UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

DIPARTIMENTO DEI SISTEMI GIURIDICI ED ECONOMICI

DOTTORATO DI RICERCA IN SCIENZE GIURIDICHE

CURRICULUM 11: FILOSOFIA E SOCIOLOGIA DEL DIRITTO (IUS 20)
XXII CICLO

Anno accademico 2010/2011

DIGITAL EVIDENCE:
PROFILI TECNICO-GIURIDICI E GARANZIE DELL'INDAGATO

TUTOR: PROF. ANDREA ROSSETTI

TESI DI DOTTORATO DI
GIUSEPPE E. VACIAGO

INDICE

Premessa

Il mondo digitale interagisce con la giustizia in molteplici segmenti: sempre più numerosi sono i casi in cui esso è sede di reati (dal furto di identità, fino ad arrivare al cyberterrorismo) e non lontani sono i tempi in cui esso sostituirà il tradizionale modo di intendere il processo (questo sta accadendo nel processo civile e presto accadrà anche nel processo penale).

Come Sherlock Holmes nel XIX secolo si serviva costantemente dei suoi apparecchi per l'analisi chimica, oggi nel XXI secolo egli non mancherebbe di effettuare un'accurata analisi di computer, di telefoni cellulari e di ogni tipo di apparecchiatura digitale[1].

In questo lavoro, non sarà esaminato tutto il complesso e molteplice sistema di queste interrelazioni, ma ci si limiterà all'analisi della prova digitale e del complesso sistema di regole e procedure per la sua raccolta interpretazione e conservazione. Nei capitoli che seguono, è stata data particolare attenzione a tre distinti aspetti.

Il primo è quello dell'estrema complessità della prova digitale. La casistica giurisprudenziale, non solo italiana, ha dimostrato come l'errata acquisizione o valutazione della prova digitale possa falsare l'esito di un procedimento e come il *digital divide* sofferto dalla maggior parte degli operatori del diritto (magistrati, avvocati e forze di polizia) possa squilibrare le risultanze processuali a favore della parte digitalmente più forte.

L'irrompere delle tecnologie informatiche sulla scena del diritto penale come nuovo veicolo di prova, ha generato differenti approcci: da un lato vi è il rischio che un atteggiamento troppo fideistico porti a considerare gli *output* di un elaboratore elettronico come verità oggettive e assolute dimenticandosi che la lettura di tali *output* dipende dalla qualità degli *input*, dal processo di

[1] Ralph C. Losey, *Introduction to e-Discovery*, 2009, ABA Publishing, p. 111.

elaborazione usato, nonchè dalle capacità tecniche di chi interpreta tali *output*; dall'altro vi è il rischio che il principio del libero convincimento del Giudice sia inteso come strumento per poter valutare anche le prove digitali raccolte in violazione di criteri scientifici di acquisizione e/o di analisi della stessa[2].

L'approccio adottato nei Paesi di *Common Law* con la sentenza "Daubert", emessa dalla Corte Suprema degli Stati Uniti del 28 giugno 1993 in tema di validazione della prova scientifica costituisce un importante punto di partenza per una corretta valutazione della prova digitale[3]. Tale sentenza indica i seguenti criteri idonei a valutare la validità e l'attendibilità delle prove scientifiche: la controllabilità, la falsicabilità e la verificabilità della teoria posta a fondamento della prova; la percentuale di errore conosciuto o conoscibile; la possibilità che la teoria o tecnica abbia formato oggetto di controllo da parte di altri esperti perché divulgata in pubblicazioni scientifiche; la presenza di *standard* costanti di verifica; il consenso generale della comunità scientifica[4]. Questa sentenza costituisce un'innovazione di portata storica, in quanto la giurisprudenza statunitense, fino a quel punto, aveva come riferimento in materia un precedente

---

[2] Il principio del libero convincimento del giudice nella valutazione della prova trova i suoi presupposti nel combinato disposto degli artt. 192 e 546, comma 1, lett. e), c.p.p.; osserva correttamente G. Canzio che le due norme pretendono, da un lato, che ogni passaggio argomentativo sia giustificato dal Giudice, che "valuta l'elemento di prova dando conto nella motivazione dei risultati probatori acquisiti e dei criteri d'inferenza adottati" e dall'altro che "la sentenza contenga, con la concisa esposizione dei motivi di fatto e di diritto su cui essa è fondata, l'indicazione delle prove poste a base della decisione stessa e l'enunciazione delle ragioni per le quali il giudice ritiene non attendibili le prove contrarie". G. Canzio, *Prova scientifica, ragionamento probatorio e libero convincimento del giudice penale*, in *Dir. Pen. Proc.*, 2003, p. 1193.

[3] *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579, *syllabus* disponibile al seguente URL: http://www.law.cornell.edu/supct/html/92-102.ZS.html). Per un approfondimento si veda: M. Taruffo, *Le prove scientifiche nella recente esperienza statunitense*, in *Riv. trim. dir. proc. civ.*, 1996, p. 219; L. Dixon, B. Gill, *Changes in the Standards for Admitting Expert Evidence in Federal Civil Cases since the Daubert Decision*, 2001, RAND Institute for Civil Justice; D.J. Faigman, D.H. Kaye, M.J. Saks, J. Sanders, *Modern Scientific Evidence. The Law and Science of Export Testimony*, 2002, St. Paul; K.R. Foster, P.W. Huber, *Judging Science. Scientific Knowledge and the Federal Courts*, 1999, Cambridge, M.I.T. Press.

[4] C. Brusco, *La valutazione della prova scientifica*, in *La prova scientifica nel processo penale*, a cura di L. De Cataldo Neuburger, 2007, Padova, Cedam, p. 38.

del 1923 (sentenza "Frey"[5]), che aveva adottato come unico criterio di attendibilità il giudizio della comunità scientifica di riferimento[6].

Un secondo aspetto, diretta conseguenza del primo, è dato dall'importanza che sta assumendo, come inevitabile effetto del procedere di questi mezzi di prova, l'alfabetizzazione informatica di tutti gli attori coinvolti: giudici, pubblici ministeri e avvocati.

Nel Regno Unito, il dibattito sulla prova digitale e sulla sua acquisizione, durante la fase investigativa, sorge agli inizi degli anni '80 del secolo scorso[7]. La *section* 69 del *Police and Criminal Evidence Act* del 1984 stabilisce che un documento generato da un computer non potrà essere ammesso come mezzo di prova a meno non si dimostri che il computer funzioni correttamente e non sia stato utilizzato in modo improprio[8]. Tale disposizione, anche se criticata dalla stessa *Law Commission*[9], è un chiaro esempio di come il Legislatore anglosassone abbia voluto porre dei paletti all'utilizzo indiscriminato della prova digitale, fin dagli albori dello sviluppo dell'utilizzo di massa dell'informatica.

Il Legislatore italiano ha ritenuto necessario dettare alcune modifiche al codice di procedura penale con riferimento all'acquisizione e alla conservazione della

---

[5] *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923) disponibile al seguente URL: http://www.law.ufl.edu/faculty/little/topic8.pdf

[6] Per un'approfondita analisi dei due casi, M. Taruffo, *Le prove scientifiche nella recente esperienza statunitense*, in *Riv. trim. dir. e proc. civ.*, 1996, p. 219; A. Dondi, *Paradigmi processuali ed* "expert witness testimony" *nell'ordinamento statunitense*, *Riv. trim. dir. e proc. civ.*, 1996, p. 261; F. Tagliaro – E. D'aloja – F.P. Smith, *L'ammissibilità della prova scientifica in giudizio e il superamento del Frye standard: note sugli orientamenti negli USA successivi al caso Daubert v. Merrel Dow Farmaceuticals, Inc.*, in *Riv. it. med. leg.*, 2000, p. 719.

