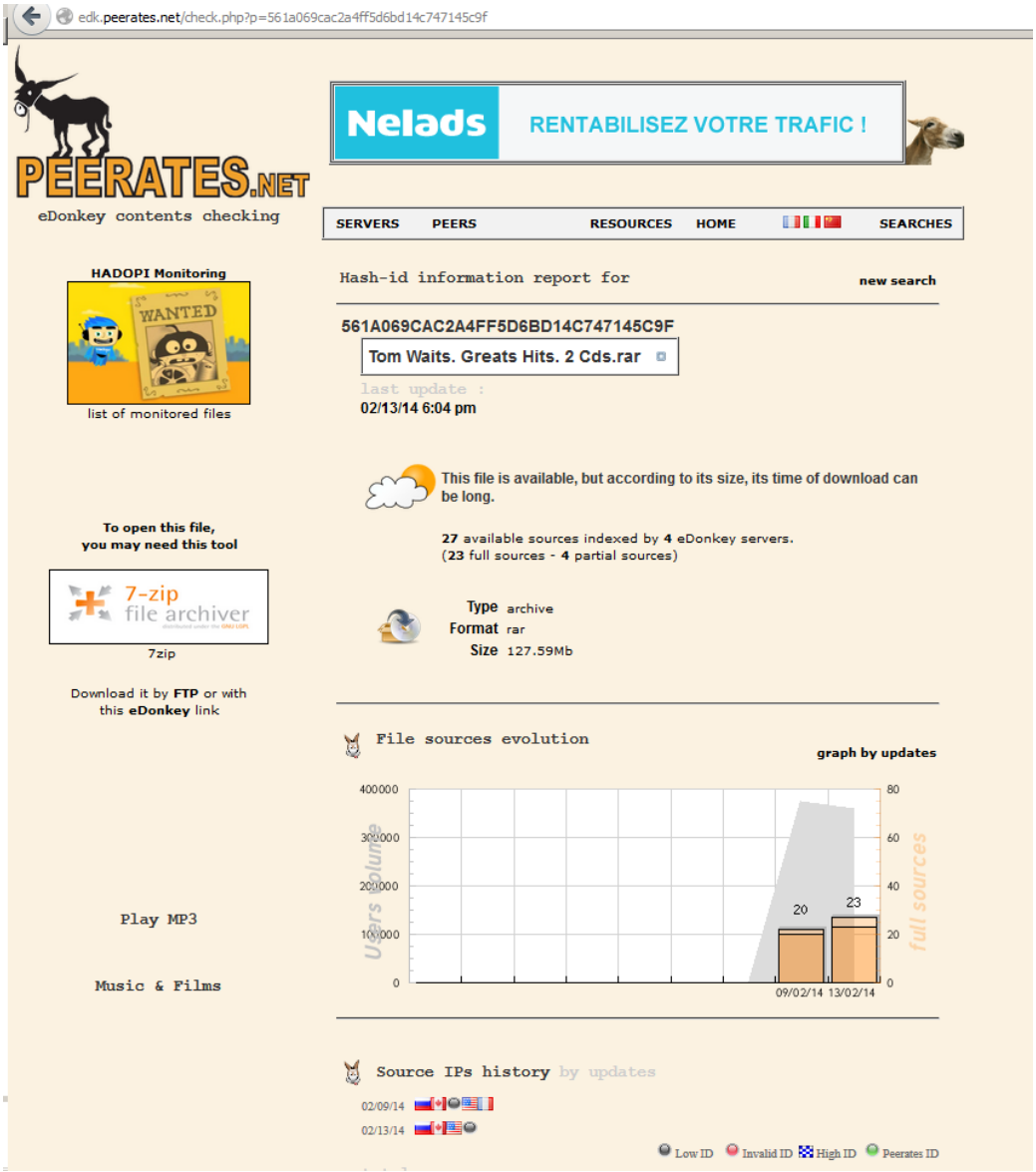


Figura 36 – Funzione di check di hash del sito *http://peerates.net*

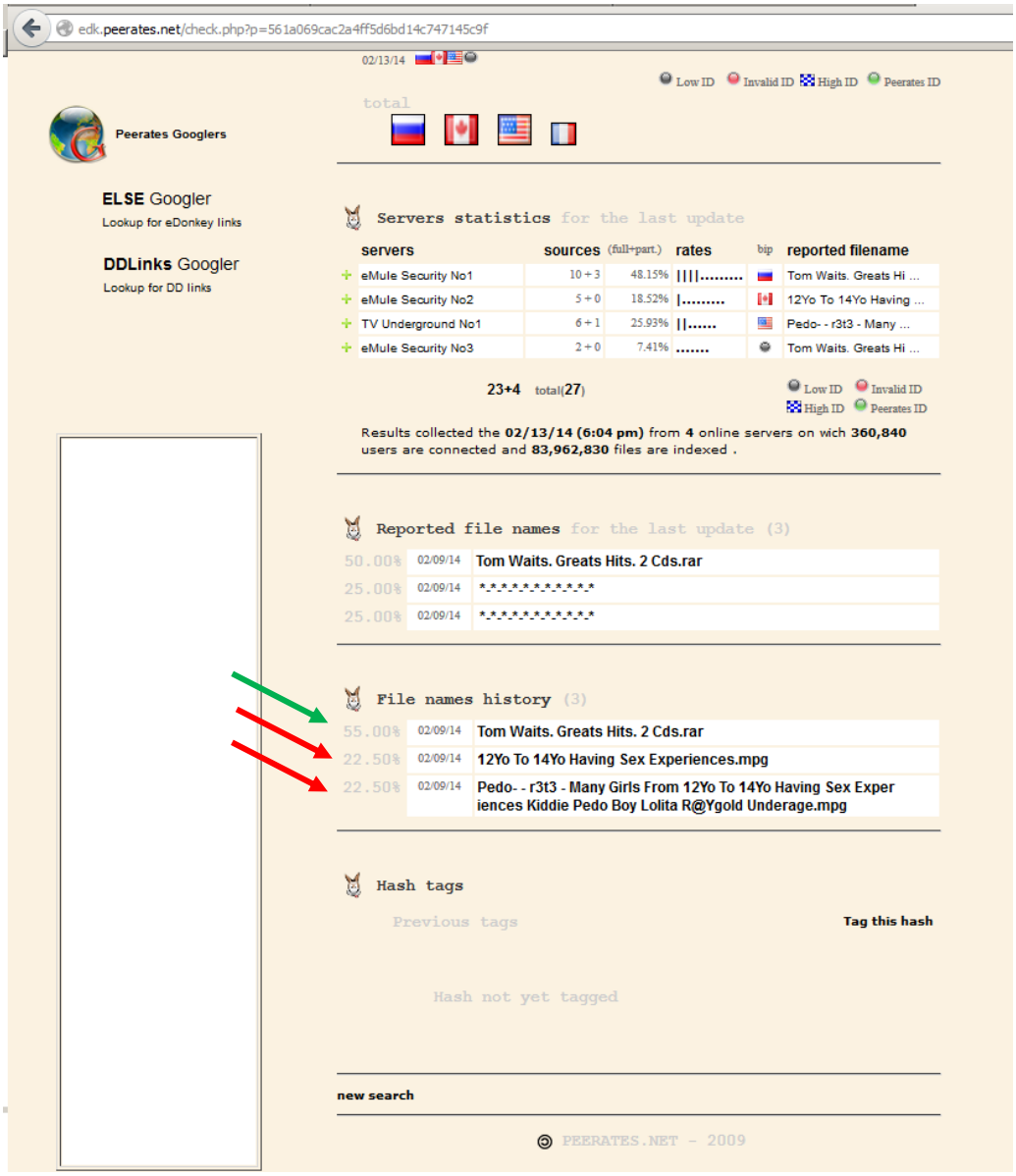


Figura 37 – Funzione di check di hash del sito *http://peerates.net*. La freccia verde indica un file con nome non riconducibile a pedopornografia, la freccia rossa a nomi riconducibili a pedopornografia

Nell'esempio mostrato nelle figure precedenti si nota come il file sia stato individuato in quattro esemplari, due dei quali rimandano ad una raccolta di due CD musicali, mentre altri due a video a contenuto pedopornografico (*12yo*, *14yo*, *pedo*, *lolita*, *r@ygold* e altre sono tipiche parole chiave che identificano questo genere di materiale).

Per verificare la consapevolezza occorre quindi effettuare una serie di verifiche dove la presenza di file a contenuto pedopornografico è solamente il

punto di partenza – e non di arrivo come accade in numerose indagini – che deve trovare numerosi elementi di riscontri in dati (file recenti, date di ultima lettura…) e in comportamenti (competenze dell'utilizzatore, metodologia di archiviazione dei dati…).

CAPITOLO 5

5. Analisi forense di reperti informatici per il reato di pedopornografia: una proposta metodologica

In questo capitolo si analizzano le peculiarità da un punto di vista tecnico dei software di file sharing su rete peer-to-peer, allo scopo di mettere in evidenza gli artefatti forensi utili nell'ambito di un accertamento tecnico. Tali elementi, unitamente alle caratteristiche dei sistemi operativi e tenuto conto dei punti rilevanti contenuti all'interno delle norme in materia ai fini di un'analisi, vengono presi in considerazione per definire una proposta di metodologia operativa che consente di analizzare in maniera precisa, dettagliata ed esaustiva un supporto informatico coinvolto in un reato di pedopornografia.

La metodologia proposta non si preoccupa del solo rinvenimento di file a contenuto pedopornografico – come purtroppo molto spesso accade di vedere nelle consulenze tecniche e nelle perizie – ma si propone di individuare tutte le tracce che consentono di verificare l'effettiva consapevolezza riguardo il possesso, così come definito dall'art. 600-quater c.p. e negli articoli di codice penale di molti altri paesi. Inoltre, altro aspetto che molto spesso viene tralasciato e dato per scontato è relativo alla relazione tra l'indagato e il bene informatico, atteso che l'associazione tra indirizzo IP, utenza telefonica e bene informatico non necessariamente trova come minimo comun denominatore l'intestatario dell'utenza telefonica che si ritrova ad essere l'unico indagato[273].

[273] Le prime considerazioni e i primi risultati su questo lavoro sono stati presentati dallo scrivente in Ferrazzano M. (2011) Reati di pedopornografia in ambiente eMule: analisi dei log per ricostruire attività di scambio tra vari utenti indagati. *In:* Attanasio A., Costabile G., eds. *IISFA Memberbook 2010*. Experta. 49–69; Ferrazzano M., Maioli C. (2011) Control of File Exchange of Illicit Materials in Peer-to-Peer Environments. In *Proceedings of the 4th International Conference on Information Law*, Thessalonica, 2011. 154–165; Ferrazzano M. (2014) Disk forensics analysis of file sharing client in peer-to-peer environments. In Boscarato C., Caroleo F., Santosuosso A., eds. *Law&Science Young Scholars Informal Symposium - 2013 Round*. Pavia University Press [in corso di pubblicazione]. Riferimenti alle modalità di analisi di sistemi informatici coinvolti nel file sharing a mezzo peer-to-peer e al software emuleforensics sono presenti in Costabile G. (2011) Peer-to-peer e digital forensics: il caso Emule. In: Aterno S., Cajani F., Costabile G., Mattiucci M., Mazzaraco G. (2011) *Computer*

5.1. Ricerca di evidenze relative alla pedopornografia

Di seguito si propongono le metodologie di analisi forense finalizzate ad individuare materiale di tipo pedopornografico all'interno di un sistema informatico.

Innanzitutto c'è da precisare che questo tipo di ricerca prescinde dal presupposto che l'utente abbia fatto uso di software peer-to-peer perché la detenzione di materiale informatico di qualsiasi genere non è legata in modo univoco alle operazione di file sharing: i file possono infatti arrivare su un computer in modi diversi:

- tramite attività di file sharing;
- navigando su siti web;
- condividendo un qualche file server online o in rete locale in una cartella condivisa;
- tramite moduli di software di chat che permettono l'invio di file;
- per posta elettronica;
- più semplicemente, senza partecipare ad una rete e copiando i dati contenuti in un device collegato al computer.

Fatta questa premessa, la ricerca di un certo tipo di dato può poi risultare più o meno rapida in base alle informazioni disponibili riguardo al canale di approvvigionamento del materiale.

5.1.1. Ricerca non automatizzata

Questa prima metodologia di ricerca di file a contenuto pedopornografico, molto semplice da un punto vista tecnico ma più lunga[274] e più precisa rispetto alle altre due presentate, si compone di due fasi:

forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici. Experta. 137–150 e in Grillo A. (2012) Indagini digitali mediante strumenti Open Source e Freeware. *In:* Carretta P., Cilli A., Iacoviello A., Grillo A., Trocchi F. *L'acquisizione del documento informatico. Indagini penali e amministrative*. LaurusRobuffo. 107–202.

[274] La presenza di un numero particolarmente elevato di immagini e video è oggi una situazione estremamente frequente in considerazione del fatto che molte persone hanno una fotocamera digitale, spesso integrata nello smartphone. Inoltre, l'analisi di un sistema informatico di tipo tradizionale come un personal computer o un notebook presenta un elevato numero di file immagine che vengono automaticamente scaricate dal browser ogni volta che si consulta una pagina web che li contiene.

1. recupero di tutti i file atti a contenere materiale multimediale (video, immagini, documenti, archivi compressi…) mediante tecniche di carving;
2. visualizzazione dei file e classificazione del contenuto.

Questo genere di ricerca può rivelarsi efficace e compiuta in tempi ragionevoli quando i sistemi da analizzare sono nell'ordine di qualche unità e, comunque, il numero di immagini, video e archivi è limitato. Inoltre, l'attività di visualizzazione di immagini può essere affidata ad un qualsiasi soggetto, anche privo di competenze tecniche, purché in grado di distinguere tra soggetti minori e soggetti maggiorenni: il candidato ideale sarebbe un professionista con competenze più mediche che informatiche, il quale certamente sarà in grado di ridurre al minimo il numero di situazioni dubbie[275]. Nella realtà quotidiana, il professionista che si occupa di questa classificazione è una persona priva di competenze mediche pertanto è opportuno che non si avventuri in una "classificazione a tutti i costi", cercando di evidenziare solo i file con contenuto certamente pedopornografico e individuando i file che invece potrebbero esserlo.

5.1.2. Ricerca mediante tecniche di image detection

Questa seconda metodologia è la più complessa, non richiede particolari competenze da parte di chi conduce l'indagine a patto che la complessità sia scaricata sul software di analisi. La metodologia prevede che sia il software, e non l'utente umano, a "visionare" i filmati, cercando apportuni pattern[276] all'interno di immagini e video che siano riconducibili alla pedopornografia.

A differenza del caso precedente questa metodologia richiede pochissime ore-uomo: l'utente umano infatti ha solo il compito di avviare la ricerca ed osservare a posteriori gli esiti, verificando quali tra i risultati siano effettivamente positivi e scartando i falsi positivi, ovvero immagini ritenute di pedopornografia che invece tali non sono. Nulla può l'utente per recuperare i falsi negativi, ovvero immagini pedopornografiche non individuate, la cui unica

[275] Si pensi al caso di fotografie con soggetti con età difficilmente identificabile o ai soggetti con tratti somatici asiatici che tendono ad apparire più giovani dell'età reale.

[276] Con il termine pattern si intende un disegno, un modello, uno schema che consente di classificare gli oggetti all'interno di un'immagine o di un video. Sul punto cfr. Stahl A., Ulges A. (2011) Automatic detection of child pornography using color visual words. In *Proceedings of the 2011 IEEE International Conference on Multimedia and Expo, ICME '11, IEEE Computer Society*, 1–6.

via di recupero è la visualizzazione manuale secondo quanto illustrato nel paragrafo precedente.

5.1.3. Ricerca per hash

Una terza metodologia, che richiede un'attività di addestramento del software, fa leva sul fatto che i file a contenuto pedopornografico che girano in rete sono spesso i medesimi e normalmente non subiscono alcuna alterazione nel passaggio da un sistema informatico ad un altro. Pertanto, disponendo di un archivio di hash rappresentativi dei file è possibile calcolare l'hash di tutti i file presenti su un supporto e confrontare il valore così ottenuto con i dati presenti nel database.

A differenza della metodologia precedente, il numero di falsi positivi è nullo se il database di hash è correttamente costruito, mentre il numero di falsi negativi è dipendente dal numero di file ignoti al database.

5.2. I principali software di file sharing su reti peer-to-peer e aspetti rilevanti ai fini delle indagini forensi

5.2.1. BearShare

BearShare è un software per Windows basato sul protocollo Gnutella che permette di condividere file in maniera distribuita, in particolare file multimediali audio e video. Una caratteristica che non ne ha permesso un particolare successo è l'impossibilità di mettere in condivisione i file in scaricamento.

