INFORMATICA GIURIDICA
collana del CIRSFID

6

INFORMATICA GIURIDICA
collana del CIRSFID

La collana ha l'obiettivo di accogliere scritti scientifici che affondino temi di informatica giuridica con originalità, innovazione, interdisciplinarietà. Ospiterà lavori dedicati ai diversi aspetti del rapporto tra discipline informatiche e diritto, spaziando dalle tecnologie informatiche per il diritto, alla logica giuridica e al diritto dell'informatica. I lavori possono comprendere riflessioni — di teoria del diritto e dell'argomentazione, bioetica, sociologia e filosofia del diritto — sugli impatti delle tecnologie dell'informazione sul sistema giuridico e sull'attività del giurista.

CIRSFID
Alma Mater Studiorum – Università di Bologna

*Vai al contenuto multimediale*

Il volume è stato pubblicato con il contributo dell'Alma Mater Studiorum – Università di Bologna, Centro Interdipartimentale di Ricerca in Storia del Diritto, Filosofia e sociologie del Di.ritto e Informatica giuridica "A. Gaudenzi – G. Fassò" sui fondi del progetto di ricerca PRIN 2015 "Soggetto di diritto e vulnerabilità: modelli istituzionali e concetti in trasformazione".

Michele Ferrazzano

# Aspetti metodologici, giuridici e tecnici nel trattamento di reperti informatici nei casi di pedopornografia

Aracne editrice

www.aracneeditrice.it
info@aracneeditrice.it



www.gioacchinoonoratieditore.it
info@gioacchinoonoratieditore.it

via Vittorio Veneto, 20
00020 Canterano (RM)
(06) 45551463

ISBN 978-88-255-1699-9



I edizione: ottobre 2018

# Indice

# 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:

— crimini per i quali i sistemi informatici o telematici[2] sono l'oggetto dell'offesa[3];

[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).

— crimini per i quali i sistemi informatici o di telecomunicazione sono lo strumento dell'azione criminale; in questo caso lo strumento tecnologico è utilizzato per "ingannare" l'utente[4] oppure per "agevolare" la commissione di un illecito[5].

Nell'ultimo ventennio si sta assistendo a una continua crescita di 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 digitale: in tutti i casi di omicidio si ricorre ai tabulati telefonici per la geolocalizzazione delle persone memorizzati presso i server delle compagnie di telefonia mobile, in tutti i casi di rapina si ricorre alle registrazioni delle telecamere a circuito chiuso memorizzate su supporti informatici e così via.

L'informatica forense (o *computer forensics*, o *digital forensics*) è la più giovane delle scienze forensi e si occupa di 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 informatica e l'esattezza dei risultati riguardanti la sua elaborazione[8] . A livello generale si tratta di

[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.

[6] BRAGHÒ G., *Le indagini in materia di reati informatici*, in POZZI P. *et alii*. Crimine virtuale, minaccia reale. ICT Security: politiche e strumenti di prevenzione, Franco Angeli, 2004, pp. 33–43.

[7] WALDEN I., *Computer crimes and digital investigations*. Oxford University Press, 2007.

[8] MARCELLA A., GREENFIELD R., *Cyber Forensics: A Field Manual for collecting, examining and preserving Evidence of Computer Crimes*. Auerbach, 2002.

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[9]. 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[10]: 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 pedopornografia, bisogna dimostrare che la detenzione di materiale illecito è da ricondurre ad un'azione consape-

[9] MAIOLI C., *Dar voce alle prove: elementi di informatica forense*, in POZZI P. *et alii*, Crimine virtuale, minaccia reale. ICT Security: politiche e strumenti di prevenzione. FrancoAngeli, 2004, pp. 66–74.

[10] FOURNIER R., LATAPY M., MAGNIEN C., *Quantifying paedophile activity in a large P2P system*, in *Information Processing and Management*, 49(1), 2013, pp. 248–263.

vole da parte dell'utente. Attualmente queste tipologie 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[11] o Autopsy[12]), 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 nella quale 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 di distribuirlo attraverso sistemi informatici e telematici, chi offre o rende disponibile materiale pedopornografico attraverso sistemi informatici e telematici, chi distribuisce o trasmette materiale pedopornografico attraverso sistemi informatici e telematici, chi si procura materiale pedopornografico attraverso sistemi informatici e telematici per sé o per altri, chi possiede materiale pedopornografico[13] in sistemi informatici e telematici o su supporti di memorizzazione digitali. La convenzione di Budapest è stata poi ratificata anche in Italia con la Legge n. 48 del 27 febbraio 2008 e il suddetto articolo ha trovato collocazione nel codice penale negli artt. 600–bis e seguenti.

[11] *https://www.guidancesoftware.com/products/Pages/encase–forensic/overview.aspx*.

[12] *http://www.sleuthkit.org/*.

[13] 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».

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[14], 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.

Il presente lavoro è rivolto a giuristi e informatici che operano nell'ambito della ricerca e in indagini e processi relative al reato di detenzione e divulgazione di materiale pedopornografico, laddove si rende necessario valutare l'evoluzione delle azioni poste in essere con i sistemi informatici oggetto di esame anche al fine di determinare l'effettivo grado di consapevolezza della condotta: in tal senso si affronta l'esame dei file di log di eMule, uno dei principali strumenti per lo scambio di materiale pedopornografico sulle reti peer–to–peer e si propone un tool denominato *emuleforensic* che consente un agevole analisi in tal senso. L'obiettivo è pertanto la definizione di una metodologia specifica per analisi forensi di sistemi informatici coinvolti in procedimenti di pedopornografia. Nell'ambito di tale definizione si rende indispensabile uno strumento software per l'analisi del traffico

[14] FAGUNDES P., *Fighting Internet Child Pornography The Brazilian Experience*, in *Police Chief*, 76(9), 2009, pp. 48–55. EDILTON E., SOUZA J., *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*, 2009, p.p. 108–113.

generato da software di file sharing su reti peer–to–peer, in particolare dei file scambiati e delle intenzioni dell'utente.

Si ringraziano la prof.ssa Monica Palmirani e il prof. Giovanni Sartor di aver ospitato il presente volume all'interno della collana.