[7] Nel 1982 la dottrina inglese afferma: "The effect of the use of computers cannot be left undebated and the need for constructive criticism of the interface between computer industry and the judicial system is apparent for our system of justice to work The gaps... in the law caused by out-of-date statutes should be noted and filled at the earliest opportunity by Parliament"; A. Kelmann e R. Sizer, *The Computer in Court. A Guide to Computer Evidence for Lawyers and Computing Professionals*, 1982, Hampshire, Gower.

[8] M. Zander, *The Police and Criminal Evidence Act 1984*, 2010, Sweet & Maxwell Ltd, p. 182.

[9] Le principali critiche alla *Section 69* del Police and Criminal Evidence Act riguardano sostanzialmente il fatto che la norma non chiarisce adeguatamente cosa si intenda per utilizzo improprio del computer, alla luce del fatto che i progressi nella tecnologia informatica rendono sempre più difficile certificare il corretto utilizzo di un personal computer. Per un approfondimento si veda la relazione della Law Commission dal titolo *Evidence in Criminal Proceedings Hearsay and Related Topics*, disponibile al seguente URL: http://www.lawcom.gov.uk/docs/lc245.pdf.

prova digitale, solo nel 2008 attraverso la legge di ratifica della Convenzione Cybercrime del 23 novembre del 2001. Nel secondo capitolo saranno descritte, alla luce di tale modifica legislativa, le cinque fasi dell'investigazione digitale (individuazione, acquisizione, conservazione, analisi e presentazione), esaurite le quali, la *digital evidence* potrà essere validamente introdotta all'interno del procedimento penale.

Il terzo e ultimo aspetto, ma non per questo meno importante, è costituito dall'analisi degli effetti pregiudizievoli che un'indagine digitale condotta in modo invasivo (soprattutto ove siano adottate tecniche in grado analizzare a distanza il contenuto dell'*hard disk*), potrebbe avere sul diritto di difesa riconosciuto all'indagato e all'imputato (ad esempio, il diritto al contraddittorio nella formazione della prova o il diritto di non rendere dichiarazioni autoincriminanti) e su alcuni diritti fondamentali dell'individuo (ad esempio il diritto alla riservatezza o il diritto alla segretezza della corrispondenza).

Il domicilio virtuale di ogni individuo, esattamente come quello fisico, merita la massima tutela: la differenza fondamentale, tuttavia, è che, mentre il domicilio fisico ha una precisa collocazione geografica, quello virtuale sempre più spesso non coincide con l'*hard disk* presente nel computer dell'indagato. La tendenza, sempre più diffusa, di utilizzare sistemi di archiviazione dati ubicati fuori dal territorio nazionale, genera molto spesso conflitti di giurisdizione e pone problemi sulla possibile legge applicabile. Il rispetto del diritto di difesa e dei diritti fondamentali dell'individuo nonchè le regole sulla giurisdizione, costituiscono indubbiamente una delle sfide più importanti che il "giurista telematico" dovrà affrontare nei prossimi anni.

Per poter affrontare compiutamente il presente lavoro, infine, non è stato possibile prescindere dagli studi e dalla *case-law* statunitense in tema di *digital evidence* e di *digital forensics*. Basti pensare che, nei paesi di *common law,* tali

temi sono stati elaborati dalla giurisprudenza e dalla dottrina da più di trent'anni e, pertanto, diventa di fondamentale importanza studiare la loro esperienza.

CAPITOLO I – INTRODUZIONE ALLA DIGITAL FORENSICS

1. La prova digitale

Tra le varie definizioni di prova digitale adottate a livello internazionale meritano di essere ricordate quella della International Organization on Computer Evidence (IOCE)[10] secondo la quale la *electronic evidence* "è un'informazione generata, memorizzata e trasmessa attraverso un supporto informatico che può avere valore in tribunale"[11] e quella adottata dallo Scientific Working Group on Digital Evidence (SWGDE)[12] per cui costituisce *digital evidence* "qualsiasi informazione, con valore probatorio, che sia o meno memorizzata o trasmessa in un formato digitale"[13].

Stephen Mason[14] osserva correttamente che i termini *electronic evidence* e *digital evidence* sono spesso usati impropriamente come sinonimi, anche se la *digital evidence* costituisce un sottoinsieme della *eletronic evidence* che ha un valore più ampio in quanto comprenderebbe anche tutti i dati in formato analogico (*analogue evidence*). Ne sono un esempio le audio e video cassette, le pellicole fotografiche e le telefonate compiute attraverso la rete pubblica. Tutte queste prove possono essere "digitalizzate", ma non nascono in formato digitale.

---

[10] IOCE è un'organizzazione internazionale costituita nel 1998 con l'obiettivo di creare un luogo di dibattito, di confronto e di scambio di informazioni tra le forze dell'ordine di tutti gli Stati aderenti. Ulteriore obiettivo è quello di redigere delle linee guida per le procedure di acquisizione della prova digitale in grado di garantire che una prova digitale raccolta in uno Stato sia ammissibile anche nello Stato richiedente.

[11] Definizione adottata da IOCE nel 2000: "Electronic evidence is information generated, stored or transmitted using electronic devices that may be relied upon in court".

[12] SWGDE è un'organizzazione internazionale costituita nel 1998, che raccoglie tutte le organizzazioni attivamente coinvolte nel settore della prova digitale e nel settore multimediale al fine di promuovere la cooperazione e di garantire la qualità nel settore della ricerca della prova digitale.

[13] Definizione adottata nel 1999 da SWGDE, all'interno del documento, *Digital Evidence: Standards and Principles*, disponibile al seguente URL: http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm.

[14] Stephen Mason è un avvocato inglese, fondatore della rivista *Digital Evidence and Electronic Segnature Law Review* e membro della IT Law committee of the Council of Bars and Law Societies of Europe.

Sulla base di queste considerazioni, egli definisce la prova elettronica "l'insieme di tutti quei dati inclusi quelli derivanti dalle risultanze registrate da apparati analogici e/o digitali) creati, processati, memorizzati o trasmessi da qualsiasi apparecchio, elaboratore elettronico o sistema elettronico, o comunque disseminati a mezzo di una rete di comunicazione, rilevanti ai fini di un processo decisionale"[15].

A livello legislativo è interessante notare che, su una ricerca effettuata all'interno di 16 Stati europei[16], non è stata rilevata nessuna definizione di prova elettronica e/o digitale. Solo negli ordinamenti di alcuni Stati si riscontrano dei riferimenti alla prova elettronica: secondo il codice di procedura civile finlandese, i supporti cartacei e quelli digitali costituiscono indistintamente "motivi che supportano l'azione"[17]; il già menzionato *Police and Criminal Evidence Act* inglese definisce la prova digitale come "l'insieme di tutte quelle informazioni contenute all'interno di un computer".

I risultati di questa ricerca mostrano, inoltre, come in tutti gli Stati vi sia una sostanziale equiparazione tra documento cartaceo e documento informatico, tra firma autografa e firma digitale e tra posta tradizionale e posta elettronica.