Di default, il programma è installato nella directory `C:/Program Files/BearShare/Applications/BearShare`. A livello di registro, il percorso di installazione dell'applicazione è indicato nella chiave `HKEY CURRENT USER/Software/BearShare/General/Home`.

I principali elementi utili per un'analisi forense di questo client sono:

- il file `ContentDirs.db`, contente i dati relativi alle cartelle condivise;
- il file `ContentFile.db`, contenente i dati relativi al timestamp dei download effettuati;
- il file shistory.im, contentente le parole chiave utilizzate per le ricerche;

- la cartella `C:/Documents and Settings/[USER]/Application Data/ BearSharenPartials`, contente i file in scaricamento;
- la chiave di registro `HKEY CURRENT USER/Software/BearShare/ General/Login`, contenente i dati sui recenti log in;
- la chiave di registro `HKEY CURRENT USER/Software/BearShare/ Preferences/Invite/DownloadCount`, contenente i dati relativi ai download effettuati.

5.2.2. BitTorrent

Un client BitTorrent si occupa di accedere all'omonima rete ed effettuare il download/upload da e verso tutti i nodi ad esso collegati: uno degli applicativi client si chiama proprio con lo stesso nome del protocollo[277].

Dal punto di vista forense, BitTorrent e installato di default nella cartella `C:/Programmi/BitTorrent`. A livello di registro, il percorso di installazione dell'applicazione e indicato nella chiave `HKEY CURRENT USER/Software/ Microsoft/Windows/CurrentVersion/AppPaths/bittorent.exe`.

A differenza di altri software di file sharing, BitTorrent non ha una cartella specifica contenente i file condivisi perchè il meccanismo di scambio e basato sulla creazione di un file con estensione .torrent che può essere messo a disposizione su un server (definito tracker) dal quale gli utenti interessati si rivolgono in un primo momento per poi contattare il possessore e procedere effettivamente allo scaricamento.

Nella directory `C:/Documenti/[USER]/Application Data/BitTorrent` è possibile trovare diversi file .dat, tra i quali risultano particolarmente interessante per fini forensi `resume.dat`, che contiene i dati sui file scaricati e sui seed[278], e `settings.dat`, che contiene dati sulla configurazione del programma[279].

[277] *http://www.bittorrent.com*

[278] Gli utenti che in BitTorrent condividono file sono chiamati seed, quando il file messo in condivisione è completamente disponibile e si dispone di tutte le sue parti (100%), oppure peers, quando il file non è completamente scaricato (ad esempio al 60%) ma le parti già ottenute sono rese disponibile agli altri utenti.

[279] Colella A., Ghirardini A., Ianulardo M. (2009) Reati di pedopornografia in ambiente P2P. Simulazione tecnica per definire i concetti di detenzione, cessione e diffusione. *In:* Attanasio A., Costabile G., eds. *IISFA Memberbook 2009*. Experta. 49–98.

5.2.3. KaZaA

KaZaA è un software per Windows basato sul protocollo FastTrack; ne esiste una versione open source chiamata giFT[280] che opera in modo analogo e garantisce maggiori prestazioni e migliore stabilità. KaZaA favorisce gli utenti che hanno un elevato livello di partecipazione, sia inteso come file condivisi che come bandwidth disponibile.

Di default, la cartella di installazione `C:/Program Files/Kazaa` e i file condivisi e in scaricamento sono salvati nella sottocartella `My Shared Folder`. A livello di registro, questa informazione è presente nella chiave `HKEY LOCAL MACHINE/Software/Kazaa/LocalContent/DownloadDir`. Qualora fossero utilizzate ulteriori cartelle condivise, i pathname possono essere trovati nella chiave di registro `HKEY CURRENT USER/Software/Kazaa/LocalContent`. In essa i file (condivisi in fase di download) vengono temporaneamente rinominati in `downloadxxxxxxxxxxxxxxxx.dat`, dove le prime dieci cifre successive alla parola "download" rappresentano il timestamp in formato Unix[281] relativamente a data e ora di inizio dello scaricamento.

Le ricerche possono essere condotte in due modalità e in entrambi i casi vengono lasciate tracce sul computer in uso:

- nella chiave `HKEY CURRENT USER/Software/Kazaa/Search` sono rinvenibili le keyword utilizzate dall'utente per una ricerca standard.
- nella cartella `C:/Program Files/Kazaa/My Search Agents` sono rinvenibili diversi file in formato `.ksa`[282], uno per ogni ricerca

[280] *http://developer.berlios.de/projects/gift-fasttrack/*

[281] Lo Unix timestamp è un contatore del tempo come totale parziale di secondi trascorsi dall'Unix Epoch (1 gennaio 1970 ore 0:00 UTC). Pertanto, il timestamp unix è il numero di secondi trascorsi da una data all'Unix Epoch.

[282] I file con estensione `.ksa` sono salvati dal software di file sharing KaZaA quando viene realizzata una ricerca utilizzando un search agent, ovvero uno strumento software atto a ricercare materiale sulla rete. La struttura del file rispetta la seguente sintassi:

```
<! ELEMENT KMDKSA (CATEGORY, KEYWORDS, CRITERIA?)>
<! ELEMENT CATEGORY (#PCDATA)>
<! ELEMENT KEYWORDS (#PCDATA)>
<! ELEMENT CRITERIA (#PCDATA)>
```

Nel tag *category* è contenuto il tipo di file ricercato, ad esempio "All" (cioè qualsiasi tipologia di file) piuttosto che "Image" o "Video" (qualora siano ricercate immagini o video). Nel tag *keywords* sono contenute le parole chiave utilizzate per la ricerca. Nel tag *criteria* sono salvati eventuali informazioni aggiuntive (non necessarie) come titolo, autore, album, dimensione.

Un esempio di file `.ksa` può dunque essere il seguente:

condotta utilizzando l'agente di ricerca.[283] A livello di registro, questa cartella e indicata nella chiave `HKEY CURRENT USER/Software/Kazaa/LocalContent/SearchAgents`.

KaZaA dispone altresì di un browser integrato nell'applicazione stessa, le cui informazioni relative agli ultimi URL visitati sono visibili nella chiave di registro `HKEY CURRENT USER/Software/Kazaa/Kazaa/BrowserSettings`.

5.2.4. Lphant

Lphant permette la connessione alla rete eDonkey, BitTorrent e, dalla versione 3.50, Kademlia, diventando di fatto un alternativa ad eMule in ragione del fatto che consente di utilizzare contemporaneamente le due reti. La possibilità di scaricare un file utilizzando i suddetti tre protocolli lo rende il primo client multiprotocollo. L'ultima versione funzionante di Lphant è la 3.51, successivamente alla quale sono risultate divulgate versioni prodotte dalla Discordia LTD, società contro la pirateria che ha di recente acquistato Lphant, che non sono – di proposito – perfettamente funzionanti e che interagiscono con server monitorati.

5.2.5. Emule

Il client peer-to-peer più noto e diffuso soprattutto in alcuni paesi, tra cui l'Italia e il Brasile, è eMule[284]: si tratta di un programma open-source il cui programma di installazione, così come i sorgenti, sono disponibile nella pagina ufficiale del progetto[285]. La partecipazione all'interno della rete può avvenire utilizzando i protocolli eDonkey e Kademlia (singolarmente o insieme). Le peculiarità e le metodologie utili per condurre un'analisi forense verranno illustrate nel paragrafo seguente.

```
<KMDKSA ver="1.0">
  <CATEGORY>Video</CATEGORY>
  <KEYWORDS>Pinocchio</KEYWORDS>
</KMDKSA>
```

[283] L'agente di ricerca funziona in maniera simile alla ricerca standard ma continua a ripetere la ricerca per le 24 ore successive ad intervalli di 30 minuti, in modo tale da ottimizzare i risultati per via del fatto che nella rete peer-to-peer è la normalità che un nuovo utente possa fare login.

[284] *http://sourceforge.net/projects/emule*

[285] Al 15 giugno 2014, la versione disponibile è la 0.50a.

5.2.5.1. Installazione di eMule

Per comprendere correttamente il funzionamento di eMule e compiere una corretta analisi forense è importante partire dalle modalità di installazione del programma: se non diversamente indicato, eMule viene installato nella directory predefinita `C:/Programmi/eMule` nella quale vengono create varie altre cartelle ausiliarie tra cui, importanti per l'analisi forense, l'archivio dei file in condivisione (di default `C:/Programmi/eMule/incoming`) e l'archivio dei file temporanei in scaricamento (di default `C:/Programmi/eMule/temp`).[286] A livello di registro è possibile individuare la cartella di installazione nella chiave di registro `HKEY CURRENT USER/Software/eMule/Install Path`.

Quando un file è completamente scaricato viene spostato dalla cartella `temp` alla cartella `incoming` (o comunque tra le cartelle designate dall'utente ad ospitare i file temporanei e completati).

5.2.5.2. L'user ID

Emule prevede un sistema di crediti il cui scopo è incoraggiare gli utenti a condividere i propri file: più file sono condivisi e inviati ad altri client, più crediti si ricevono e quindi più velocemente si scalano le code di attesa per i download.

Il valore dei crediti maturati è conservato all'interno del file denominato `clients.met` dai singoli nodi remoti, ovvero dai nodi a cui si è inviato dei file, dove ogni utente è identificato mediante un valore a 16 byte noto come *user ID*. Lo *user ID* si presenta simile ad un digest MD4 in quanto stringa a 128 bit e viene assegnato a ciascun utente alla prima esecuzione di eMule utilizzando una funzione di concatenazione di numeri casuali, ad eccezione del sesto e quindicesimo byte, i cui valori sono sempre rispettivamente i valori esadecimali `0x0E` e `0x6F`.

Poiché il valore di *user ID* è fondamentale per la corretta gestione dei crediti, un algoritmo di identificazione che prevede un meccanismo di cifratura

[286] In alternativa, la cartella dei file condivisi può essere impostata nel profilo personale di ogni utente, per cui in C:/Documents and Settings/[USER]/My Documents/eMule Downloads/Incoming o in C:/Users/[USER]/Downloads/eMule/Incoming, a seconda il sistema operativo sia Windows XP o Windows Vista/7). Stesso discorso vale per la cartella dei file temporanei.

con chiavi pubbliche e private RSA viene utilizzato al fine di evitare che un utente si spacci per un altro utilizzandone così il vantaggio accumulato[287].

5.2.5.3. Il file ID

Ogni file disponibile nella rete è caratterizzato univocamente da un identificato detto *file ID* calcolato mediante l'algoritmo di hash MD4[288] specifico di eDonkey[289] dal client che ne ha disponibilità: i file di dimensione superiore a 9,28MB vengono suddivisi in una serie di parti (grandi al massimo circa 9 MB) e per ognuna di esse viene calcolato un valore hash MD4: in questo modo, una volta scaricato l'intero file, il client può verificarne la correttezza confrontando l'hash dell'intero file; qualora questo non fosse concordante può ancora effettuare una verifica sulle singole parti e, rintracciata la porzione danneggiata, procedere al download correttivo[290].

Quando il file supera i 9,28 MB, eMule procede al download nella cartella `temp` di singole parti, anche in maniera non consecutiva, che verranno poi riassemblate al termine dello scaricamento, ma immediatamente rese disponibili alla divulgazione verso i nodi che ne facessero richiesta.

È comunque importante sottolineare che l'utente che richiede il download non solo non può scegliere uno specifico nodo remoto da cui scaricare o a cui inviare un file, ma è ignaro di come funzioni, e non ha il potere di influire, il meccanismo con cui:

- si stabilisce il numero di utenti remoti da coinvolgere nello scaricamento del file;
- si selezionano gli utenti remoti da cui scaricare il file;
- si frazioni il file e in quale ordine si prelevino le varie parti;
- si pone in condivisione il file, o sue parti già scaricate;
- si accettano le richieste di invio del file da parte di altri utenti.

[287] Bickson D., Kulbak Y. (2005) *The emule protocol specification*. *Op. cit.*

[288] Dettagli sull'algoritmo MD4 e sua implementazione sono disponibili all'indirizzo *http://www.ietf.org/rfc/rfc1320.txt*.

[289] Per calcolare il digest di un file utilizzando lo stesso algoritmo impiegato da eDonkey è possibile utilizzare l'applicazione HashCalc disponibile all'url *http://www.slavasoft.com/hashcalc/*.

[290] Lange R., Ghedini Ralha C. (2011) Identificação de Artefatos Periciais do eMule. In *Proceedings of the Sixth International Conference on Forensic Computer Science*. 44–53.

Può tuttavia verificarsi la circostanza per la quale due o più utenti si accordino in modo tale da utilizzare la rete eDonkey con un server privato con il quale condividere solo file di una certa tipologia.

5.2.5.4. File di eMule

Oltre ai file oggetto di condivisione, l'analisi forense su un sistema che utilizza eMule richiede la valutazione anche di una serie di file salvati nella cartella `config` che vengono gestiti dal software di file sharing per il corretto funzionamento dello stesso.

Tra essi, l'unico file in formato testuale è denominato `AC_SearchString.dat` e contiene la lista delle ultime keyword utilizzate per cercare file utilizzando il motore di ricerca interno al software[291].

Gli altri file (in formato binario) utili per un'indagine sono:

- `emfriends.met`, che contiene la lista degli amici con cui si sono svolte conversazioni di chat: eMule dispone infatti anche di un modulo per conversare con altri utenti, ma delle conversazioni non viene mantenuta traccia;
- `known.met`, che contiene la lista dei file posti in condivisione, scaricati e in scaricamento;
- `client.met`, che contiene la lista degli altri utenti con i quali si e condiviso un file (in download o in upload).
- `preferences.dat`, che contiene l'user ID dell'utente.

5.3. Prodotti commerciali esistenti per l'analisi forense del peer-to-peer

Sebbene le indagini che richiedano l'analisi di software di file sharing su reti peer-to-peer siano frequenti, il panorama della computer forensics è estremamente carente in fatto di strumenti software per l'analisi dell'attività di file sharing. Nel caso della pedopornografia in particolare le indagini e le analisi forensi spesso si concludono con la sola – ed insufficiente – verifica

[291] La ricerca di file utilizzando il protocollo eDonkey e realizzabile sia utilizzando il motore di ricerca del software eMule che utilizzando appositi motori di ricerca presenti su pagine web: in tal caso viene fornito un link del tipo `ed2k://|file|DivX-Pinocchio.avi|733947904|09C6A943B3D613351343C4AAA`; il clic permette all'utente di aggiungere il file desiderato nella lista dei file in scaricamento.

della presenza di tracce di file ritraenti minori in atteggiamenti sessuali su un sistema informatico in uso all'indagato o all'imputato. Come definito all'inizio del capitolo, tale ricerca si può compiere anche in maniera manuale e senza la necessità di un particolare software di analisi forense.

Tuttavia, stante la dimensione del fenomeno e la necessità di ricostruire le relazioni tra più indagati in uno stesso procedimento, diventa indispensabile un software che sia di ausilio al consulente tecnico o alla polizia giudiziaria per la rapida analisi delle attività poste in essere sul peer-to-peer. Infatti senza strumenti automatizzati il lavoro di un investigatore forense per trovare le prove di attività illecite compiute mediante software di file sharing richiede molto tempo ed è meno efficace.

P2PMarshal è un tool per Windows realizzato dall'Architecture Technology Corporation[292] che permette l'analisi automatica di client di file sharing su reti peer-to-peer. Il software (gratuito per il personale delle forze dell'ordine degli Stati Uniti, del costo di 995$ per gli altri utenti) permette di analizzare l'uso di software di peer-to-peer Ares, BitTorrent, FrostWire, LimeWire, uTorrent, Azureus Vuze ed eMule su copie forensi di sistemi Windows (dalla versione XP a 8).

Secondo il produttore, P2P Marshal segue le best practices della computer forensics e mantiene un log dettagliato delle attività svolte. Permette inoltre di fare ricerche, mostrare anteprime dei file e produrre report in diversi formati (CSV, HTML, PDF e RTF).

Il software è disponibile in due versioni:

- P2P Marshal Forensic Edition che consente di installare ed analizzare immagini forensi mediante una workstation forense;
- P2P Marshal Field Edition che è avviabile da chiavetta, senza necessità di installazione, anche direttamente sul sistema oggetto di indagine.

Internet Evidence Finder (noto anche con il suo acronimo IEF) è un software della Magnet Forensics[293] (la cui licenza ha un costo di circa 1000 $) che consente di operare analisi sui dati generati su un sistema durante attività in rete che coinvolgono browser, social network, chat, software di file sharing.

[292] *http://www.atc-nycorp.com/*

[293] *http://www.magnetforensics.com/*.

5.4. Link analysis in analisi forensi riguardanti il peer-to-peer

Il data mining e il processo di elaborazione e analisi automatico di un'ampia mole di dati al fine di scoprire modelli o regole significativi[294]. Con il termine massive forensics si intende indicare non solo la mole di dati, ma in generale l'analisi forense di una grossa quantità di reperti informatici.