In Italia, l'art. 1 lett. p) del D.lgs. 82/05, anche denominato "codice dell'amministrazione digitale" definisce documento informatico qualsiasi "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti". Tramite la legge di ratifica della Convenzione di Budapest (legge 48/08), inoltre, è stata abrogata l'aporia normativa esistente nel nostro ordinamento, che vedeva la compresenza, accanto alla definizione appena citata, di quella contenuta

[15] S. Mason, *Electronic Evidence. Discovery & Admissibility*, 2007, LexisNexis Butterwoorths, par. 2.03.: "Electronic Evidence: data (comprising the output of analogue evidence devices or data in digital format) that is created, manipulated, stored or communicated by any device, computer or computer system or transmitted over a communication system, that is relevant to the process of adjudication".

[16] La ricerca è stata effettuata sui seguenti paesi: Austria, Belgio, Danimarca, Finlandia, Francia, Germania, Grecia, Olanda, Irlanda, Italia, Lussemburgo, Portogallo, Romania, Spagna, Svezia e Inghilterra. Per ulteriori informazioni, F. Insa, *The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime—Results of a European Study*, in *Journal of Digital Forensic Practice*, 2006, p. 285.

[17] Legal Proceedings Code of Finland, Chapter 17, Section 11b.

nell'art. 491-*bis* c.p. con la quale si intendeva per documento informatico qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli[18]

Questa nozione faceva riferimento alla materialità del supporto informatico contenente dati o informazioni aventi efficacia probatoria. Oggi, dunque, possiamo definire documento informatico qualsiasi *file* avente un *quid* rappresentativo espresso in linguaggio binario: un testo, un'immagine, un suono, e, dunque, anche le pagine *web* o e-mail.

Paolo Tonini ha efficacemente evidenziato come la rappresentazione del fatto è la medesima sia essa incorporata in uno scritto o in un *file.* Quello che cambia è soltanto il metodo di incorporamento su base materiale. Se il *file* di testo viene stampato su carta, siamo di nuovo dinanzi ad un documento "tradizionale", che esplicita in modo visibile il contenuto del documento informatico. Dunque la differenza tra i due concetti (documento tradizionale e documento informatico) sta tutta nel metodo di incorporamento, e non nel metodo di rappresentazione. I metodi di incorporamento, sempre secondo Tonini, si possono dividere in due categorie fondamentali: quella analogica e quella digitale. L'incorporamento analogico è "materiale" nel senso che la rappresentazione non esiste senza il supporto fisico sul quale è incorporata. Ad esempio, su di uno scritto si opera la cancellazione, resta comunque traccia della manipolazione. Attraverso il metodo digitale, invece, una rappresentazione è incorporata su di una base "materiale mediante grandezze fisiche variabili": si tratta di una sequenza di *bit*. L'incorporamento digitale ha, dunque, la caratteristica dell'immaterialità, poiché

[18] L'attuale formulazione dell'art. 491-*bis* c.p. come modificato dalla legge 48/08 recita: "Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private".

la rappresentazione esiste indifferentemente dal tipo di supporto fisico sul quale il dato informatico è incorporato[19].

Negli Stati Uniti, Eoghan Casey[20], ha definito la prova digitale come "qualsiasi dato digitale che possa stabilire se un crimine è stato commesso o che può fornire un collegamento tra il crimine e chi l'ha commesso"[21].

Nel Regno Unito, Stephen Mason[22] ha classificato la prova digitale in tre diverse categorie:

- la prova creata dall'uomo: è tale ogni dato digitale che figuri come il risultato di un intervento o di un'azione umana. Questo può essere di due tipi: *human to human*, come ad esempio uno scambio di e-mail, che presuppone un'interazione tra due individui e *human to PC*, come ad esempio la redazione di un documento attraverso un software di videoscrittura. Da un punto di vista probatorio sarà indispensabile dimostrare che il contenuto del documento non sia stato alterato e che le dichiarazioni in esso contenute possono essere considerate rispondenti al vero;

- la prova creata autonomamente dal computer: ogni dato che figuri come il risultato di un processo effettuato da un software secondo un preciso algoritmo e senza l'intervento umano (esempi possono essere i tabulati telefonici o i *file* di *log*). Da un punto di vista probatorio è, in questo caso, necessario dimostrare che il software che ha generato questo risultato abbia funzionato correttamente e, ovviamente, che la prova non abbia subito alterazioni dopo che è stata prodotta;

- la prova creata sia dall'essere umano che dal computer: ogni dato che risulta essere il frutto di un contributo umano e di un calcolo generato e memorizzato da

---

[19] P. Tonini, *Nuovi profili processuali del documento informatico*, in *Scienza e processo penale: linee guida per l'acquisizione della prova scientifica*, a caura di L. De Cataldo Neuburger, 2010, Padova, Cedam, p. 427.

[20] Eoghan Casey ha conseguito una laurea in Ingegneria Meccanica presso la Berkeley University, e un Master in "Educational Communication and Technology" alla New York University ed è il direttore della rivista "International Journal of Digital Forensics e Incident Response".

[21] E. Casey, *Digital Evidence and Computer Crime*, 2004, Second edition, Elsevier, p. 12: "*Digital evidence: any data stored or transmitted using a computer that support or refuse a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi*".

[22] S. Mason, *op. cit.*, par. 2.03.

un elaboratore elettronico (un esempio può essere un foglio di calcolo elettronico dove i dati vengono inseriti dall'essere umano, mentre il risultato viene calcolato dal computer). Da un punto di vista probatorio, sarà necessario dimostrare sia la genuinità dei contenuti immessi dall'essere umano sia il corretto funzionamento dell'elaboratore elettronico.

Se dal 1992, data in cui Collier e Spaul introducono il tema delle modalità di acquisizione della prova digitale come categoria autonoma nella dottrina statunitense[23], la disciplina ha avuto un processo espansivo senza soluzioni di continuità, mai come ora si sente la necessità di una definizione chiara del concetto di *digital evidence*.

2. La Digital Forensics negli Stati Uniti

La maggior parte delle pubblicazioni scientifiche fino ad ora scritte in materia, hanno utilizzato il termine "computer forensics"; tale termine venne coniato nel 1984, quando il *Federal Bureau of Investigation* (FBI) elaborò il progetto *Magnetic Media Program*, divenuto qualche anno *Computer Analysis and Response Team* (CART)[24].

A distanza di quasi trent'anni, Ken Zatyko, docente della John Hopkins University è uno dei primi autori che ha preferito utilizzare il sintagma 'digital forensics', invece che 'computer forensics'[25].

Ritengo più appropriata la scelta del sintagma digital forensics, in quanto le analisi forensi sul dato digitale riguarderanno sempre di meno il personal computer e sempre di più altre tipologie di supporti (*smartphone*, lettori mp3,

[23] P.A. Collier, B.J. Spaul, *A Forensic Methodology for Countering Computer Crime*, in 32 *J. For. Sc.*, 1992, p. 27.

[24] Il progetto CART era costituito da un gruppo di specialisti nell'indagine delle informazioni contenute negli elaboratori. Ulteriori informazioni sul team di lavoro sul progetto CART sono disponibili all'URL: http://www.fbi.gov/hq/lab/org/cart.htm e all'interno del volume *Handbook of Forensic Services*, 2007, disponibile al seguente URL: http://www.fbi.gov/hq/lab/handbook/forensics.pdf.

[25] K. Zatiko, *Commentary: Defining digital forensics*, in Forensic Magazine, 2007, disponibile al seguente URL: http://www.forensicmag.com/node/128.

console di videogiochi, navigatori satellitari) e di risorse *hardware* o software distribuite in remoto ("cloud computing"), dove sono normalmente archiviati i dati utili ad un indagine.

Basti pensare che oggi uno smartphone contiene molto spesso le medesime informazioni utili ad un'indagine che potrebbero essere contenuto da un personal computer. In quest'ottica, il termine *computer forensics* potrebbe essere riduttivo e non comprendere tutte le categorie in cui viene archiviato il dato digitale.

Eugene Spafford[26], uno dei padri della materia, è il primo a comprendere questo problema e propone di creare tre distinte categorie di analisi del dato digitale:

- *computer forensics* in senso stretto (collegata al computer)
- *network forensics* (collegata alla rete)
- *intrusion forensics* (collegata alla violazione di sistemi informatici).

Questa ripartizione, anche se condivisibile, corre il rischio di essere superata dal progresso tecnologico: come già detto, ciò che sta accadendo è la dilatazione della ricerca dei dati dal piccolo bacino del singolo computer all'oceano della Rete (passaggio alla *network forensics*).

Tuttavia, dal momento che la dottrina maggioritaria preferisce utilizzare il termine *computer forensics* anche per l'analisi di dati digitali che a tale categoria non appartengono, nel prosieguo della trattazione verranno indistintamente utilizzati sia il più tradizionale "computer forensics" sia il più generale ed ampio "digital forensics"[27].

Sgombrato il campo da possibili equivoci terminologici è opportuno ripercorrere le varie definizioni di *digital* e/o *computer forensics* che si sono susseguite negli ultimi anni a livello nazionale e a livello statunitense.

---

[26] B.D. Carrier, E.H. Spafford, *Categories of digital investigation analysis techniques based on the computer history model*, in *Digital Investigation*, 3, 2006, p. 121.

[27] È interessante osservare che nel contesto statunitense, è spesso utilizzato il termine *e-discovery* per connotare l'analisi forense del dato digitale in ambito civilistico, mentre il termine *computer forensics* ha un'accezione prettamente penalistica.

Il *National Institute for Standard and Technology* (NIST) distingue quattro fasi della *computer forensics*: la raccolta, l'esame, l'analisi, la presentazione, tutte riferite alla prova digitale[28].

La raccolta consiste nell'identificazione, etichettatura, registrazione e acquisizione dei dati digitali, nel rispetto di procedure che preservino l'integrità degli stessi.

L'esame consiste nel processo di valutazione del dato digitale attraverso metodi automatizzati e manuali, che preservino l'integrità del dato digitale.

L'analisi consiste nel processo di verifica dei risultati dell'esame dei dati, al fine di ottenere le risposte ai quesiti per i quali è stato raccolto ed esaminato il dato digitale stesso.

La presentazione dei risultati dell'analisi comprende infine la descrizione delle attività compiute e degli strumenti utilizzati, oltre all'eventuale elencazione delle ulteriori operazioni che sarebbero necessarie per completare l'analisi forense.

Nel noto glossario di termini tecnologici (*whatis*) realizzato dal sito Techrarget, la *computer forensics*, anche denominata *cyberforensics*, viene definita come l'attività di ricerca e di analisi sulle apparecchiature digitali finalizzata al reperimento di prove producibili in Tribunale[29].

Questa definizione è analoga a quella proposta durante la Sedona Conference[30] per la quale "la *computer forensics* consiste nell'uso di tecniche specialistiche per recuperare, autenticare e studiare dati elettronici, nei casi in cui è necessario effettuare una ricostruzione dell'utilizzo del computer, un esame dei dati

---

[28] K. Kent, S. Chevalier, T. Grance, H. Dang, *Guide to integrating Forensic Techniques into Indente Response*, 2006, NIST publication, http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

[29] Search Security è uno dei tanti siti che trattano il tema della sicurezza informatica. La peculiarità di tale sito è rappresentata dalla presenza di un glossario di grande utilità: http://whatis.techtarget.com/ al cui interno è presente la citata definizione di *computer forensics* o *Cyberforensics* http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1007675,00.html.

[30] Il Sedona Conference Institute è costituito da un gruppo di giuristi, avvocati, consulenti tecnici che si confrontano su alcuni temi come antitrust, proprietà intellettuale e *computer forensics*, organizzando conferenze a cadenza trimestrale per permettere agli interessati di ragionare insieme sulle prospettive di sviluppo nelle materie oggetto di studio. Per quanto riguarda la *e-discovery*, uno degli ultimi incontri si è svolto nel gennaio del 2010 (http://www.thesedonaconference.org/conferences/20100128).

cancellati e una certificazione della non alterazione di un dato digitale. La *computer forensics* richiede competenze specifiche che vanno al di là della mera raccolta e conservazione dei dati effettuata dall'*end-user* e generalmente richiede il massimo rispetto della catena di custodia[31]".

Ken Zatyko, definendo la *digital forensics* come "l'applicazione della informatica e delle tecniche investigative in ambito legale", ha distinto otto livelli nel processo di "validazione" della prova digitale:

1. Perquisizione da parte dell'autorità procedente.
2. Rispetto della catena di custodia.
3. Validazione del dato digitale attraverso la funzione di *Hash*.
4. Validazione degli strumenti software utilizzati.
5. Analisi del dato digitale.
6. Ripetibilità.
7. Presentazione dei risultati dell'indagine.
8. Eventuale relazione tecnica da parte di un esperto.

È ovvio che il percorso di validazione della prova indicato da Zatyko impone di avere un consulente tecnico che conosca le dinamiche della *digital forensics* ed è importante che si crei una sinergia tra i legali e gli informatici.

Per Ralph C. Losey[32], il vero protagonista della serie televisiva Star Trek è Scotty, il tecnico che solo raramente appare da protagonista sulla scena, ma assicura la presenza di tutti i dati e di tutti i collegamenti al momento della decisione. Per comprendere l'importanza del "ruolo di Scotty", è possibile portare ad esempio il caso Kevin Keithley v. The Home Store.com[33]. In questo caso, la società convenuta aveva realizzato il codice per siti web molto famosi tra cui anche homebuilder.com o realtor.com ed era stata chiamata in causa per aver violato il brevetto di uno dei loro principali clienti (homestore.com).

[31] Per una definizione più approfondita della catena di custodia si rimanda ai prossimi capitoli.
[32] R. C. Losey, *Introduction to e-Discovery*, 2009, ABA Publishing, p. 113.
[33] *Kevin Keithley v. The Home Store.com*, August 12 2008, U.S. Dist. LEXIS 61741 disponibile al seguente URL: http://www.ralphlosey.file.wordpress.com/2008/08/keithley.doc

L'atteggiamento di sufficienza verso la legge, aveva portato la società a dichiarare in accordo con l'avvocato che tutti i dati relativi al sito web erano stati cancellati. Questa affermazione convinse il Giudice Laporte a sanzionare il convenuto per distruzione di prove con una multa di 320.000 dollari, oltre a condannarlo nel merito. Quindici mesi dopo la sentenza di condanna, il nuovo legale insieme al consulente tecnico riuscì a produrre alcuni dei codici sorgente che erano stati cancellati e con questa nuova e più collaborativa strategia evitarono che il Giudice Laporte ordinasse, oltre alla sentenza di condanna, anche la chiusura della società. Il consulente, quindi, che ritrova il codice sorgente, svolge il ruolo di "Scotty" e riconduce Star Trek su una rotta più sicura.

Tuttavia, questo caso non deve portare a un eccesso di fiducia nell'analisi forense del dato digitale: come osserva correttamente John Patzakis[34], legale della Guidance Software, effettuare una copia forense di un *hard disk* di notevoli dimensioni per poi andare ad analizzare tutti i singoli *file* cancellati, senza precisi indizi che consentano all'investigatore di escludere buona parte dei risultati, può portare ad una consulenza tecnica particolarmente onerosa e senza alcun risultato concreto.