Varie ricerche hanno portato allo sviluppo di diverse tecniche di data mining per analisi di informatica forense e, più in generale, di applicazioni destinate ad usi forensi[295]; principalmente si tratta di classificare, raggruppare per affinità i dati presenti nei dischi e creare relazioni. Tra queste si citano:

- estrazioni di entità, ovvero l'identificazione di particolari pattern (testo, immagini, audio) che possono essere utilizzati per identificare persone (o loro caratteristiche), indirizzi, veicoli… ; ad esempio nella computer forensics l'estrazione di codici di software permette all'investigatore digitale di raggruppare programmi simili scritti dagli hacker per poi scoprire comportamenti malevoli analoghi presenti in altri sorgenti;
- associazioni di regole o di sequenze di pattern, ovvero di comportamenti operati da criminali nel compimento di certe azioni; un esempio classico e la registrazione delle modalità con cui si verifica un attacco informatico utilizzando la rete;
- classificazione, che permette di associare proprietà comuni a diversi crimini, organizzarli in classi e definire delle relazioni tra essi;
- comparazione testuale, una tecnica che permette di confrontare dei campi di un database e trovare similitudini tra essi; bisogna però ottimizzare questa tecnica che altrimenti rischia di avere dei tempi di computazione molto elevati;
- analisi di social network, una tecnica che descrive regole e interazioni di nodi in una rete sociale virtuale.

Nel caso di indagini che coinvolgono lo scambio di materiale illecito su reti peer-to-peer è possibile far leva su alcuni elementi caratterizzanti dei file e degli utenti al fine di ricostruire a posteriori dei grafi orientati che ripercorrono gli scambi di file. Nella rete eDonkey, atteso che i file sono identificati da un file

[294] Berry M, Linoff G.(2002) *Data mining. L'azienda intelligente e la gestione strategica delle informazioni*. Apogeo.

[295] Chau M., Chen H., Chung W., Qin Y., Xu J., Wang G. (2004) Crime data mining: a general framework and some examples. In *IEEE Computer society*, 37(4), 50–56.

ID e gli utenti da un user ID, non viene memorizzato in alcun file quale sia il file inviato da un utente A ad un utente B. Tuttavia, sfruttando le proprietà degli insiemi è possibile disegnare un grafo orientato che tenti di ricostruire gli scambi avvenuti. Ciò dunque per chiarire sin da subito che sarà impossibile provare l'avvenuto invio di file a contenuto illecito utilizzando una rete peer-to-peer analizzando i sistemi informatici di un singolo utente.

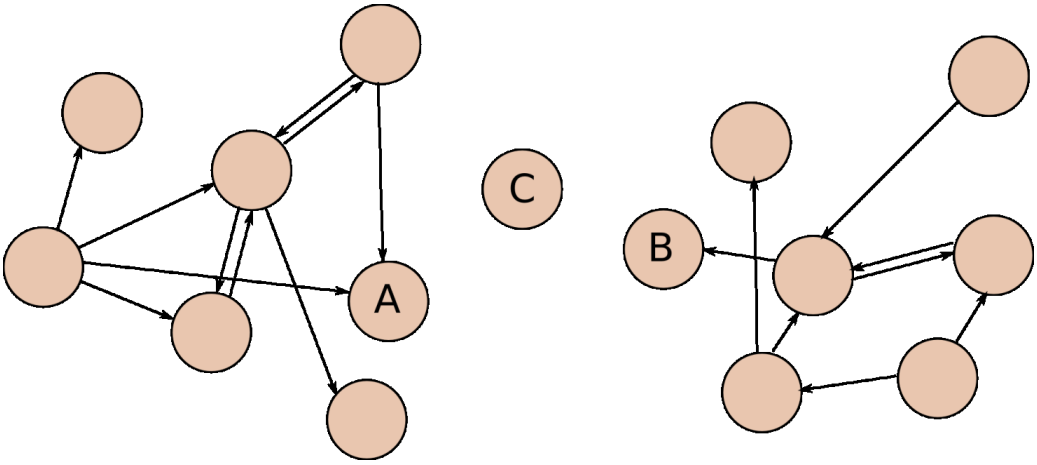


Figura 38 - Esempio n.1 di connessioni tra utenti

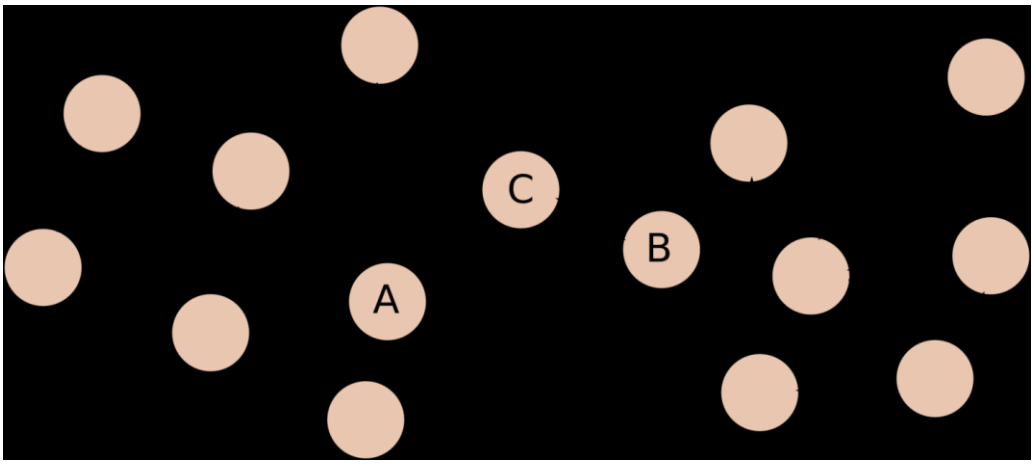


Figura 39 - Esempio n. 2 di connessioni tra utenti

Posto che per entrambe le immagini si tratti di grafo orientato bidirezionale che rappresenta le relazioni tra chi utente che invia e utente che scarica, i cerchi rappresentano i nodi della rete e le frecce gli invii di file; la freccia indica il senso della condivisione, per cui nel caso A → C si è verificato che l'utente C ha scaricato un file dall'utente A (ovvero, che A ha inviato un file a C).

Per spiegare come può mutare l'interpretazione della scena criminis si considerino le immagini precedenti:

- nella prima figura non si dispone dei dati del nodo C, ovvero C non è stato coinvolto nell'indagine oppure non sono stati recuperati i dati di traffico di eMule. C risulta isolato e non coinvolto nell'attività di condivisione. L'esclusione di C potrebbe avere anche effetti sui rapporti tra gli altri nodi;
- nella seconda figura si dispone dei dati di C e si verifica che C ha partecipato attivamente allo scambio, inviando file agli utenti A e B e ricevendo dati da S. Si riscontra come la parte di grafo a destra ha subito l'influenza della parte di grafo a sinistra che, per tramite di C, potrebbe aver immesso in circolo altro materiale.

Se C fosse un nodo particolarmente attivo nello scambio, l'assenza di C potrebbe portare ad un notevole partizionamento della rete, non riuscendo ad identificare il principale distributore di materiale. Una singola componente può dunque incidere, positivamente o negativamente, anche su altre.

Un'analisi forense di massa quindi richiede strumenti software idonei da impiegare per l'analisi dei reperti informatici ed attenzione in fase di identificazione, per evitare di lasciare fuori dall'analisi alcuni reperti informatici indispensabili per la corretta ricostruzione del grafo delle relazioni.

5.5. eMuleForensic: un nuovo strumento

Per sopperire all'assenza di strumenti specifici per l'analisi di eMule, parzialmente disponibili solo in prodotti commerciali, il lavoro di ricerca si propone di progettare e sviluppare un software, battezzato eMuleForensic, che preso atto delle esigenze e delle caratteristiche del software di file sharing e delle esigenze di analisi intende candidarsi a strumento di riferimento per analisi di questo tipo.

Tale software è una parte della proposta complessiva di protocollo operativo che verrà fornita al termine.

5.5.1. Specifica dei requisiti

5.5.1.1. Funzionalità del prodotto

L'obiettivo principale del software è l'estrazione di informazioni relativamente ai file condivisi, scaricati ed inviati ad altri utenti utilizzando il software di peer-to-peer eMule.

Tali informazioni sono presenti nei file di configurazione del software eMule installato su un sistema informatico, pertanto il programma dovrà operare dopo aver recuperato tutte le suddette informazioni disco per disco. Il recupero dei file prescinde dal software stesso in quanto l'attività di estrazione può essere compiuta sia direttamente dai dischi (opportunamente protetti in scrittura con un write blocker), sia da immagini forensi (prodotte con dd, EnCase…) nonché da un'immagine non forense (ad esempio, prodotta con software tipo Ghost o TrueImage).

Una volta ricavati tutti i file di configurazione, l'analisi e il successivo incrocio (nei casi di analisi che coinvolgono più sistemi appartenenti a soggetti diversi) deve risultare particolare semplice e veloce.

Deve essere possibile definire una timeline di possesso dei file a contenuto pedopornografico al fine di individuare per ogni coppia di utenti il primo che ne è entrato in possesso; per quanto possibile, nella coppia di utenti si dovrebbe identificare chi ha inviato e chi ha ricevuto[296].

Aspetto fondamentale è poter identificare i file oggetto di scambio o comunque messi in condivisione, potendo stabilire se i file sono stati scaricati dalla rete o forniti dall'utente (ad esempio in quanto autoprodotti).

Un requisito auspicabile è la classificazione dei file automatica, potendo definire la natura del file senza necessità di visualizzazione da parte dell'operatore forense.

5.5.1.2. Tipologia di utenti

L'utente tipo del software è un consulente tecnico o perito informatico, dunque una figura con elevate competenze tecniche.

Altra tipologia di utente è un'agente di forze dell'ordine: in questo caso il livello di competenze atteso può essere estremamente variabile.

[296] A tal proposito si precisa che eMule non mantiene dei log molto dettagliati, pertanto bisogna prestare attenzione a non giungere ad una conclusione non supportate in maniera esplicita da dati relativi alle attività realmente verificatesi: le informazioni presenti nei file di configurazione sono di tipo aggregato, per cui in riferimento ad ogni utente remoto si hanno dati complessivi di upload e download, senza alcuna indicazione riguardo ai file effettivamente condivisi. Per maggior precisione si evidenzia che tale valore aggregato non permette neppure di capire quanti sono i file inviati e scaricati, pertanto l'unico modo per poter affermare con assoluta certezza l'attività compiuta prevede una situazione in cui due utenti abbiano solo un file in comune.

Oltre agli operatori forensi, il software potrebbe essere utilizzare da altre tipologie di utenti intenzionati a verificare le attività poste in essere con il software di file sharing: si pensi ad esempio ad un amministratore di sistema.

5.5.1.3. Vincoli e requisiti

Nessun vincolo implementativo è stato individuato.

Tenendo presente che l'utente tipo del programma dispone di elevate competenze tecniche, si può scegliere qualsiasi linguaggio di programmazione e dunque qualsiasi sistema operativo di utilizzo.

Considerato che nell'ambito dell'informatica forense sono particolarmente diffuse le distribuzioni forensi Linux, la scelta implementativa è ricaduta sul linguaggio C per sistemi Linux, producendo un'applicazione eseguibile a riga di comando. Un'ulteriore versione viene sviluppata in linguaggio Java, producendo un'applicazione completa di ambiente grafico che può essere utilizzata non solo con comandi testuali ma anche con l'utilizzo del puntatore.

Un'ulteriore versione, sottoprodotto della versione C per Linux, viene resa disponibile come servizio consultabile via web alla pagina http://www.emuleforensic.com, attraverso la quale è possibile ottenere il report in output utilizzando un qualsiasi computer connesso ad Internet, anche se non attrezzato con particolari software forensi. La versione web richiede l'upload dei file da analizzare che comunque non contengono dati sensibili: in ogni caso, al termine della computazione il dato viene immediatamente distrutto.

Requisiti funzionali:

- il sistema non deve alterare i reperti originali;
- il sistema deve essere eseguibile sia a riga di comando che mediante interfaccia grafica;
- il sistema deve essere in grado di convertire i file binari di log e di configurazione di eMule in un file XML[297];
- l'output del sistema deve essere definito da un XMLSchema[298] al fine di poter riutilizzare i dati anche in momenti futuri secondo modalità non attualmente previste; XMLSchema è l'unico linguaggio di descrizione XML che abbia già raggiunto la

[297] a scelta di utilizzare XML come formato intermedio permette di mantenere la struttura logica dei dati, facilitando un'eventuale attività di trasferimento dei dati in un DBMS.

[298] XMLSchema, come la DTD, è un linguaggio di descrizione del contenuto di un documento XML.

validazione ufficiale del W3C; definendo la struttura dell'output con XMLSchema risulterà più facile in futuro aggiungere ulteriori moduli che consentano di aumentare le funzionalità del programma relativamente all'elaborazione dei vari file di output; inoltre lo stesso XML può essere facilmente modificato con una trasformazione XSLT (ad esempio per essere stampato su carta in un formato più leggibile);

- il sistema deve permettere di verificare se i file sono stati scaricati o se sono stati immessi dall'utilizzatore;
- il sistema deve permettere di verificare se c'è stata attività di download di file, anche se questi fossero stati spostati o cancellati;
- il sistema deve permettere di verificare se c'è stata attività di upload di file, anche se questi fossero stati spostati o cancellati;
- il sistema deve permettere di classificare i file senza necessità di visualizzarli, comparando l'hash con un database di hash già disponibile; il sistema deve altresì consentire di incrementare il database degli hash noti;
- il sistema deve permettere di verificare i rapporti di scambio tra più sistemi coinvolti, rappresentando anche graficamente gli scambi avvenuti.
- il sistema deve produrre dei report delle attività svolte.

Requisiti non funzionali:

- il sistema deve essere semplice da apprendere e da ricordare;
- il sistema deve portare a termine la computazione nell'ordine di qualche secondo;
- il sistema deve richiede la minima interazione possibile;
- il sistema non deve richiedere particolari risorse computazionali;
- il sistema deve essere indipendente da altri programmi in esecuzione.

5.5.2. Codifica dei file binari

Il problema principale che si riscontra analizzando i file di eMule è rappresentato dalla codifica degli stessi. Pertanto certamente l'applicazione deve prendere in input i file:

- `preferences.dat`;

- `AC SearchStrings.dat`;
- `clients.met`;
- `known.met`.

Il file preferences.dat contiene l'user ID utilizzato nella rete eDonkey per l'identificazione dell'utente. Come già rappresentato nei paragrafi precedenti, tale valore è una stringa a 128 bit simile ad un digest MD4 ma non generata mediante applicazione dell'algoritmo di hash.

Il file AC SearchStrings.dat contiene le ultime keyword utilizzate per la ricerca di file utilizzando il motore di ricerca interno al client eMule.

Il file `clients.met` contiene gli utenti con i quali c'è stata attività di condivisione, sia in upload che in download. L'utente remoto è identificato tramite l'user ID: quindi se un utente A comunica con un utente B, il valore dell'user ID contenuto nel file preferences.dat di A trova riscontro nel file `clients.met` di B e viceversa. Tale attività non è meglio definita e le uniche informazioni memorizzate sono relative alla mole di dati trasferite da uno verso l'altro e viceversa, oltre ad alcune statistiche meno significativi per i fini forensi.

Le informazioni a proposito dei file condivisi sono mantenuti all'interno di `known.met` che contiene tutti i riferimenti ad essi: nome, dimensione, hash (sia dell'intero file che dei file delle parti), data di ultima modifica, quantità di richieste di upload ricevute e quantità di richieste accettate, altre statistiche.

La definizione della struttura di tali file binari è certamente l'attività più complessa a causa di assenza di documentazione. L'interpretazione e la visualizzazione del contenuto di questi file è possibile solo con lo stesso eMule, MetMedic[299] e known.met viewer[300]:

- *eMule* è il software utilizzato per l'attività di file sharing, quindi supporta nativamente questi file; ma, poiché il suo obiettivo è la condivisione dei file, non rientra tra i suoi obiettivi disporre di una funzione per generare una reportistica, neppure basilare, relativamente ai file condivisi; l'unica strada che consente di generare documentazione stampabile su carta è la produzione di screenshot, ovvero stampe dello schermo, che però non può in alcun

[299] MetMedic è disponibile all'url *http://www.emule.it/guida_emule/files/MetMedic_Installer_v3.4.1547.41324.NSIS.zip*.
[300] known.met viewer è disponibile all'url *http://www.gaijin.at/en/dlemmetview.php*.

modo essere rielaborata o utilizzata anche per operazioni banali come la ricerca per parola chiave;

- *MetMedic* è un software che permette di correggere errori presenti in alcuni dei file binari con estensione *met*, per cui il contenuto degli stessi viene unicamente mostrato a video in una tabella, senza la possibilità di operare una conversione verso un qualche formato testuale; anche in questo caso, una banale operazione di ricerca per parola chiave non è consentita;
- *known.met viewer* è il prodotto che più si avvicina a al software che potrebbe servire all'analista perché consente di convertire in formato CSV il file `known.met`; tuttavia tale conversione è limitata proprio al solo file `known.met`, non riuscendo in tal modo a soddisfare a pieno le esigenze di analisi.