Patzakis, in altri termini, raccomanda una ricerca di dati che sia il più possibile precisa e limitata, in quanto più la ricerca è vasta, meno è probabile che vengano trovati dati effettivamente utili all'indagine.

Del resto, in ambito civile, gli Stati Uniti hanno adottato nel 2006 all'interno del Federal Rules of Civil Procedure[35] la regola 26(b)(2)(B) [36] che circoscrive fortemente l'utilizzabilità delle tecniche invasive per la ricerca di dati

[34] John Patzakis è stato per molti anni il legale della *Guidance Software* che ha realizzato *Encase* il software di *digital forensics* più utilizzato a livello mondiale: nel 2008, l'80% delle indagini vengono svolte attraverso questo *software*. R. C. Losey, *op. cit.*, p. 102.

[35] Le *Federal Rules of Civil Procedure* in vigore dal 1938, ma soggette a numerose modifiche nel corso degli anni sono le regole rispettate all'interno dei Tribunali federali dei singoli Stati. In sostanza vi sono due "codici di procedura civile" negli Stati Uniti: quello del singolo Stato e quello federale.

[36] Per una più approfondita analisi della regola 26(b)(2)(B) si veda G.B. Moore, *Federal Rule of Civil Procedure 26(b)(2)(B) and "Reasonable Accessibility": The Federal Courts' Experience in the Rule's First Year*, in *Privacy & Data Security Law Journal*, disponibile al seguente URL: http://www.bmpllp.com/file/1202334716.pdf.

inaccessibili[37]. La regola prevede che "una parte non è tenuta a fornire la prova di una informazione digitale immagazzinata all'interno di un supporto che essa riconosce come non ragionevolmente accessibile per l'eccessivo volume di dati o per i costi di estrazione […]. La Corte può ugualmente ordinare di fornire tale prova, qualora la parte richiedente dimostri di avere delle valide ragioni, nel rispetto dei limiti previsti dalla regola 26(b)(2)(C)"[38].

Uno dei primi casi dove è stata applicata tale regola (Ameriwood v. Lieberman[39]), riguardava un datore di lavoro che fu autorizzato dalla Corte a realizzare una copia forense dell'*hard disk* di un dipendente, perché aveva fornito alla Corte stessa una "valida ragione" (*good cause*) per effettuare tale copia. La "good cause" si verifica, in particolare, nei casi di sospetta sottrazione di prove, come quando una parte sente il dovere di raccontare che un hacker notturno ha cancellato tutti i suoi *file*, o viene misteriosamente smarrito un portatile il giorno prima di un "subpoena duces tecum"[40].

In un altro caso del 2007 (Hedenburg v. Aramark American Food Services[41]), la Corte applicò rigidamente la regola 26(b)(2)(B) e rifiutò l'esecuzione della copia

---

[37] "Specific Limitations on Electronically Stored Information. A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery".

[38] Rule 26(b)(2)(C): "When Required. On motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that: (i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues".

[39] *Ameriwood Industries, Inc. v. Lieberman et al*., 2007 U.S. Dist. LEXIS 93380, E.D. Mo. Dec. 27, 2006, diponibile all'URL: http://www.jenner.com/file/tbl_s69NewsDocumentOrder/FileUpload500/1584/Ameriwood_v._Liberman.pdf.

[40] Negli Stati Uniti un "subpoena duces tecum" corrisponde a una diffida, soggetta a sanzione se non rispettata, emessa da una Corte. In tale diffida è ordinato a una parte di apparire producendo una determinata prova da usare all'interno di un processo.

[41] *Hedenburg v. Aramark American Food Services*, 2007 US Dist. LEXIS 3443, WD Wash. Jan. 17, 2007.

forense richiesta dal datore di lavoro nei confronti computer di un impiegato, per farla esaminare da un esperto forense. L'avvocato sostenne piuttosto superficialmente che indagini di quel tipo "erano ormai piuttosto diffuse" e che "di solito, salta fuori qualcosa di nuovo". Il Giudice respinse questo tentativo, che costituiva, secondo lui, una modalità di "andare illegittimamente a caccia di prove". Conviene ribadire che la regola 26(b)(2)(B) si applica a quelle ricerche in cui la "candela del dato" sarebbe di gran lunga inferiore, come resa, alla complessità e al costo del "gioco della ricerca".

Questa interpretazione è, naturalmente, destinata ad evolversi in funzione della tecnologia: la nascita di *hardware* e software sempre più performanti ed efficaci potrà sicuramente modificare la tendenza delle Corti ad interpretare in modo restrittivo la regola.

Rimane il fatto che, nelle Corti civili statunitensi, prove digitali di particolare complessità sono ammesse con riserva al fine di evitare che esse vengano strumentalizzate per paralizzare i processi.

Eoghan Casey, nel 2004, nel tentativo di definire la *computer forensics*, intesa come insieme delle metodologie e delle regole per le investigazioni digitali in ambito penale, distingue, *in primis*, tra il computer utilizzato "come arma" e il computer come "contenitore di dati" relativi alle attività di chi lo utilizza[42].

Nel primo caso siamo in presenza, secondo Casey, di *computer forensics* in senso proprio, mentre nel secondo si assiste a un semplice impatto della dinamica sociale nei sistemi informativi, che non sempre e non dovunque richiede l'utilizzo di tecnologia "forensics" per la ricerca o la conservazione della prova.

Un'altra distinzione molto importante da evidenziare è quella tra *computer forensics* e *computer security*; quest'ultima rappresenta un'area tradizionale della *Information Technology* e si occupa della sicurezza del dato. Tale disciplina in

[42] E. Casey, *op. cit.*, p. 23.

qualche modo interseca il percorso della *computer forensics*, che quel dato vuole acquisire e interpretare.

La differenza fondamentale è che per la *computer forensics* il dato non va solo protetto, ma interpretato e portato in giudizio e l'operatore deve disporre capacità informatiche e di abilità investigative.

Alcune capacità di base sono comuni agli esperti dei due campi:

- il procedimento di base, ossia l'approfondita conoscenza del computer, è comune ad entrambi;
- l'esperto di *forensics* deve avere, anche, l'intuizione di dove potrebbe trovarsi l'elemento di prova;
- deve anche sapere come conservarla, deve inquadrarla nel contesto dell'indagine e, soprattutto, deve assicurarsi che essa regga in tribunale.

Una data molto importante per la informatica forense è, naturalmente, l'11 settembre del 2001; da quel giorno la *digital forensics* cessa di essere soltanto uno strumento di indagine e assume anche la veste di strumento utilizzato dalle autorità governative per accedere sostanzialmente senza limiti a tutte le attività che potrebbero potenzialmente essere collegate a iniziative terroristiche.

Questo tipo di utilizzo ha generato una pericolosa, ma in parte inevitabile, tensione tra gli operatori della *digital forensic*s e un fronte esteso di "*antiforensics*", rappresentato dai difensori della privacy, ma anche dal variegato mondo degli *hacker*.

3. La Digital Forensics in Italia

Anche la dottrina italiana ha avviato un proprio filone di ricerca intorno alla definizione e ai contenuti della *computer forensics*, concentrandosi solo sulla parte relativa ai profili penali delle indagini telematiche. Si tratta di un lavoro

ancora embrionale e soprattutto meno suffragato da una giurisprudenza consolidata, ma che, comunque, merita il massimo sostegno.