Dei tre, l'unico software che offre il codice sorgente disponibile è eMule, pertanto l'unica strada che consente di entrare in possesso di informazioni sulla struttura dei file binari di tipo *met* richiede l'analisi del codice sorgente relativamente alle definizione dei tipi di dato e alle funzioni che si occupano di gestire i vari file citati e ritenuti indispensabile per l'efficace conclusione dell'analisi forense.

Tuttavia, il software MetMedic è stato utilizzato per la sola attività di debugging allo scopo di verificare il corretto funzionamento della nuova applicazione creata.

Il file `AC_SearchStrings.dat` memorizza i dati in maniera testuale e dunque non richiede un'analisi dettagliata. Si presentano invece i dettagli degli altri file binari.

5.5.2.1. preferences.dat

Il file binario `preferences.dat` ha dimensione fissa di 61 byte. Ai fini dell'analisi forense sono interessanti solo i primi 17 byte:

- il primo byte indica la versione del file ed è il valore esadecimale `0x20`;
- i successivi 16 byte memorizzano l'user ID dell'utente utilizzatore dell'istanza di eMule presente sul reperto oggetto di indagine, un valore casuale generato dal programma di file sharing in fase di installazione.

La struttura del file è contenuta nel file sorgente `srchybrid/preferences.h` e si presenta come segue:

```
struct Preferences_Ext_Struct{
  uint8   version;
  uchar   userhash[16];
  WINDOWPLACEMENT EmuleWindowPlacement;
}
```

La struttura `WINDOWSPLACEMENTE` contiene informazioni di scarso interesse ai fini forensi.

5.5.2.2. clients.met

Il file `clients.met` mantiene traccia degli utenti con i quali almeno in una circostanza l'utente ha avuto una comunicazione, a prescindere che sia stata realizzata allo scopo di cedere e/o acquisire file. L'uso di un file del genere in eMule è giustificato dal sistema dei crediti ma per scopi forensi diventa fondamentale perché consente di ricavare gli hash degli altri utenti con cui c'è stato lo scambio di file[301] e il traffico generato in download o in upload con essi.

Poiché il numero di client noti è variabile nel tempo, anche il file stesso assume dimensioni variabili:

- il primo byte indica la versione del file (`0x0C` per i file utilizzati da versioni antecedenti la 0.29b di eMule oppure `0x0E` per le ultime versioni);
- i successivi 4 byte sono utilizzati per un intero (a 32 bit quindi) che tiene traccia del numero di client conosciuti;
- quindi, supponendo che il contatore di client noti misuri `n`, nel file sono presenti ulteriori byte di dati, tra i quali i più significati sono:
    - i primi 16 byte rappresentano l'user ID costruito come indicato nei paragrafi precedenti;

[301] L'identificazione fisica degli utenti con cui si e avuto uno scambio di file è possibile allorché si è in possesso anche dei file preferences.dat altrui. Nel caso in questione ogni utente ha avuto contatti con decina di migliaia di utenti sparsi nel mondo, ma l'attenzione si è focalizzata unicamente verso coloro i quali erano implicati nello stesso procedimento penale.

- i successivi 4 byte rappresentano la parte basse di un intero a 8 byte che contiene la quantità di dati inviati dall'utente possessore del file verso l'utente correntemente letto;
- ancora 4 byte rappresentano la parte basse di un intero a 8 byte che contiene la quantità di dati scaricati, inviati dall'utente correntemente letto verso il possessore del file;
- 4 byte rappresentano il timestamp in formato unix ed indica l'ultima occasione in cui c'è stata comunicazione tra le parti;
- due interi a 4 byte che rispettivamente rappresentano la parte alta dell'intero a 8 byte di upload e di download.

Oltre questa struttura presentata, il file ha subito un'evoluzione a partire dalla versione 0.29b di eMule: da allora e stato aggiunto un campo per il controllo dell'identità dell'utente.

Il file `client.met` ha subito una evoluzione: dalla versione 0.29b di eMule è stato esteso per consentire un maggior controllo per evitare "truffe" da parte degli utenti che si spacciavano per altri. Entrambe le strutture sono contenute nel file `srchybrid/ClientCredits.h`. Se l'intero a 8 bit vale `0x12`, la struttura di ogni client è la seguente:

```
struct CreditStruct_29a{
  uchar           abyKey[16];   //userhash
  uint32          nUploadedLo;    // uploaded to him
  uint32          nDownloadedLo;  // downloaded from him
  uint32          nLastSeen;
  uint32          nUploadedHi;    // upload high 32
  uint32          nDownloadedHi;  // download high 32
  uint16          nReserved3;
}
```

Se invece l'intero a 8 bit vale `0x12`, la struttura è la seguente:

```
struct CreditStruct{
  uchar           abyKey[16];   // userhash
  uint32          nUploadedLo;    // uploaded to him
  uint32          nDownloadedLo;  // downloaded from him
  uint32          nLastSeen;
  uint32          nUploadedHi;    // upload high 32
  uint32          nDownloadedHi;  // download high 32
  uint16          nReserved3;
```

```
  uint8           nKeySize;
  uchar           abySecureIdent[MAXPUBKEYSIZE];
}
```

dove `MAXPUBKEYSIZE` vale 80.

5.5.2.3. known.met

Il file `known.met` contiene tutte le informazioni relative ai in condivisione, scaricati da altri utenti oppure spostati/copiati nella cartella dei file condivisi di iniziativa dell'utente, e per ognuno di essi sono mantenute una grande quantità di informazioni come di seguito evidenziato.

```
<known.met>          ::= 0x0e <File details list>
<File details list>  ::= DWORD <File details>*
<File details>       ::= 0x02 <Date> <File hash> <Meta tag list>
                         [ 0x01 <B part hashes> ]
                         [ 0x01 <S part hashes> ]
<B part hashes>      ::= HASH*
<S part hashes>      ::= HASH8*
<known.v04.met>      ::= 0x0e DWORD <File details v04>*
<File details v04>   ::= <Date> <File hash> <Part hash list>
                <Meta tag list>
<Date>               ::= DWORD
<File hash>          ::= HASH    // MD4 of file
<Part hash list>     ::= WORD HASH*
<Meta tag list>      ::= DWORD <Meta tag>*
<Meta tag>           ::= 0x00 Undefined
                     ||= 0x01 <Meta tag name> HASH
                     ||= 0x02 <Meta tag name> <String>
                     ||= 0x03 <Meta tag name> DWORD
                     ||= 0x04 <Meta tag name> FLOAT
                     ||= 0x05 <Meta tag name> BOOL
                     ||= 0x06 <Meta tag name> BOOL Array
                     ||= 0x07 <Meta tag name> BLOB
<Meta tag name>      ::= WORD <Special tag>
                     ||= <String>
<Special tag>        ::= 0x01 // name
                     ||= 0x02 // size: size of file
                     ||= 0x03 // type: Audio, Video...
                     ||= 0x04 // format: file extension
                     ||= 0x05 // Collection (depricated)
                     ||= 0x06 // Part Path
                     ||= 0x07 // Part Hash
                     ||= 0x08 // copied
                     ||= 0x09 DATA   // gap start
                     ||= 0x0a DATA   // gap end
```

```
                    ||= 0x0b        // description
                    ||= 0x0c        // ping
                    ||= 0x0d        // fail
                    ||= 0x0e        // preference
                    ||= 0x0f        // port
                    ||= 0x10        // ip
                    ||= 0x11        // version
                    ||= 0x12        // tempfile
                    ||= 0x13        // priority
                    ||= 0x14        // status
                    ||= 0x15        // availability
                    ||= 0x16        // QTime
                    ||= 0x17        // Parts
                    ||= <eMule special tag>
<eMule special tag> ::= 0x20        // Compression
                    ||= 0x21        // UDP client port
                    ||= 0x22        // UDP version
                    ||= 0x23        // Source exchange
                    ||= 0x24        // Comments
                    ||= 0x25        // Extended request
                    ||= 0x26        // Compatible client
<String>            ::= <String length> DATA
<String length>     ::= WORD
DATA                  // Data of custom length
DWORD                 4 bytes integer
```

Quando è appena creato e fino a quando non ci sono file in condivisione e in download, il contenuto del file è molto elementare e comprende unicamente un byte che rappresenta la versione del file e un intero a quattro byte che indica il numero di file noti (quindi 0): il contenuto iniziale del file è quindi in rappresentazione esadecimale `0E 00 00 00 00`.

Rispetto agli altri le presi in considerazione per l'analisi forense di eMule, la struttura di `known.met` è estremamente variabile e per ogni file sono memorizzate informazioni diverse. In generale i dati più interessanti ai fini forensi sono:

- la data di fine scaricamento del file (che equivale alla data di ultima modifica memorizzata nel sistema);
- l'hash MD4 del file e di tutte i suoi file delle parti;
- il nome e la dimensione del file scaricato;
- il numero di richieste di upload ricevute;
- il numero di richieste di upload accettate (e dunque di invii).

Aprendo il file con un editor di testo si riuscirebbero a leggere solo informazioni relative a nome del file, hash e poche altre informazioni interessanti.

Figura 40 - Il file `known.met` visualizzato con un editor di testo

Per riuscire ad ottenere ulteriori informazioni occorre visualizzare il file mediante un editor esadecimale. Tuttavia ancora non sono facilmente identificabile le informazioni utili per l'analisi.

```
00000000  0e 2a 00 00 00 a6 a8 0e  4b 09 df 29 d9 e7 20 2c  |.*......K..).. ,|
00000010  ce e2 cf 39 4f 79 5c ea  fd 00 00 0a 00 00 00 02  |...9Oy\.........|
00000020  01 00 01 1c 00 50 65 61  72 6c 20 4a 61 6d 20 2d  |.....Pearl Jam -|
00000030  20 4a 75 73 74 20 42 72  65 61 74 68 65 2e 6d 70  | Just Breathe.mp|
00000040  33 03 01 00 02 4f 9e 5d  00 02 01 00 27 20 00 37  |3....O.]....' .7|
00000050  52 5a 46 36 42 47 58 33  34 4f 35 49 56 4e 43 42  |RZF6BGX34O5IVNCB|
00000060  4b 32 58 45 4f 43 47 44  58 4e 54 4a 4d 58 45 03  |K2XEOCGDXNTJMXE.|
00000070  01 00 34 4b d2 39 4b 03  01 00 50 00 d0 02 00 03  |..4K.9K...P.....|
00000080  01 00 54 00 00 00 00 03  01 00 51 01 00 00 00 03  |..T.......Q.....|
00000090  01 00 52 01 00 00 00 03  01 00 19 05 00 00 00 02  |..R.............|
000000a0  01 00 12 08 00 30 30 38  2e 70 61 72 74 07 f5 d5  |.....008.part...|
000000b0  4a 2d 63 33 76 d1 2d 9a  a1 c6 ac 31 55 7d 90 93  |J-c3v.-....1U}..|
000000c0  7b 00 00 04 00 00 00 02  01 00 01 21 00 41 6c 65  |{..........!.Ale|
000000d0  73 73 61 6e 64 72 61 20  41 6d 6f 72 6f 73 6f 20  |ssandra Amoroso |
000000e0  2d 20 49 6d 6d 6f 62 69  6c 65 2e 6d 69 64 03 01  |- Immobile.mid..|
000000f0  00 02 27 b6 62 00 02 01  00 27 20 00 55 48 56 43  |..'.b....' .UHVC|
00000100  46 51 4e 4f 59 46 53 47  58 57 4c 4e 59 5a 57 59  |FQNOYFSGXWLNYZWY|
00000110  4f 52 4e 50 58 56 36 59  56 4a 36 48 03 01 00 34  |ORNPXV6YVJ6H...4|
```

Figura 41 - Il file `known.met` visualizzato con un editor di esadecimale.

È doveroso ricordare come allo scopo di identificare i file realmente illeciti e di costruire il database di hash di file a contenuto illegale, i valori da memorizzare sono quelli relativi a hash e dimensione, atteso che il nome non è affatto importante dal momento che un file può essere rinominato e addirittura può presentarsi con un nome che riconduce ad altra tipologia di dato.

5.5.3. Formato di output per ogni reperto

Il programma eMuleForensic procede quindi a trasformare i file binari elencati in un file xml, la cui struttura è definita dal seguente XMLSchema.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns="http://www.emuleforensic.com"
 targetNamespace="http://www.emuleforensic.com"
 elementFormDefault="qualified">
 <xsd:element name="case" type="typeCase" />
 <xsd:complexType name="typeCase">
  <xsd:sequence>
   <xsd:element name="info" type="typeInfo" />
   <xsd:element name="search" type="typeSearch" />
   <xsd:element name="userinfo" type="typeUserinfo"/>
   <xsd:element name="clientsMet" type="typeClientsMet" />
   <xsd:element name="knownMet" type="typeKnownMet" />
  </xsd:sequence>
 </xsd:complexType>
 <xsd:complexType name="typeInfo">
  <xsd:sequence>
   <xsd:element name="code" type="xsd:string"/>
   <xsd:element name="description" type="xsd:string" />
   <xsd:element name="examinator" type="xsd:string" />
  </xsd:sequence>
 </xsd:complexType>
 <xsd:complexType name="typeSearch">
  <xsd:sequence>
   <xsd:element name="keyword" type="xsd:string"
   minOccurs="0" maxOccurs="unbounded" />
  </xsd:sequence>
 </xsd:complexType>
 <xsd:complexType name="typeUserinfo">
  <xsd:sequence>
   <xsd:element name="code" type="xsd:string"/>
   <xsd:element name="hash" type="xsd:string"/>
  </xsd:sequence>
 </xsd:complexType>
 <xsd:complexType name="typeClientsMet">
  <xsd:sequence>
   <xsd:element name="client" type="typeClient"
   minOccurs="0" maxOccurs="unbounded" />
  </xsd:sequence>
```

```
     <xsd:attribute        name="clients"        use="required"
type="xsd:integer"/>
    </xsd:complexType>
    <xsd:complexType name="typeClient">
     <xsd:sequence>
      <xsd:element name="code" type="xsd:string"/>
      <xsd:element name="hash" type="xsd:string"/>
      <xsd:element name="nUploaded" type="xsd:integer" />
      <xsd:element name="nDownloaded" type="xsd:integer" />
      <xsd:element name="nLastSeen" type="xsd:string" />
     </xsd:sequence>
     <xsd:attribute          name="id"          use="required"
type="xsd:integer"/>
    </xsd:complexType>
    <xsd:complexType name="typeKnownMet">
     <xsd:sequence>
      <xsd:element name="file" type="typeFile"
      minOccurs="0" maxOccurs="unbounded" />
     </xsd:sequence>
     <xsd:attribute         name="files"         use="required"
type="xsd:integer"/>
    </xsd:complexType>
    <xsd:complexType name="typeFile">
     <xsd:sequence>
      <xsd:element name="code" type="xsd:string"/>
      <xsd:element name="date" type="xsd:string"/>
      <xsd:element name="hashfile" type="typeHash" />
      <xsd:element name="filename" type="xsd:string"/>
      <xsd:element name="size" type="xsd:integer"/>
     </xsd:sequence>
     <xsd:attribute          name="id"          use="required"
type="xsd:integer"/>
    </xsd:complexType>
    <xsd:simpleType name="typeHash">
     <xsd:restriction base="xsd:string">
      <xsd:pattern value="[0123456789ABCDEF]{32}"/>
      <xsd:length value="32"/>
     </xsd:restriction>
    </xsd:simpleType>
   </xsd:schema>
```

Un esempio minimale di output generate è il seguente.