Cesare Maioli definisce la *computer forensics*[43] come "la disciplina che studia l'insieme delle attività rivolte all'analisi e alla soluzione dei casi di criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un computer, diretti a un computer, o in cui il computer può rappresentare comunque un elemento di prova. Secondo lo stesso autore "gli scopi dell'informatica forense sono di conservare identificare acquisire documentare o interpretare i dati presenti in un computer. A livello generale si tratta di individuare le modalità migliori per:

- acquisire le prove senza alterare il sistema informatico in cui si trovano;
- garantire che le prove acquisite su altro supporto siano identiche a quelle originarie;
- analizzare i dati senza alterarli".

Per Marco Mattiucci e Giuseppe Delfinis la 'forensic computing', altro sintagma per indicare la medesima disciplina, si occupa di trattare dati informatici a fini investigativi e/o giudiziari[44]. Il concetto fondamentale cui deve riferirsi la disciplina in esame è quello di "documento informatico", ossia la rappresentazione informatica di atti o fatti giuridicamente rilevanti. Una visione di questo tipo porta gli autori a dare due definizioni della *forensic computing*:

1) "Il processo di identificazione conservazione analisi e presentazione della *digital evidence* (prova legale ottenuta attraverso strumenti digitali).

2) La raccolta e analisi di dati secondo una prassi che ne garantisca la libertà da distorsioni e pregiudizi, cercando di ricostruire dati e azioni avvenuti nel passato all'interno del sistema informatico"[45].

---

[43] C. Maioli, *introduzione all'informatica forenze, in la sicurezza preventiva della comunicazione,* a cura di P. Pozzi, 2004, Torino, Franco Angeli, disonibile all' URL: http://www.jus.unitn.it/users/dinicola/criminologia-ca/topics/materiale/dispensa_4_1.PDF

[44] M. Mattiucci, G. Delfinis, *Forensic Computing*, in *Rassegna dell'Arma dei Carabinieri*, 2, 2006, p. 52.

[45] A. Ghilardini, G. Faggioli, *Computer Forensics*, 2008, Milano, Apogeo, p. 1

Ritengo più corretta la seconda definizione, in quanto chiarisce meglio la necessità che durante l'acquisizione del dato digitale non avvengano alterazioni e manipolazioni.

Da ultimo, un informatico, Andrea Ghilardini, e un giurista, Gabriele Faggioli, definiscono la computer forensics come "la disciplina che si occupa della preservazione, dello studio, delle informazioni contenute nei computer o nei sistemi informativi, al fine di evidenziare prove utili allo svolgimento dell'attività investigativa".

Un nuovo fronte si sta aprendo per il futuro della *digital forensics*. La disciplina non potrà essere circoscritta all'aspetto tecnologico, ma dovrà aprirsi alla considerazione di tutti gli aspetti legali interconnessi.

- il problema dell'aggiornamento delle tecnologie di ricerca, che rischiano di diventare obsolete con conseguente perdita di una grande quantità di dati;
- il problema della "proceduralizzazione certa" nell'acquisizione e nell'utilizzo della prova informatica;
- il problema della privacy e della sua interconnessione (specie dopo l'11 settembre) con l'analisi digitale;

Lo studio in campo penale di questa nuova disciplina non può prescindere:

- da un lato, dal tema della congruità dei nuovi mezzi di prova rispetto ai valori fondamentali dell'ordinamento
- dall'altro quello dell'idoneità delle singole attrezzature e dei singoli protocolli applicativi a garantire i diritti della difesa.

Nel prossimo paragrafo prima di analizzare alcuni degli aspetti tecnici e processualpenalistici della materia, porteremo due esempi che dimostrano quali effetti negativi può avere il mancato rispetto delle regole della *digital forensics*.

4. Il caso Amero

Come è stato ampiamente descritto nei precedenti paragrafi, la prova digitale è infinitamente più complessa di qualunque altra fonte di prova. Il caso Amero costituisce, al riguardo, un caso di scuola[46].

Julie Amero, una supplente della Kelly School di Norwich nel Connecticut venne condannata per aver mostrato in classe a ragazzi minori di 16 anni immagini pornografiche.

Questi i fatti: alle 7.30 del 19 ottobre 2004, l'insegnante di ruolo Matthew Napp, prima di assentarsi per un corso di formazione, si accertò che tutto fosse predisposto per la lezione affidata al suo sostituto, Julie Amero. Egli impostò, con la propria password, il computer utilizzato per segnare le presenze dei ragazzi secondo la procedura adottata dalla scuola, in quanto non era possibile per i supplenti avere un proprio *account* all'interno dei computer della scuola. Verso le 8 del mattino Julie Amero, dopo essere entrata in classe, chiese a Matthew Napp, di restare in classe per consentirle di andare in bagno, ma al suo ritorno non lo trovò più e notò, invece, due ragazzi davanti al computer. La supplente invitò i ragazzi a lasciare la cattedra e iniziò la sua lezione, che durò dalle 8.30 fino alle 14.30. Durante buona parte della mattinata, immagini "inadatte ai ragazzi" apparvero come *pop-up*[47] all'interno del personal computer, ma Julie Amero non fu in grado di arrestare l'elaboratore. Durante il processo, Julie Amero dichiarò che ogni volta che cercava di chiudere la finestra *pop-up*, attraverso il comando appropriato, si aprivano nuove finestre. È inutile dire che, per chi ha una sufficiente compentenza del mondo della Rete, questo fatto è riconducibile a una particolare tecnica di *DNS hijacking* definita

[46] Superior Court, New London Judicial District at Norwich, GA 21; 3, 4 and 5 January 2007 (Docket number CR-04-93292). Il caso è stato ampiamente descritto da S. Mason, *International Electronic Evidence*, British Institute of International and Comparative Law, 2008, p. xxxvi, disponibile all' URL: http://www.stephenmason.eu/wp-content/uploads/2009/06/stephen-mason-editor-international-electronic-evidence-introduction.pdf.

[47] Per *pop-up* si intende una particolare visualizzazione di una pagina web che si apre automaticamente quando viene aperta una nuova finestra dal *browser*. La finestra *pop-up* viene spesso generata da un *JavaScript*, ma esistono altri mezzi per ottenere lo stesso risultato.

mousetrapping[48], in forza della quale alcuni siti web trattengono i propri visitatori lanciando un'infinita serie di *pop-up*. La giuria della *Superior Court* di *Norwich*, evidentemente, non aveva tale competenza e ha condannato in primo grado Julie Amero per il reato previsto dal *Connecticut General Statute Section 53-21(a)(1)* di offesa alla morale di un minorenne[49].

La modalità con cui si è svolto il dibattimento rappresentano una sorta di *vademecum* di come non si dovrebbero mai svolgere i processi aventi ad oggetto la prova digitale.

Il docente titolare dichiarò nella sua testimonianza che, dopo essere stato informato da uno studente circa fatti accaduti il 19 ottobre 2004, si recò il giorno dopo in aula per controllare quale tipo di attività era stata effettuata sul suo personal computer. Egli, avendo notato che i *temporary cache file* contenevano riferimenti a siti pornografici, avvisò il preside e un esperto informatico che, senza alcun rispetto delle *best practices* di *digital forensics*, stampò alcuni risultati delle ricerche effettuate il giorno precedente, senza alcuna indicazione della data e dell'ora della stampa. Già solo queste prime attività avevano inesorabilmente inficiato la prova, in quanto era stata svolta un'attività di analisi sul computer, prima che venisse effettuata una copia *bit stream* dell'*hard disk* al fine di garantire la non alterazione della *digital evidence*.