```
<?xml version="1.0"?>
<case xmlns="http://www.emuleforensic.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.emuleforensic.com schema.xsd">
 <info>
  <code>CASO0001</code>
  <description>Indagato: Mario Rossi (reperto 34)</description>
  <examinator>Michele Ferrazzano</examinator>
 </info>
 <search>
  <keyword>lino banfi</keyword>
  <keyword>antonello venditti</keyword>
  <keyword>wii</keyword>
  <keyword>wii mario kart</keyword>
  <keyword>porno</keyword>
  <keyword>sex</keyword>
  <keyword>7yo</keyword>
 </search>
 <userinfo>
  <code>1</code>
  <hash>1237B460D90E0DAB8B82EA5399FF6FA6</hash>
 </userinfo>
 <clientsMet clients="2">
  <client id="1">
   <code>CASO0001</code>
   <hash>FAADA708A30EE7DB6A00B005E0B76FF8</hash>
   <nUploaded>0</nUploaded>
   <nDownloaded>17167506</nDownloaded>
   <nLastSeen>Tue Sep 8 18:28:39 2009</nLastSeen>
  </client>
  <client id="2">
   <code>CASO0001</code>
   <hash>E5C0EAD1EA0EA5195077EBF9216E6F73</hash>
   <nUploaded></nUploaded>
   <nDownloaded>3445450</nDownloaded>
   <nLastSeen>Tue Aug 3 20:23:48 2009</nLastSeen>
  </client>
 </clientsMet>
 <knownMet files="2">
  <file id="0">
   <code>CASO0001</code>
   <date>Tue Sep 8 18:28:39 2009</date>
   <hashfile>77034E2B890ABC2EE8943954610FA48A</hashfile>
   <filename>young girls baby sex 7yo porno cum.avi</filename>
   <size>35893040</size>
  </file>
  <file id="1">
   <code>CASO0001</code>
   <date>Tue Oct 6 21:59:37 2009</date>
   <hashfile>1B5954D171240BBCDF57C7B3E50EF0DE</hashfile>
   <filename>[DivX]Il.diavolo.veste.prada.avi</filename>
   <size>744534366</size>
  </file>
 </knownMet>
```

```
</case>
```

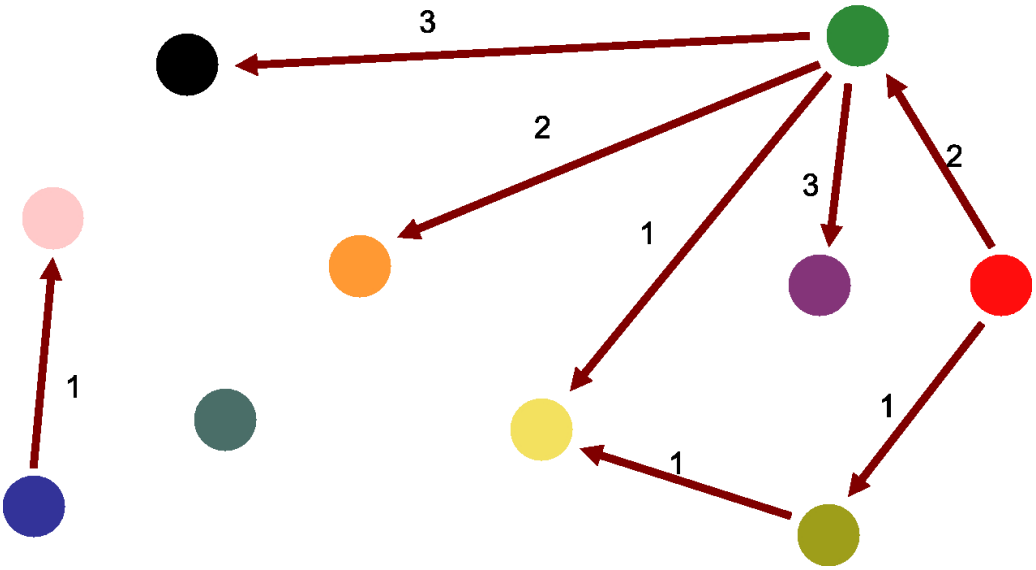
Da un output così composto, ottenibile nel giro di un secondo o poco più se l'attività di file sharing è stata particolarmente intensa, risulta evidente quali sono le ultime keyword utilizzate dall'indagato, i file scambiati, da quali utenti ha ricevuto e verso quali ha inviato.

Diventa molto semplice verificare il possesso di un file a contenuto illecito senza visualizzarlo. Supponiamo che l'utente abbia fatto sparire qualsiasi traccia del file "young girls baby sex porno cum.avi" tramite cancellazione sicura: disponendo di un archivio di hash, è possibile verificare se effettivamente quel file è stato in un momento precedente catalogato come file pedopornografico. Incrociando questa informazione con il dato relativo alle parole chiave utilizzate nella ricerca (nell'esempio proposto la keyword "young") è possibile inferire un'ipotesi di ricerca e detenzione consapevole di materiale pedopornografico.

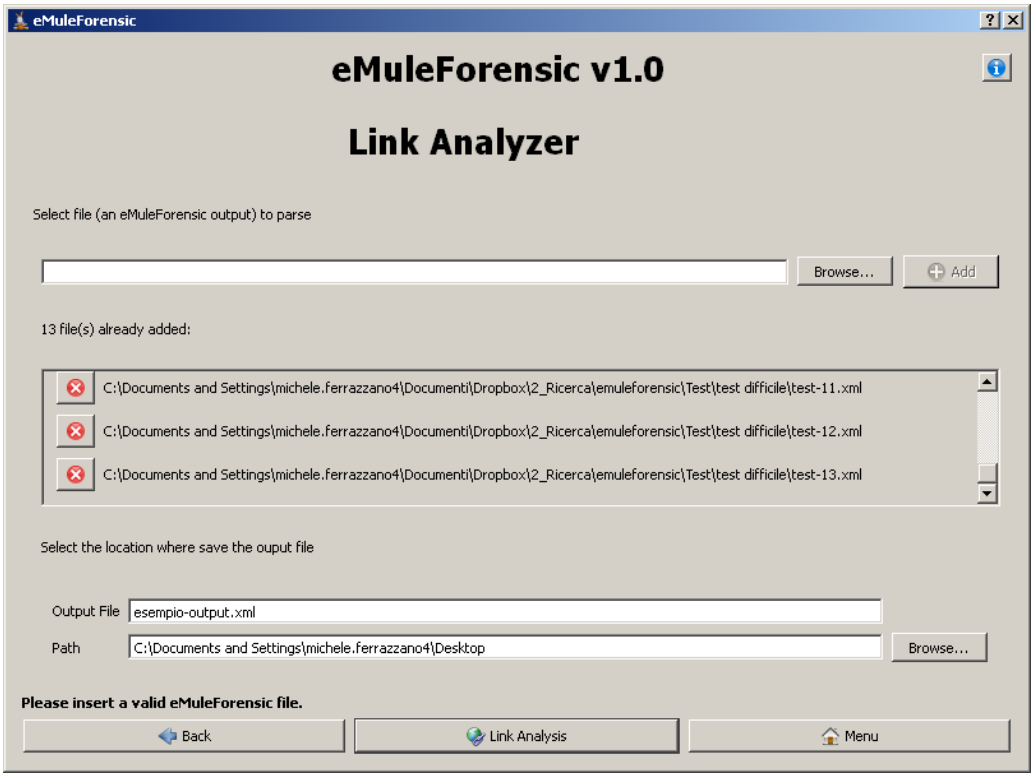
Utilizzando lo stesso criterio è altresì possibile identificare le circostanze in cui l'utente ha scaricato un file illecito per errore: si supponga ad esempio il caso in cui risulti presente un denominato "Pinocchio.avi", che tra le keyword di ricerca risulti la parola "pinocchio" e che l'hash associato al file sia rinvenibile nel database dei file catalogati come pedopornografici: è possibile inferire un'ipotesi di ricerca di file non di tipo pedopornografico che si è invece poi tradotta in scaricamento di file cosiddetto *fake* che l'utente ha poi provveduto a cancellare.

5.5.4. Link analysis: relazioni tra client

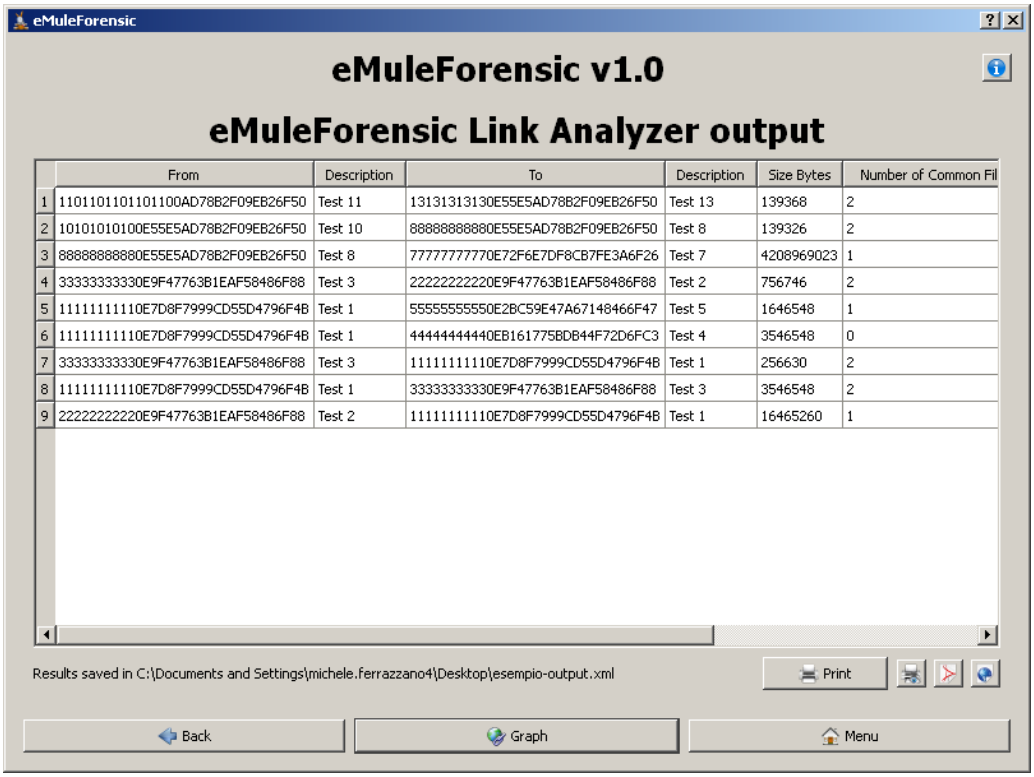
Una volta ottenuti i vari file xml da tutti i supporti oggetto di analisi, è possibile procedere ad una verifica incrociata degli output al fine di verificare le effettive connessioni tra gli utenti della rete peer-to-peer, potendo rappresentare le relazioni con un grafo di questo genere.



Tale attività incrociata può essere svolta utilizzando il modulo grafico implementato in Java oppure "manualmente" utilizzando uno strumento come Access. Il modulo di incrocio implementato in Java prevede che l'investigatore carichi tutti i file xml precedentemente generati.

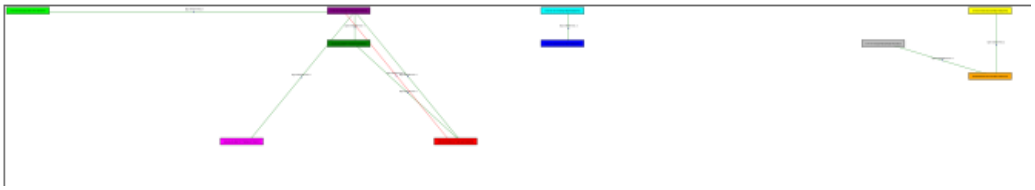


Quindi procedendo con l'analisi viene fornita una schermata che rappresenta in forma tabellare tutte le coppie con almeno un file in comune.



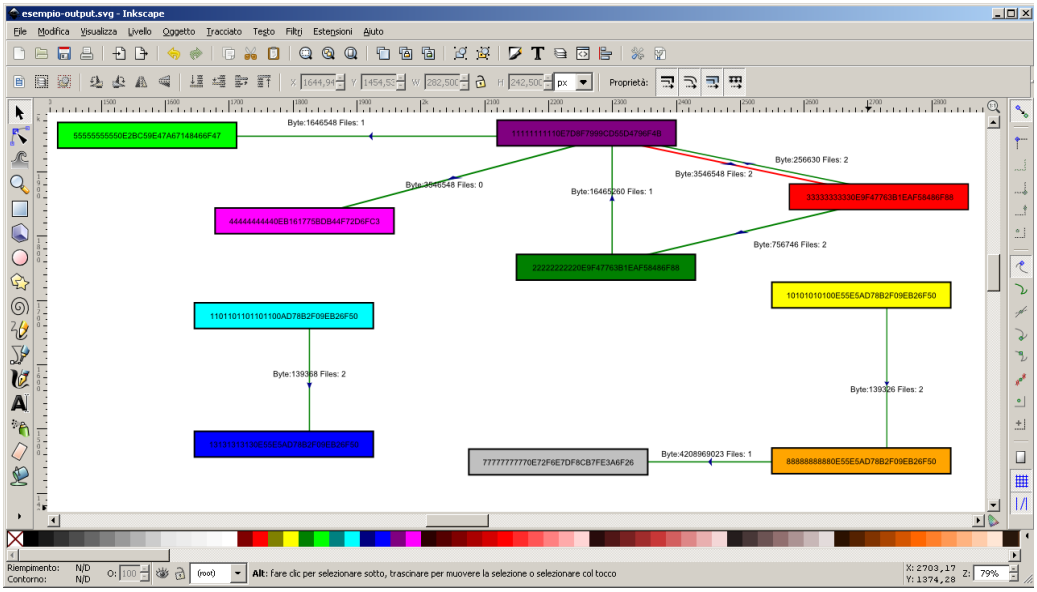
	From	Description	To	Description	Size Bytes	Number of Common Fil
1	1101101101101100AD78B2F09EB26F50	Test 11	13131313130E55E5AD78B2F09EB26F50	Test 13	139368	2
2	10101010100E55E5AD78B2F09EB26F50	Test 10	88888888880E55E5AD78B2F09EB26F50	Test 8	139326	2
3	88888888880E55E5AD78B2F09EB26F50	Test 8	77777777770E72F6E7DF8CB7FE3A6F26	Test 7	4208969023	1
4	33333333330E9F47763B1EAF58486F88	Test 3	22222222220E9F47763B1EAF58486F88	Test 2	756746	2
5	11111111110E7D8F7999CD55D4796F4B	Test 1	55555555550E2BC59E47A67148466F47	Test 5	1646548	1
6	11111111110E7D8F7999CD55D4796F4B	Test 1	44444444440EB161775BDB44F72D6FC3	Test 4	3546548	0
7	33333333330E9F47763B1EAF58486F88	Test 3	11111111110E7D8F7999CD55D4796F4B	Test 1	256630	2
8	11111111110E7D8F7999CD55D4796F4B	Test 1	33333333330E9F47763B1EAF58486F88	Test 3	3546548	2
9	22222222220E9F47763B1EAF58486F88	Test 2	11111111110E7D8F7999CD55D4796F4B	Test 1	16465260	1

Lo stesso risultato viene prodotto in un file XML delle coppie e in un file SVG[302] che può essere visualizzata in un qualsiasi editor per immagini di questo tipo, quale ad esempio Inkscape.



Il file può poi essere manipolato per spostare gli oggetti e rappresentare in maniera più gradevole e meno caotica il grafo già generato automaticamente da eMuleForensic.

[302] Il formato SVG (Scalable Vector Graphics) è una tecnologia derivata dall'XML in grado di visualizzare oggetti di grafica vettoriale.



5.5.5. Simulazione e valutazione dei risultati

Nella versione eseguibile a riga di comando[303], il programma Il programma viene eseguito a riga di comando indicando la cartella `config` in input, il file in cui salvare l'output e le informazioni utili ad identificare il reperto (codice del caso, descrizione del caso, nome dell'investigatore). Il comando da lanciare è quindi il seguente:

```
emuleforensic -i [INPUT DIR] -o [OUTPUT.xml] -c [CODICE CASO] -
d [DESCRIZIONE CASO] -e [NOME INVESTIGATORE]
```

5.6. Proposta di un protocollo operativo per l'analisi forense di reperti informatici per il reato di pedopornografia

Esaminate le norme in tema di pedopornografia e ponendo particolare attenzione agli aspetti di consapevolezza, analizzate le caratteristiche tecniche dei sistemi di condivisione di file nel peer-to-peer, individuato un insieme di parole chiave maggiormente utilizzate per la classificazione e la ricerca del materiale pedopornografico in rete, individuati e sviluppati i software che consentono di eseguire con maggiore efficacia l'analisi forense di supporti informatici coinvolti in tali reati, si propone in conclusione un protocollo

[303] La versione a riga di comando è disponibile nella distribuzione DEFT 7.1.

operativo per un'analisi forense completa ed esaustiva di un reperto informatico nei casi di pedopornografia.

Si suppone che il reperto informatico sia correttamente individuato, dunque come previsto dallo standard ISO/IEC 27037:2012 si procede al sequestro del supporto (se previsto) e comunque in ogni caso all'acquisizione forense al fine di produrre almeno una doppia copia forense.

L'analisi forense, come in ogni caso di indagini di informatica forense, viene svolta sulle copie forensi ottenute e si pone quattro obiettivi, a prescindere dal fatto che l'analisi sia finalizzata ad individuare elementi di colpevolezza o di innocenza:

1. ricerca di file a contenuto pedopornografico;
2. aspetti di consapevolezza in capo all'utilizzatore tramite ricerca di stringhe testuali utili ad individuare materiale pedopornografico, siti web consultati, email e più in generale di parole chiave riconducibili alla pedopornografia;
3. individuazione di elementi utili per apprezzare il possesso consapevole, ovvero verificare che l'utilizzatore del sistema informatico fosse a conoscenza del contenuto dei file posseduti e, laddove fosse possibile accertarlo, individuare elementi che consentano di apprezzare la consultazione e il livello di complessità di accesso alle risorse;
4. individuazione di elementi utili a ricondurre la paternità di quanto individuato ai punti precedenti in capo ad una persona fisica, attesa che l'associazione tra possessore (o utilizzatore) e reperto informatico non necessariamente viene sempre rispettata, specialmente in ambiente domestico; a tal proposito diventa altresì opportuno cercare di tracciare un profilo di competenze dell'utilizzatore al fine di poter esprimere una valutazione tecnica sulla possibilità che, ad esempio, lo scaricamento o l'accesso a tali dati sia avvenuto in maniera involontaria o senza consapevolezza.

Il protocollo proposto è valido sia nei casi in cui si intenda difendere un soggetto indagato (o imputato) di detenzione e divulgazione di materiale pedopornografia, sia nei casi in cui si cerchino prove di colpevolezza. Lo schema proposto in Figura 1Figura 42 riassume graficamente i vari passi previsti dalla metodologia proposta.

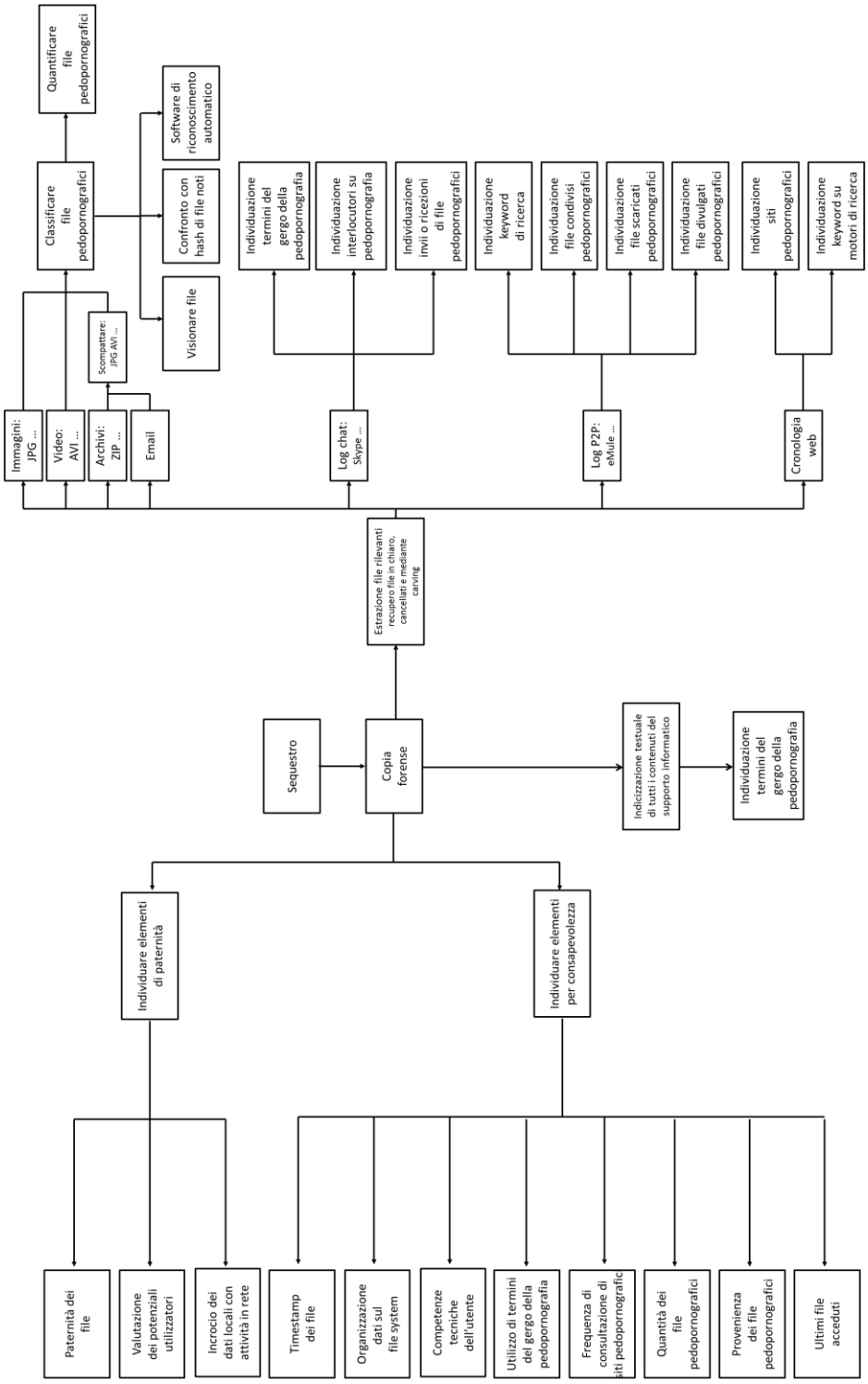


Figura 42 – Proposta di protocollo operativo per l'analisi forense di reperti informatici per il reato di pedopornografia

Si tratta di individuare elementi relativi al possesso consapevole, a eventuali rapporti con altri soggetti, a pratiche poste in essere con coscienza in relazione a ricerca, scaricamento e invio. Ogni singolo passo viene di seguito analizzato in dettaglio.

5.6.1. Individuazione dei file a contenuto pedopornografico

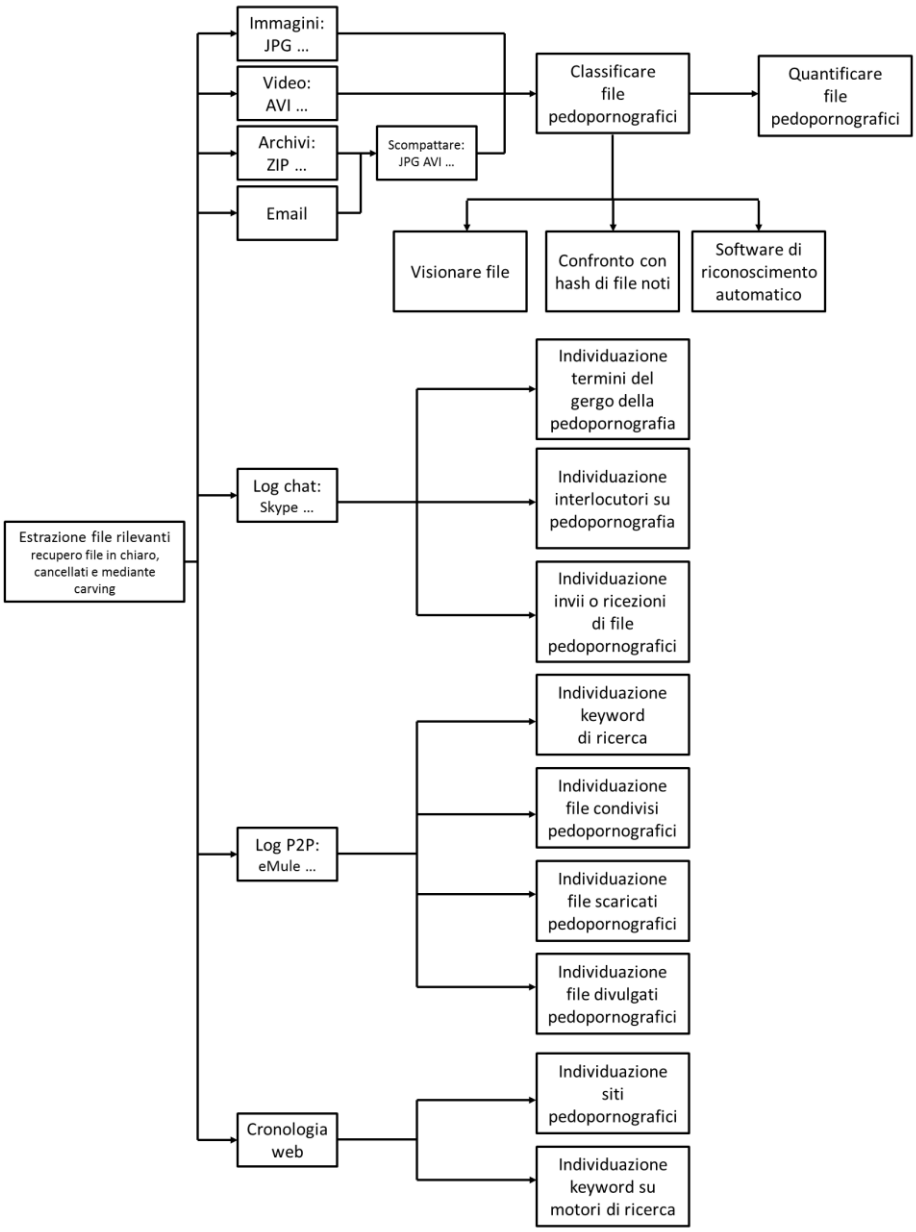


Figura 43 – Dettaglio dello schema di Figura 42 relativo all'estrazione dei file rilevanti ai fini dell'individuazione del materiale pedopornografico

Ingrandendo parte dello schema precedente, in primo luogo va definito cosa si intende per file pedopornografico al fine di poter quantificare in maniera quanto più possibile univoca ed efficace la quantità complessiva, valore rilevante per la commisurazione della pena[304]. Se per un file immagine la risposta è piuttosto evidente, nel caso di un video comincia a diventare più complessa:

- un video di 10 minuti vale "1" o vale "*n*" dove *n* sono i fotogrammi?[305]
- 100 fotogrammi estratti dal video del punto precedente valgono 100 file o 1?
- un file immagine prodotto come collage di *n* immagini vale "1" o "*n*"?
- un file rinvenuto in *n* punti diversi si considera "1" o "*n*"?
- la presenza del video e dei relativi fotogrammi o è da considerare doppione?
- un archivio compresso contenente *n* file vale "1" o vale "*n*"? E se vale "*n*", qualora si rinvengano anche alcuni file estratti si sommano?
- un documento (pdf, doc…) contenente *n* immagini vale "1" o vale "*n*"?

La difficoltà di individuare una risposta condivisa a queste domande trova facile riscontro nelle consulenze tecniche, dove l'accusa tende a quantificare a livello superiore mentre la difesa al minimo. A nostro parere sarebbe corretto quantificare i file senza inserire nel conteggio i doppioni, ovvero sia file con medesimo contenuto che file derivati (ad esempio, fotogrammi di un video o file estratti da archivi compressi), tranne nei casi in cui tali derivazioni non siano palesemente classificate: si pensi ad esempio al caso di un archivio decompresso in diversi file lasciati nella cartella in cui sono stati estratti rispetto agli stessi file organizzati per età dei soggetti raffigurati.

Per quanto concerne le modalità di individuazione dei file, come già esposto nei capitolo precedenti, occorre procedere all'estrazione di tutti i file

[304] In tema di commisurazione della pena si ricorda che la quantificazione del numero di file è determinante a causa dell'aggravante prevista nell'ordinamento giuridico italiano all'art. 600-quater c.p., comma 2, dove tuttavia non viene fornito alcun parametro per stabilire le modalità di valutazione dei file né la soglia limite.

[305] In tal proposito, la totalità delle sentenze si orienta sul valore 1.

che potenzialmente possono contenere scene di pornografia minorile per poi passare alla fase di analisi dei contenuti al fine di determinare la reale natura dei file: tale classificazione può essere fatta manualmente da chi procede all'analisi, mediante comparazione di hash qualora si disponga di un database sufficientemente ampio oppure mediante l'impiego di strumenti di riconoscimento di pattern all'interno delle immagini e dei video che tuttavia al momento non raggiungono ancora un grado di affidabilità sufficiente[306], richiedendo comunque un'attività di verifica da parte dell'utilizzatore.

In ogni caso, a prescindere dal criterio scelto per la quantificazione dei file e diversamente da quanto accade nella quasi totalità dei casi reali di indagini di informatica forense su reati di pedopornografia, la ricerca di file rilevanti non può limitarsi unicamente all'individuazione di file a contenuto pedopornografico dal momento che è necessario individuare ulteriori elementi che consentano di apprezzare la consapevolezza da parte dell'utente: l'analisi di log di navigazione ad internet e delle conversazioni di chat sono certamente tra gli elementi più utili per riuscire a determinare il grado di consapevolezza, nonché per riuscire a tracciare un profilo della persona fisica che realmente utilizzava il sistema e le relative competenze. A tal proposito, la produzione di un supporto contenente i soli file pedopornografici è inutile se non accompagnata dal resto dell'analisi, atteso che consente unicamente di quantificare il materiale ma non apprezzare la consapevolezza né individuare univocamente l'utilizzatore e le modalità di approvvigionamento del materiale.

Altro elemento rilevante è l'analisi dei log dei software di file sharing individuati sul sistema in esame: la progettazione e l'implementazione di eMuleForensic trova impiego in questa fase oltre nella successiva, consentendo di rinvenire tracce di scaricamenti e divulgazioni di materiale pedopornografico, nonché dei volumi di scambio e delle parole chiave utilizzate per ricercare il materiale sulla rete peer-to-peer.

[306] Un esempio di software che opera la ricerca automatiche di scene di pedopornografia in immagine è NuDetective descritto in de Castro Polastro M., da Silva Eleuterio P. (2010) NuDetective: A Forensic Tool to Help Combat Child Pornography through Automatic Nudity Detection. In *Workshop on Database and Expert Systems Applications (DEXA)*. Bilbao. 349–353.

5.6.2. Individuazione di elementi utili per apprezzare la consapevolezza

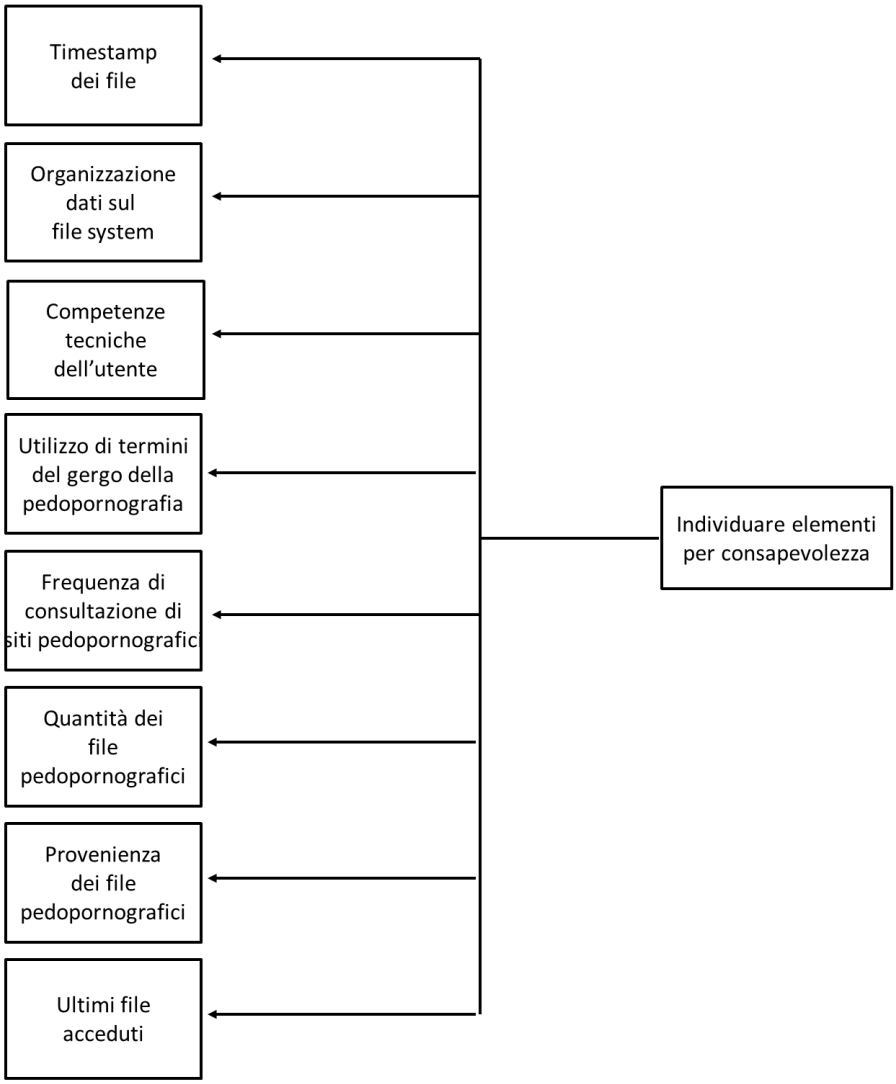


Figura 44 – Dettaglio dello schema di Figura 42 relativo all'individuazione di elementi di consapevolezza

La prova della colpevolezza per i reati di pedopornografia consiste: nell'accertamento positivo dell'elemento oggettivo delle fattispecie di divulgazione, procacciamento o detenzione di immagini pornografiche minorili, anche virtuali; nella prova del nesso causale tra la condotta del soggetto e gli eventi sopraccitati; nell'accertamento positivo dell'elemento soggettivo del

reato, consistente nella consapevolezza o nella coscienza e volontà dell'agente, con l'esclusione del dolo eventuale[307].

Qualora siano stati individuati file di natura pedopornografica, indispensabili per poter sostenere un'accusa di pedopornografia, l'accusa ha dunque l'onere di provare il possesso consapevole dei dati mentre la difesa ha interesse a dimostrare come i dati presenti sul sistema informatico non consentano di sostenere tale ruolo consapevole. Per giungere a conclusione sono molteplici gli elementi da prendere in esame come evidenziato nell'immagine di Figura 44.

La riconducibilità dei fatti in un preciso spazio temporale è senza dubbio uno degli elementi principali per la corretta interpretazione della scena criminis in quanto consente di rivelare la dinamica degli eventi nell'ordine in cui gli stessi si sono verificati. Lo strumento che consente di effettuare l'analisi forense sul tempo è la timeline, cioè la rappresentazione cronologica di avvenimenti chiave all'interno di un particolare arco temporale: si tratta cioè di una fotografia di tutti gli eventi relativi ai file (ultimo accesso, ultima modifica, creazione, stampa…) avvenuti su un sistema informatico[308]. In particolare, ai fini dell'analisi forense finalizzata alla ricerca di elementi utili a determinare la consapevolezza in relazione al reato di pedopornografia, l'elenco degli ultimi file acceduti, posto in relazione al rilevamento temporale di ultima modifica e creazione, è un'evidenza fondamentale. Infatti, gli ultimi file consultati dall'utente sono rinvenibili in una cartella del sistema sotto forma di collegamento ed evidentemente questo dato consente di sostenere che l'utente ha effettivamente consultato, ovvero valutato ed entrato in conoscenza, il contenuto del file che è presente sul supporto informatico; i timestamp dei file – ovvero il riferimento temporale di ora e data di ultimo accesso, creazione e ultima modifica del file – consentono di verificare gli accessi ai file che si sono verificati in tempi successivi alla creazione (cioè alla memorizzazione dei file sul file system del reperto in analisi) anche quando questi non sono ormai più presenti nella lista dei file recenti. Tuttavia c'è da tenere in considerazione che l'alterazione della data di ultimo accesso è un evento che si può verificare anche in seguito ad eventi automatici quali la copia dei dati, che può comunque essere rilevante ai fini della consapevolezza, o la ricerca di file per parola chiave

[307] Novario F. (2009) Pornografia minorile e file sharing: l'influenza della tecnologia informatica sull'asse probatorio. *Diritto penale e processo*, 10/2009, 1290–1292.

[308] Calabrò V., Dal Checco P., Fiammella B. (2012) La timeline: aspetti tecnici e rilevanza processuale. *In:* Attanasio A., Costabile G., eds. *IISFA Memberbook 2011*. Experta. 93–149.

mediante la funzione "cerca" offerta dai sistemi operativi che dunque non rileva alcun tipo di consultazione o accesso da parte dell'utilizzatore del sistema informatico.

Altro elemento rilevante ai fini della consapevolezza è il rinvenimento all'interno di documenti e file prodotti dall'utente, volontariamente o in maniera automatica sotto forma di file di log, di parole chiave riconducibili alla pedopornografia utilizzate per cercare o catalogare il materiale pedopornografico: tale informazione evidenzia la padronanza lessicale in capo all'utilizzatore del sistema nonché la volontà di conservare il materiale o informazioni utili al reperimento.

Sempre in tema di consapevolezza è altresì determinante individuare le locazioni di memoria in cui i file sono allocati e la relativa organizzazione, la distribuzione degli stessi sui vari supporti informatici e le percentuali rispetto alle altre tipologie di file a disposizione dell'utilizzatore: la presenza di pochi file archiviati in maniera più o meno casuale su vari supporti lascia propendere per la non consapevolezza, atteso che l'utilizzatore di un sistema informatico, per quanto poco pratico, utilizza criteri logici nell'organizzazione dei file; al contrario la presenza di file in maniera concentrata, soprattutto se con archiviazione che evidenzia pignoleria da parte dell'utilizzatore, e la facilità di raggiungimento dei file (si pensi ai file accedibili con un clic dal Desktop) depongono a favore di una condotta di detenzione consapevole. Numerose ricerche internazionali hanno dimostrato che i pedofili hanno una forte propensione verso il collezionismo di materiale pornografico, sia di tipo tradizionale (libri, riviste, giornali, fotografie…) sia come file multimediali[309]. Elemento rilevante è anche il rapporto tra numero di file pedopornografici e materiale di pornografia adulta in ragione del fatto che l'utente interessato alla pornografia può accidentalmente incappare anche in file pedopornografici[310].