Inoltre, la consulenza tecnica della difesa evidenziò chiaramente che il 20 ottobre 2004, ossia il giorno dopo i fatti, alcune cartelle contenente i riferimenti ai siti pornografici erano state rimosse e che nei giorni precedenti al fatto erano state effettuate navigazioni non pertinenti all'attività educativa svolta dal docente

---

[48] Il Prof. Richard Stern della George Washington University Law School ha chiarito in un modo estramamente efficace e anche ironico quali siano le implicazioni giuridiche di tale tecnica. R. Stern, *Mousetrapping and Pagejacking: Introduction*, disponibile al seguente URL: http://docs.law.gwu.edu/facweb/claw/mousetrap1.htm.

[49] *Connecticut General Statute Section 53-21(a)*: "**Injury or risk of injury to, or impairing morals of, children. Sale of children**. (a) Any person who (1) wilfully or unlawfully causes or permits any child under the age of sixteen years to be placed in such a situation that the life or limb of such child is endangered, the health of such child is likely to be injured or the morals of such child are likely to be impaired, or does any act likely to impair the health or morals of any such child […]".

titolare: erano, infatti, stati visionati siti di sport, di home banking e, soprattutto, era stato effettuato il *download* di uno *screensaver* che conteneva un *adware*[50] denominato 'newdot-net' che era, probabilmente, la causa del comportamento anomalo del personal computer[51]. Tale consulenza non fu mai prodotta dall'avvocato di Julia Amero, poiché non era completa il giorno in cui avrebbe dovuto essere depositata.

La polizia giudiziaria che intervenne su segnalazione del preside non fu da meno, in quanto non rispettò alcuna delle procedure previste dalle *guidelines* stabilite dal Dipartimento di Giustizia Statunitense sulla *Forensics Examination of Digital Evidence*[52]: gli agenti di polizia, oltre a non effettuare una copia *bit-stream* dell'*hard disk,* non furono nemmeno chiari sull'effettiva data del sequestro ammettendo, inoltre, che l'ultima data di utilizzo dell'elaboratore risaliva al 26 ottobre 2004. Lo stesso agente di polizia, inoltre, pur sostenendo di essere un esperto di *cybercrime*, non si preoccupò di verificare se il personal computer contenesse al suo interno *spyware* o *adware*, quando in realtà dalla consulenza tecnica della difesa risultò che il *software anti-virus* installato non era stato aggiornato dal marzo dell 2004.

Nel corso delle udienze sia il Pubblico Ministero, sia l'avvocato della difesa non evidenziarono mai tali circostanze e soprattutto non rilevarono che il computer fosse stato utilizzato dal 20 al 26 ottobre, con il conseguente rischio che essenziali elementi di prova avrebbero potuto essere stati alterati in quei giorni.

---

[50] Il termine *adware* indica una modalità di licenza d'uso dei programmi *software* che prevede la presentazione all'utente di messaggi pubblicitari durante l'uso, a fronte di un prezzo ridotto o nullo. Talvolta i programmi *adware* presentano rischi per la stabilità e la sicurezza del computer: alcuni di essi aprono continuamente popup pubblicitari, che rallentano notevolmente le prestazioni della macchina, altri modificano le pagine html direttamente nelle finestre del browser per includere link e messaggi pubblicitari propri, con la conseguenza che all'utente viene presentata una pagina diversa da quella voluta dall'autore.

[51] A livello tecnico si consiglia: M. Carney, M. Rogers, *The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction*, 2004, in *International Journal of Digital Investigation, p. 39.*

[52] *Forensics Examination of Digital Evidence: A Guide for Law Enforcement*, disponibile al seguente URL: http://www.ncjrs.gov/pdffiles1/nij/199408.pdf.

Per completare il tragicomico quadro probatorio, emerse che il computer presentava uno scarto di dodici minuti, ma l'esperto che visionò per primo la macchina non fu in grado di ricordare se tale scarto fosse in ritardo o in anticipo rispetto all'orario esatto. Poiché risultò che il primo sito pornografico venne visionato alle 8.35, si potrebbe ipotizzare che in realtà tale pagina fosse stata aperta alle 8.23 oppure alle 8.47; nel primo caso Amero era fuori dalla classe, nel secondo era in classe. Né la difesa né l'accusa si preoccuparono di approfondire con la Polizia questo punto.

La stessa Amero si lasciò indurre a dichiarare che le immagini pornografiche proseguirono fino alle 14.30, mentre l'analisi dell'*hard disk* dimostrò che esse non furono più riprodotte dopo le 11.13. L'avvocato della difesa non si preoccupò di avvertire la propria assistita, processata a due anni di distanza dall'evento, della gravità di una simile autolesionistica ammissione.

Esiste, a livello nazionale e nel Connecticut, un regolamento sull'uso del computer nelle scuole[53], che proibisce l'accesso a internet se non previo inserimento di un software adeguato a schermare ogni connessione non protetta. È evidente, pertanto, che la prima responsabilità dell'accaduto risiede nella direzione scolastica e nei responsabili educativi sovraordinati. L'unica accusa che può essere rivolta alla povera Julia Amero è la sua incompetenza informatica, pressoché totale, che non le permette neanche di sapere che è possibile disattivare lo schermo senza disconnettere il computer.

Fortuntamente per la supplente della Kelly School di Norwich e per la giustizia, in generale, la New London Superior Court garantì un nuovo processo all'esito del quale venne assolta dai capi di accusa principali che prevedevano una condanna fino a 40 anni di reclusione. Tuttavia, nel novembre del 2008 ottenne un nuovo processo dalla Norwich Superior Court in cui fu condannata al

[53] A livello nazionale: *Children's Internet Protection Act*, disponibile al seguente URL: http://ifea.net/cipa.pdf; a livello Statale, *Connecticut Education Network and E-Rate* (2006-R-0036), disponibile al seguente URL: http://www.cga.ct.gov/2006/rpt/2006-R-0036.htm.

pagamento di 100 dollari di multa e le venne revocata l'abilitazione all'insegnamento.

Indipendentemente dall'esito finale, il processo di primo grado contro Julia Amero, ci permette di riflettere su un punto: se tutto ciò è potuto accadere negli Stati Uniti, indiscussa capitale della cultura informatica, quale sarà lo stato della Giustizia (e della Scuola) in tutti gli altri paesi del mondo?

5. Il caso "Garlasco"

Il 17 dicembre del 2009 il Giudice Vitelli del tribunale di Vigevano assolveva Alberto Stasi dall'accusa di omicidio della fidanzata Chiara Poggi. Il caso, che ha avuto una grande attenzione mediatica, costituisce un altro esempio di quanto possa essere significativo il corretto utilizzo delle tecniche di *digital forensics* per il raggiungimento della verità processuale. Uno degli elementi decisivi del processo, infatti, è costituito dall'*alibi* di Stasi, che egli ricostruisce intorno al proprio personal computer[54].

Questi i fatti: la morte di Chiara Poggi, secondo il medico legale nominato dal Pubblico Ministero, è avvenuta tra le 10.30 e le 12 del 13 agosto 2007. Nei due verbali di sommarie informazioni assunti alle 16 e alle 23.45 dello stesso giorno, Stasi ha ricostruito la mattinata dell'omicidio, senza menzionare il proprio personal computer, dichiarando di:

- essersi svegliato alle 9, dopo essere rincasato la sera prima all'una di notte circa;
- di aver tentato, senza successo, di raggiungere al telefono la fidanzata alle 9.45, alle 10.47, alle 11.37, alle 12.46, alle 13.26 e alle 13.30;
- di aver ricevuto una telefonata della madre alle 9.55;

[54] Per una lettura integrale del testo della sentenza si rimanda al seguente URL: http://static.repubblica.it/laprovinciapavese/pdf/SENTENZA_STASI.pdf

- di aver mangiato alle 13.30 e, preccupato del fatto di non essere riuscito a sentire la fidanzata, di essersi recato con la propria autovettura a casa sua;
- di aver tentato nuovamente a chiamare Chiara Poggi sia sul numero di cellulare sia sul numero di casa durante il tragitto.