La definizione di un profilo di competenze tecniche dell'utilizzatore è un elemento importante da prendere in esame per poter stabilire il livello di

[309] Florindi E., Strano M. (2006) La pedopornografia. *In:* Strano M., ed. *Abusi sui minori: manuale investigativo*. Nuovo Studio Tecna.

[310] In tal senso si richiama la sentenza del Tribunale di Avezzano del 25 maggio 2011, n. 254, richiamata in Venturini S. (2012) Sequestro probatorio e fornitori di servizi telematici. *In:* Luparia L., ed. *Internet Provider e giustizia penale*. Giuffrè. 107–140. Il Tribunale di Avezzano ha assolto l'imputato dall'accusa di divulgazione in rete di materiale pedopornografico poiché dalla consulenza tecnica non era emersa la prova che lo stesso avesse volontariamente posto il file tra il materiale da condividere. Inoltre, il file risultava cancellato (ma recuperato) in una cartella in cui si trovavano numerosi file a contenuto pornografico.

consapevolezza dell'utente: tale valutazione deve prendere in esame la formazione, il lavoro svolto, il tempo medio trascorso al computer, le attività tipiche svolte al computer, i siti consultati, le tipologie di ricerca condotte e così via.

Infine, un'ulteriore modalità di analisi che può giovare nella valutazione di elementi di consapevolezza prevede l'uso di macchine virtuali[311] per la riproposizione delle sequenza di operazioni messe in atto dall'utilizzatore del sistema informatico.

5.6.3. Individuazione di elementi utili a rilevare il reale utilizzatore

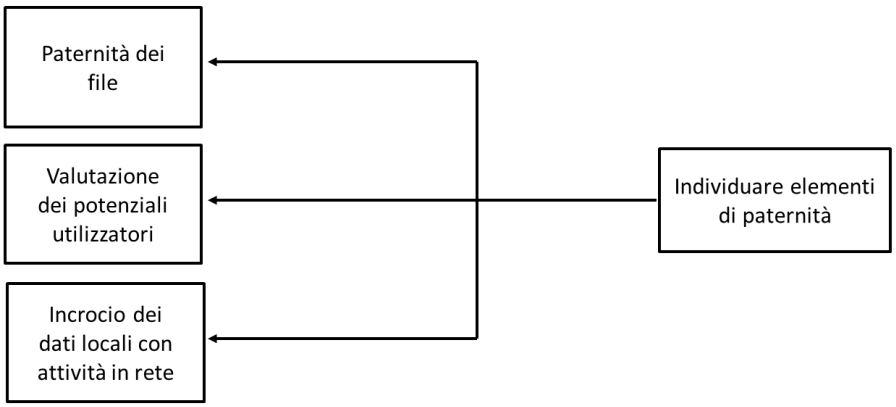


Figura 45 – Dettaglio dello schema di Figura 42 relativo all'individuazione di elementi di paternità per l'identificazione del reale autore del reato

Nei casi in cui il sistema informatico sia stato reperito in un luogo in cui avevano facilità di accesso più di un soggetto, occorre ricostruire anche il profilo dell'utilizzatore, ovvero cercare di individuare la persona fisica che realmente ad una certa ora di un certo giorno ha compiuto una determinata azione: per far ciò, la valutazione della navigazione in Internet con particolare riferimento all'accesso a siti di social networking o comunque ad accesso riservato (ad esempio, una casella di posta elettronica) e l'analisi dei file

[311] Il termine macchina virtuale indica l'emulazione di una macchina reale mediante l'uso di un software che realizza un finto computer su cui può essere eseguito un sistema operativo. Nel caso dell'informatica forense, il sistema eseguito dalla macchina virtuale potrebbe essere il sistema oggetto di analisi. Sul tema, *cfr.* Caccavella D. (2007) "Case study: l'uso delle macchine virtuali nella Disk e Network forensics". *In:* Atti del Convegno di Varenna (Lecco) del 16 febbraio 2007. *Reati informatici e attività di indagine: dal cyberterrorismo alla computer forensics*. Experta. 107–117.

elaborati consente di determinare quale fosse la persona che realmente aveva posto in essere le attività illecite contestate.

5.6.4. Analisi testuale dei supporti

Nei casi in cui nelle fasi precedenti non si ottengano sufficienti elementi per sostenere accuse di consapevolezza, nonché nei contesti in cui si intenda dimostrare l'assenza di elementi che conducano inequivocabilmente alla pedopornografia, l'analisi testuale dei supporti è lo strumento che consente di individuare – se presenti – keyword rilevanti, riuscendo a riscontrare il contesto e la frequenza di uso.

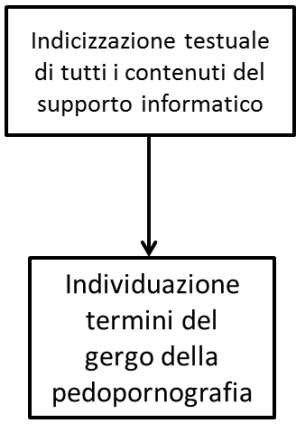


Figura 46 – Dettaglio dello schema di Figura 42 relativo all'individuazione di termini del gergo della pedopornografia

Le parole chiave da impiegare in questo genere di analisi sono quelle tipiche della pedopornografia già presentate nei capitoli precedenti[312], nonché specifiche stringhe testuali del caso in esame, quale ad esempio un indirizzo di un sito web monitorato.

[312] In 4.3.1.

Conclusioni

In questo lavoro è stata inquadrata la prova informatica quale prova scientifica che richiede l'adozione di precauzioni come in un qualsiasi altro accertamento scientifico. In tale ottica è stata fornita una panoramica sugli aspetti metodologici e applicativi dell'informatica forense alla luce del recente standard ISO/IEC 27037:2012 in tema di trattamento del reperto informatico nelle fasi di identificazione, raccolta, acquisizione e conservazione del dato digitale. Tali metodologie si attengono scrupolosamente alle esigenze di integrità e autenticità richieste dalle norme in materia di informatica forense, in particolare della Legge 48/2008 di ratifica della Convenzione di Budapest sul Cybercrime.

In merito al reato di pedopornografia è stata offerta una rassegna della normativa comunitaria e nazionale, ponendo l'enfasi sugli aspetti rilevanti ai fini dell'analisi forense. Rilevato che il file sharing su reti peer-to-peer è il canale sul quale maggiormente si concentra lo scambio di materiale illecito, è stata fornita una panoramica dei protocolli e dei sistemi maggiormente diffusi, ponendo enfasi sulla rete eDonkey e il software eMule che trovano ampia diffusione tra gli utenti italiani. Sono state accennate le problematiche che si incontrano nelle attività di indagine e di repressione del fenomeno, di competenza delle forze di polizia, per poi concentrarsi e fornire il contributo rilevante in tema di analisi forensi di sistemi informatici sequestrati a soggetti indagati (o imputati) di reato di pedopornografia: la progettazione e l'implementazione di eMuleForensic consente di svolgere in maniera estremamente precisa e rapida le operazioni di analisi degli eventi che si verificano utilizzando il software di file sharing eMule.

Partendo dagli errori e dalle carenze normalmente riscontrate nelle relazioni tecniche di consulenti tecnici e forze dell'ordine, il forte contributo del presente lavoro è nella definizione di una completa metodologia per l'analisi del sistema informatico non finalizzato alla sola individuazione del materiale ma anche alla raccolta di dati utili ad apprezzare la consapevolezza nella condotta e la paternità delle operazioni compiute. Nell'ottica di fornire una metodologia non solo esaustiva ma anche rapida, lo sviluppo del software opensource emuleforensic intende mettere a disposizioni di tutti gli operatori uno strumento che si prefigge di verificare in tempi quantificabili nell'ordine di secondi le

attività che si sono verificate utilizzando il software eMule: in tal modo, sin dalle fasi della perquisizione informatica è possibile stabilire se un sistema informatico sia coinvolto nel reato e in che misura, ottimizzando a cascata anche le fasi successive dell'accertamento.

Il tool è stato già da alcuni anni reso disponibile sia in rete all'url *http://www.emuleforensic.com*, sia come tool all'interno della distribuzione forense DEFT: per quanto riguarda il sito web si sono registrati oltre 2000 contatti in due anni con diverse richieste via email di precisazioni da parte di utenti (principalmente forze dell'ordine) di tutto il mondo, in particolare Italia, Brasile e Stati Uniti, ottenendo numerosi feedback positivi sull'usabilità e l'efficacia in termini di tempi e risultati.

Allo stato dell'arte il tool sviluppato è l'unico software forense opensource che consenta l'analisi di sistemi informatici coinvolti nel file sharing sul peer-to-peer e comunque uno dei pochi disponibili se si considerano anche un paio di tool commerciali. Si auspica lo studio più dettagliato degli altri protocolli di file sharing e lo sviluppo di relativi tool di analisi che consentano una rapida analisi anche degli altri software che si vanno affermando, in particolar modo BitTorrent.

Bibliografia

Aidouni F., Latapy M., Magnien C. (2009) Ten weeks in the life of an eDonkey server. In *Sixth International Workshop on Hot Topics in Peer-to-Peer System (Hot-P2P 2009)*. Roma, Maggio 2009.

Akdeniz Y. (2008) *Internet Child Pornography and the Law*. Ashgate.

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

Attanasio A., Cajani F., Costabile G., Vannini W. (2013) Lo stato dell'arte della computer forensics in Italia. *In:* Attanasio A., Costabile G., eds. *IISFA Memberbook 2012*. Experta. 123–151.

Barrett D., Broom N., Rudolph K., Salomon M., Tittel E. (2011) *Computer forensics jumpstart*. Second edition. Sybex.

Battiato S., Farinella G., Puglisi G. (2012) Image/video forensics: casi di studio. *In:* Attanasio A., Costabile G., eds. *IISFA memberbook 2011*. Experta. 261–292.

Battiato S., Messina G., Rizzo R. (2009) Image forensics contraffazione digitale e identificazione della camera di acquisizione: status e prospettive. *In:* Attanasio A., Costabile G., eds. *IISFA Memberbook 2009*. Experta. 49–98.

Bauer K., Grunwald D., McCoy D., Sicker D. (2009) Bitstalker: Accurately and efficiently monitoring bittorrent traffic. *Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS)*, London, UK, 2009.

Bellissimo L., Crisafi M., Trunfio E. (2010) *Pedofilia. Disciplina, tutele e strategie di contrasto*. Giuffrè.

Belbèze C., Latapy M. (2009) Detecting keywords used by paedophiles. *In:* Seifi M., ed. *Proceeding of International Conference Advances in the Analysis of Online Paedophile Activity*, 93–96.

Belbèze C., Chavalarias D., Denoyer L., Fournier R., Guillaume J., Latapy M., Magnien C., Valadon G., Vehovar V., Žiberna A. (2010) *Technical report on Automatic Identification of Paedophile Keywords*. *http://antipaedo.lip6.fr.*

Berry M, Linoff G.(2002) *Data mining. L'azienda intelligente e la gestione strategica delle informazioni*. Apogeo.

Bickson D., Kulbak Y. (2005) *The emule protocol specification*. Online *http://leibniz.cs.huji.ac.il/tr/731.pdf*.

Braghò G. (2004) Le indagini in materia di reati informatici. In Pozzi P., Masotti R., Bozzetti M., eds. *Crimine virtuale, minaccia reale. ICT Security: politiche e strumenti di prevenzione*, Franco Angeli, 33–43.

Caccavella D. (2007) Case study: l'uso delle macchine virtuali nella Disk e Network forensics. *In:* Atti del Convegno di Varenna (Lecco) del 16 febbraio 2007. *Reati informatici e attività di indagine: dal cyberterrorismo alla computer forensics*. Experta. 107–117.

Cadoppi A. (2006) *Commentario delle norme contro la violenza sessuale e contro la pedofilia*. Cedam.

Cajani F., Costabile G., Mazzaraco G. (2008) *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria*. Giuffrè.

Calabrò V., Dal Checco P., Fiammella B. (2012) La timeline: aspetti tecnici e rilevanza processuale. *In:* Attanasio A., Costabile G., eds. *IISFA Memberbook 2011*. Experta. 93–149.

Carrier B. (2006) *A hypothesis-based approach to digital forensic investigations*. PhD thesis, Purdue University.

Carrier B. (2005) *File system forensic analysis*. Addison Wesley.

Carrier B., Spafford E. (2003) Getting physical with the digital investigation process. *International Journal of Digital Evidence*, 2(2).

Casey E. (2004) *Digital Evidence and Computer Crime. Forensic science, computers and the Internet*. Elsevier.

Catullo F. (2004) Nota in tema di pornografia minorile e di prostituzione via Internet. *Cassazione penale*, XLIV, novembre 2004, 3577–3585.

Chau M., Chen H., Chung W., Qin Y., Xu J., Wang G. (2004) Crime data mining: a general framework and some examples. In *IEEE Computer society*, 37(4), 50–56.

Choo R. (2009) *Online child grooming: a literature review on the misuse of social networking sites for sexual offences*. Australian Institute of Criminology.

Chothia T., Cova M., González C., Novakovic C. (2013) The Unbearable Lightness of Monitoring: Direct Monitoring in BitTorrent. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, 106, 185–202.

Christin N., Chuang J., Weigend A. (2005) Content Availability, Pollution and Poisoning in Peer-to-Peer File Sharing Networks. In *ACM E-Commerce Conference (EC'05)*, June 2005.

Colella A., Ghirardini A., Ianulardo M. (2009) Reati di pedopornografia in ambiente P2P. Simulazione tecnica per definire i concetti di detenzione, cessione e diffusione. *In:* Attanasio A., Costabile G., eds. *IISFA Memberbook 2009*. Experta. 49–98.

Conti C., Tonini P. (2012) *Il diritto delle prove penali*. Giuffrè.

Convey G. (2007) Collecting volatile and non-volatile data. *IISA Journal*, August 2007, 28–31.

Costabile G. (2011) Peer to peer e digital forensics: il caso Emule. In: Aterno S., Cajani F., Costabile G., Mattiucci M., Mazzaraco G. (2011) *Computer forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*. Experta. 137–150.

Cowen D. (2013) *Computer Forensics InfoSec Pro Guide*. McGraw Hill.

Davidson J., Gottschalk P. (2011) *Internet child abuse. Current research and policy*. Routledge.

Davidson J., Martellozzo E. (2008) Protecting children in cyberspace. In: Legherby G., Birch P., Cain M., Willimas K., eds. *Sex Crime*. Willan Publishers.

Dazeley R., Layton R., Watters P. (2011) How much material on BitTorrent is infringing content? A case study. *Information Security Technical Report*, 16(2), 79–87.

D'Agostini D., D'Angelo S., Violino L. (2007) *Diritto penale dell'informatica: dai computer crimes alla digital forensic*. Experta.

D'Aiuto G., Levita L. (2012) *I reati informatici. Disciplina sostanziale e questioni processuali*. Giuffrè.

de Castro Polastro M., da Silva Eleuterio P. (2010) NuDetective: A Forensic Tool to Help Combat Child Pornography through Automatic Nudity Detection. In *Workshop on Database and Expert Systems Applications (DEXA)*. Bilbao. 349–353.

De Marco F., Mattiucci M., Rossi A., Strano M. (2006) Le investigazioni sulla pedofilia on-line. *In:* Strano M., ed. *Abusi sui minori: manuale investigativo*. Nuovo Studio Tecna, 86–94.

Dhungel P., Ross K. Schonhorst B., Wu D. (2008) A Measurement Study of Attacks on Bit-Torrent Leechers. In *Proceedings of Seventh International Workshop on Peer-to-Peer Systems (IPTPS)*, Tampa Bay, USA.

Dominioni O. (2005) *La prova penale scientifica*. Giuffrè.

Edilton E., Souza J. (2009) EspiaMule e Wyoming ToolKit: Ferramentas de Repressão à Exploração Sexual Infanto-Juvenil em Redes Peer-to-Peer. In *Proceedings of the Fourth International Conference of Forensics Computer Science*. 108–113.

Erdely R., Kerle T., Levine B., Liberatore M., Shields C. (2010) Forensic investigation of peer-to-peer file sharing networks. In *Digital investigation*, 7, 95–103.

Fagioli G., Ghirardini A. (2013) *Digital forensics*. Apogeo.

Fagundes P. (2009) Fighting Internet Child Pornography The Brazilian Experience. *Police Chief*, 76(9), 48–55.

FBI (2007) *Handbook of Forensic science*. Online *http://www.fbi.gov/about-us/lab/handbook-of-forensic-services-pdf*.

Ferrazzano M. (2014) Disk forensics analysis of file sharing client in peer-to-peer environments. In Boscarato C., Caroleo F., Santosuosso A., eds. *Law&Science Young Scholars Informal Symposium - 2013 Round*. Pavia University Press [in corso di pubblicazione].

Ferrazzano M. (2011) Reati di pedopornografia in ambiente eMule: analisi dei log per ricostruire attività di scambio tra vari utenti indagati. *In:* Attanasio A., Costabile G., eds. *IISFA Memberbook 2010*. Experta. 49–69.

Ferrazzano M., Maioli C. (2011) Control of File Exchange of Illicit Materials in Peer-to-Peer Environments. In *Proceedings of the 4th International Conference on Information Law*, Thessalonica, 2011. 154–165.

Florindi E. (2012) *Computer e diritto. L'informatica giuridica nella società dell'informazione e della conoscenza*. Giuffrè.

Florindi E., Strano M. (2006) La pedopornografia. *In:* Strano M., ed. *Abusi sui minori: manuale investigativo*. Nuovo Studio Tecna. 191–203.

Fournier R., Latapy M., Magnien C. (2013) Quantifying paedophile activity in a large P2P system. In *Information Processing and Management*, 49(1). 248–263.

Fournier R., Latapy M., Magnien C., Seifi M. (2010) *Maps of paedophile activity. http://antipaedo.lip6.fr.*

Fournier R., Latapy M., Magnien C., Valadon G. (2009) Tracing paedophile eDonkey users through keyword-based query. *In:* Seifi M., ed. *Proceeding of International Conference Advances in the Analysis of Online Paedophile Activity*, 97–98.

Gabrini D., Perri P., Specchio G. (2012) Live forensics. *In:* Attanasio A., Costabile G., eds. *IISFA Memberbook 2011*. Experta. 151–200.

Gammarota A. (2004) Un caso di studio di informatica forense: danneggiato di un sistema informatico della Pubblica Amministrazione. *In*: Pozzi P., Masotti R., Bozzetti M., eds. *Crimine virtuale, minaccia reale. ICT Security: politiche e strumenti di prevenzione*. FrancoAngeli.

Garcia J. (2009) FIVES and P2P-based Intelligence Gathering. *In:* Seifi M., ed. *Proceeding of International Conference Advances in the Analysis of Online Paedophile Activity*, 27–31.

Garrison C., Lillard T., Schiller C., Steele J. (2010*) Forensics for Network, Internet, and Cloud Computing. A Forensic Evidence Guide for Moving Targets and Data*. Elsevier.

Grance T., Mell J. (2011) *The NIST definition of cloud computing*. NIST. *http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf*.

Grillo A. (2012) Indagini digitali mediante strumenti Open Source e Freeware. *In:* Carretta P., Cilli A., Iacoviello A., Grillo A., Trocchi F. *L'acquisizione del documento informatico. Indagini penali e amministrative*. LaurusRobuffo. 107–202.

Gubitosa C. (1999) *Italian Crackdown*. Apogeo.

Guillaume J., Latapy M., Magnien C., Valadon G. (2008) *Content rating and fake detection system. http://antipaedo.lip6.fr*.

Helfer M. (2007) *Sulla repressione della prostituzione e pornografia minorile. Una ricerca comparatistica*. Cedam.

Intini A., Picozzi M. (2009) *Scienze Forensi. Teoria e prassi dell'investigazione scientifica*. Utet.

Jenkins P. (2003) *Beyond Tolerance: Child Pornography on the Internet*. NYU Press.

Kohler E., Liogkas N., Nelson R., Zhang L. (2006) Exploiting BitTorrent For Fun (But Not Profit). In *Proceedings 5th International Workshop on Peer-to-Peer Systems (IPTPS)*, Santa Barbara, USA, 2006.

Kohno T., Krishnamurthy A., Piatek M. (2008) Challenges and Directions for Monitoring P2P File Sharing Networks - or - Why My Printer Received a DMCA Takedown Notice. In *Proceedings of the USENIX Workshop on Hot Topics in Security*, San Jose, USA.

Krone T. (2004) A typology of online child pornography offending. In *Australian Institute of Criminology, Trends and Issues in Crime and Criminal Justice*, 279.

Krone T. (2005) International Police Operations Against Online Child Pornography. In *Australian Institute of Criminology, Trends and Issues in Crime and Criminal Justice*, 296.

Kumar R., Liang J., Xi Y., Ross K. (2005) Pollution in P2P file sharing systems. In *IEEE INFOCOM 2005*.

Heiser J., Kruse W. (2001) *Computer forensics. Incident Response Essentials*. Addison-Wesley.

Lange R., Ghedini Ralha C. (2011) Identificação de Artefatos Periciais do eMule. In *Proceedings of the Sixth International Conference on Forensic Computer Science*. 44–53.

Latapy M., Magnien C., Valadon G. (2009) Measurement of paedophile activities in eDonkey. *In:* Seifi M., ed. *Proceeding of International Conference Advances in the Analysis of Online Paedophile Activity*, 7–8.

Layton R., Watters P. (2010) *Investigation into the extent of infringing content on BitTorrent networks*. Internet Commerce Security Laboratory.

Liang J., Naoumov N., Ross K. (2006) The Index Poisoning Attack in P2P File Sharing Systems. In *Proceedings INFOCOM 2006 25th IEEE International Conference on Computer Communications*, April 2006.

Luparia L., Ziccardi G. (2007) *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*. Giuffrè.

Locher T., Moor P., Schmid S., Wattenhofer R. (2006) Free Riding in BitTorrent is Cheap. In *Fifth Workshop on Hot Topics in Networks*. ACM, Irvine, 2006.

Macilotti G. (2011) Il contrasto alla pedopornografia online: esperienze italiane e francesi a confronto. *Rivista di Criminologia, Vittimologia e Sicurezza*, V(1), 81–107.

Maioli C. (2004) Dar voce alle prove: elementi di informatica forense. *In:* Pozzi P., Masotti R., Bozzetti M. (eds.) *Crimine virtuale, minaccia reale. ICT Security: politiche e strumenti di prevenzione*. FrancoAngeli, 66–74.

Maioli C., Sanguedolce E. (2012) *I "nuovi" mezzi di ricerca della prova fra informatica forense e L. 48/2008.* Altalex, 07 maggio 2012. *http://www.altalex.com/index.php?idnot=18096*.

Malzer E., Poisel R., Tjoa S. (2013) Evidence and cloud computing: The virtual machine introspection approach. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 4(1), 135–152.

Marcella A., Greenfield R. (2002) *Cyber Forensics: A field manual for collecting, examining and preserving evidence of computer crimes*. Auerbach.

Marturana F., Tacconi S. (2013) Il digital forensics nel contest del cloud computing. *In:* Attanasio A., Costabile G., eds. *IISFA Memberbook 2012*. Experta. 123–151.

Mason S. (2008) *International Electronic Evidence*. British Institute of International and Comparative Law.

Mellars B. (2004) Forensic examination of mobile phones. In *Digital Investigation*, 1, 266–272.

Mengoni E. (2008) *Delitti sessuali e pedofilia*. Giuffrè.

Milner C., O'Donnel O. (2007) *Child pornography. Crime, computers and society*. Cullompton.

Nelson B., Phillips A., Enfinger F., Steuart C. (2009) *Guide to computer forensics and investigation*. 4th edition. Cengage learning.

Novario F. (2009) Pornografia minorile e file sharing: l'influenza della tecnologia informatica sull'asse probatorio. *Diritto penale e processo, 10/2009*, 1290–1292.

Ost S. (2009) *Child pornography and sexual grooming*. Cambridge.

Petrone L., Troiano M. (2005) *E se l'orco fosse lei? Strumenti per l'analisi, la valutazione e la prevenzione dell'abuso al femminile*. Franco Angeli.

Picotti L. (2008) La ratifica della convenzione cybercrime del Consiglio d'Europa: profili di diritto penale sostanziale. In *Diritto penale e processo*, 6/2008, 700–716.

Picotti L. (2008) Ratifica della convenzione cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo. In *Diritto penale e processo*, 5/2008, 437–448.

Pistorelli L. (2006) Colmate le lacune della pregressa disciplina. In *Guida al diritto*, 9.

Quayle E., Taylor M. (2003) *Child pornography: an Internet crime*. Routledge.

Rao S., Sun X., Torres R. (2007) DDoS Attacks by Subverting Membership Management in P2P Systems. In *Third IEEE Workshop on Secure Network Protocols*, Beijing, China, October 2007.

Salvadori I. (2011) Los nuevos delitos informáticos introducidos en el Código Penal español con la ley orgánica n. 5/2010. Perspectiva de derecho

comparado, in Anuario de Derecho Penal y Ciencias Penales. In *Anuario de derecho penale y ciencias penales*, LXIV(1), 221–252.

Salvadori I. (2010) Legal problems of possession and viewing child pornography in the Internet. *In:* Herczeg J., Hilgendorf E., Grivna T., eds. *Internet kriminalität und die neuen Herausforderungen der Informationsgesellschaft des 21*. Jahrunderts.

Salvadori I. (2010) Possesso di pornografia infantile, accesso a siti pedopornografici, child-grooming e tecniche di anticipazione della tutela penale. *In:* Ruggieri F., Picotti L., eds. *Nuove tendenze della giustizia penale di fronte alla criminalità informatica*. Giappichelli, 20–31.

Sarzana C. (2008) La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa. In *Diritto penale e processo*, 12/2008, 1562–1577.

Signorile O. (2009) Computer Forensics Guidelines: un approccio metodico-procedurale per l'acquisizione e analisi delle digital evidence. In *Ciberspazio e Diritto*, 2, 197–209.

Stahl A., Ulges A. (2011) Automatic detection of child pornography using color visual words. In *Proceedings of the 2011 IEEE International Conference on Multimedia and Expo, ICME '11, IEEE Computer Society*, 1–6.

Tate T. (1990) *Child pornography: An Investigation*. Methuen.

Tirelli L.A. (2008) *La répression pénale des consommateurs de pédopornographie á l'heure de l'Internet*. Schulthess.

Tonini P. (2013) *Diritto processuale penale. Manuale breve*. Giuffrè.

Tonini P. (2009) Documento informatico e giusto processo. In *Diritto penale e processo*, 4/2009, 401–406.

Trocchi F. (2012) Computer forensics e procedure standardizzate. *In:* Carretta P., Cilli A., Iacoviello A., Grillo A., Trocchi F. *L'acquisizione del documento informatico. Indagini penali e amministrative*. LaurusRobuffo. 69–105.

Stahl A., Ulges A. (2011) Automatic detection of child pornography using color visual words. In *Proceedings of the 2011 IEEE International Conference on Multimedia and Expo, ICME '11, IEEE Computer Society*, 1–6.

United States General Accounting Office (2003) *File-sharing programs - peer-to-peer networks provide ready access to child pornography*. Online *http://www.gao.gov/new.items/d03351.pdf*.

Vacca J. (2005) *Computer forensics. Computer Crime Scene Investigation*. Charles River Media.

Venturini S. (2012) Sequestro probatorio e fornitori di servizi telematici. *In:* Luparia L., ed. *Internet Provider e giustizia penale*. Giuffrè. 107–140.

Sorgato A., Vittorini Giuliano S. (2009) *Reati su soggetti deboli. Percorsi giurisprudenziali*. Giuffrè.

Vaciago G. (2012) *Digital Evidence*. Giappichelli.

Walden I. (2007) *Computer crimes and digital investigations*. Oxford University Press.

Wang C., Chiu C. (2011) Copyright protection in p2p networks by false pieces pollution. In *Lecture Notes in Computer Science*, 6906, 2011, 215–227.

Willassen S. (2005) Forensic Analysis of Mobile Phone Internal Memory. *In:* Pollitt M., Shenoi S. (eds.) *Advances in Digital Forensics - IFIP International Conference on Digital Forensics, National Center for Forensic Science*, 191–204.

Zeno Zencovich V. (1998) La pretesa estensione alla telematica del regime della stampa: note critiche. In *Il diritto dell'informazione e dell'informatica*, Giuffrè, 15

Altra documentazione e risorse web

- ISO/IEC 27037:2012 — Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence
- *http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf*
- *http://www.marcomattiucci.it/lab.php*
- *https://www.sandvine.com/downloads/general/global-internet-phenomena/2013/sandvine-global-internet-phenomena-report-1h-2013.pdf*
- *http://www.readwriteweb.com/archives/p2p_growth_trend_watch.php*
- *https://www.iwf.org.uk/assets/media/annual-reports/annual_report_2013.pdf.pdf*