Alcuni testimoni hanno confermato le affermazioni di Stasi sul suo ritorno a casa la sera del 12 agosto all'una di notte circa e la sua uscita da casa il 13 agosto alle 13.30 circa per andare dalla fidanzata, mentre è stato possibile riscontrare alcune delle telefonate del giovane sull'utenza di casa e di cellulare della vittima.

Il giorno dopo l'omicidio, Stasi ha consegnato spontaneamente il proprio personal computer e, solo nel verbale di sommarie informazioni del 17 agosto, ha riferito di aver utilizzato il proprio computer per lavorare sulla sua tesi di laurea dalle 10.45 fino alle 12.20[55].

Dal 14 agosto, data in cui l'indagato ha consegnato il proprio personal computer alla polizia giudiziaria, fino al 29 agosto, data in cui i Carabinieri hanno affidato l'elaboratore ai consulenti del Pubblico Ministero[56], sono stati effettuati ripetuti e scorretti accessi a tutto il contenuto del computer in contrasto con i protocolli operativi di indagine forense riconosciuti dalla comunità scientifica.

Nel verbale di consegna del 29 agosto gli stessi Carabinieri hanno segnalato di aver condotto alcune operazioni sul personal computer dell'indagato. La successiva analisi da parte dei consulenti tecnici del Pubblico Ministero ha delineato una serie ancora più completa di violazioni delle regole cardine della *digital forensic*: sono stati riscontrati sette accessi al personal computer di Stasi, la non corretta indicazione dell'accesso al disco esterno, l'installazione di alcune periferiche *USB*, nonché accessi multipli al *file* della tesi di laurea in vari percorsi

[55] Si fa presente che in sede di spontanee dichiarazioni rese ai sensi dell'art. 374 c.p.p. il giorno 22 agosto 2007, l'allora indagato ha nuovamente specificato gli orari di utilizzo del personal computer, dichiarando di aver iniziato alle 9.45 circa e di avere finito alle 12.20.

[56] I consulenti tecnici del Pubblico Ministero provenivano dal Reparto Investigazioni Scientifiche (R.I.S.) di Parma.

di memorizzazione e, infine, fu concesso all'imputato di poter copiare la propria tesi su una *pen drive* al momento della consegna del computer il 14 agosto.
Anche i consulenti tecnici del Pubblico Ministero rilevarono queste scorrettezze, ma affermarono anche che, dalle 10.17 in poi, non vi erano tracce informatiche in grado di dimostrare una presenza umana attiva di fronte al computer, in quanto non erano presenti *file* temporanei[57].
Il consulente tecnico della difesa ha affermato che il *file* della tesi è stato aperto proprio alle 10.17 e che, durante la mattinata, Stasi ha lavorato su tale documento; cionondimeno, a causa delle attività non idonee compiute dai Carabinieri sul personal computer sequestrato, la difesa ha eccepito l'inutilizzabilità come fonte di prova del contenuto del supporto informatico. Il Tribunale, però, ha respinto tale eccezione, nell'udienza del 17 marzo 2009.
Al riguardo si osserva che il documento informatico è, per definizione, volatile, e deve essere maneggiato rispettando alcuni vincoli e procedure: una delle più importanti è quella che impone di formare copie *bit stream* dell'*hard disk*, come si vedrà nel prossimo capitolo, in modo da disporre di una prova non alterabile e genuina.
Nel caso di Garlasco le indagini di polizia giudiziaria compiute dai Carabinieri non configurano né sequestro (dato che il personal computer è stato spontaneamente consegnato), né ispezione, ma una mera ricognizione di dati potenzialmente utili all'Autorità giudiziaria ai sensi del combinato disposto degli artt. 55 e 348 c.p.p.. La ricognizione non si pone come accertamento tecnico ai sensi degli agli artt. 359 e 360 c.p.p., in quanto sono mancati: il quesito del PM, la capacità tecnica degli operatori e una relazione sui risultati raggiunti. Certo è che gli operatori di polizia giudiziaria in oggetto avrebbero dovuto operare in

[57] I *file* temporanei risultano creati attraverso una procedura specifica. Tutte le volte che un'utente attiva la funzione di salvataggio, il programma Microsoft Word genera una copia dello stato del *file* in corso di modifica, generando un *file* temporaneo a partire da esso.

presenza di esperti capaci di suggerire loro tecniche di salvaguardia della prova digitale.

Il mancato rispetto, da parte degli operatori, di protocolli già all'epoca noti, anche se non ancora trasfusi in apposite norme di legge, dimostra che sono stati compiuti gravi errori di metodo, sia pure in perfetta buona fede.

Ne sono derivate, secondo il Giudice, due conseguenze di segno opposto:

- da un lato che anche la migliore indagine forense condotta dai periti delle parti su prove, ormai, irrimediabilmente compromesse, avrebbe comunque trovato l'imputato nella posizione di chi non può veder confermato il suo *alibi*[58];
- dall'altro che anche il Pubblico Ministero non avrebbe trovato conferma alla sua tesi circa la falsità dell'*alibi* dell'imputato, stante l'alterazione del supporto informatico;

Si rendeva perciò necessario, anche a causa del rito abbreviato richiesto dall'imputato, nominare un collegio peritale cui rimandare l'esame del dato informatico potenzialmente compromesso in fase di indagine.

Il collegio appurò che gli interventi dei Carabinieri sul personal computer dell'imputato erano stati quantitativamente devastanti: su 56.000 *file*, 39.000 avevano subito accessi, 1.500 *file* erano stati modificati e 500 nuovi *file* erano stati creati. Un intervento così invasivo sull'elaboratore elettronico da parte di soggetti non esperti ha reso impossibile inferire su aspetti, quali il movente, che avrebbero potuto essere individuati solo attraverso un'indagine svolta correttamente.

I periti, tuttavia, riuscirono a pronunciarsi sull'"alibi informatico"[59] di Stasi dimostrando che, a differenza di quanto sostenuto dai consulenti del Pubblico

[58] Aderisce a questa tesi E. Colombo, *La sentenza del caso di Garlasco e la* computer forensics, in *Ciberspazio e Diritto*, 2010, p. 454.

[59] Si noti come alcuni esperti stiano studiando come un soggetto possa creare un finto "alibi informatico" attraverso l'utilizzo di alcuni software che consentono l'automazione di determinate attività svolte sul

Ministero, egli aveva utilizzato il suo personal computer la sera del 12 agosto. Dal momento che non risultavano presenti *file* temporanei anche nella sera del 12 agosto, se ne dedusse che la tesi dei consulenti del Pubblico Ministero, in forza della quale la mancanza di *file* temporanei potesse comportare l'assenza di attività sulla tesi di laurea, non fosse fondata.

Smontata la tesi dell'accusa, i periti del Tribunale, assistiti da quelli delle parti, hanno provato a cercare un'altra strada per dimostrare l'*alibi* di Stasi e l'hanno trovata grazie ai metadati[60] presenti nel *file* della tesi; il collegio peritale ha, infatti, provato un'evidenza non contestata neppure dai consulenti del Pubblico Ministero, in forza della quale è stato possibile dimostrare che vi è stata un'attività umana ininterrotta sul computer di Stasi fra le 10.17 e le 12.20 del 13 agosto. Tale attività è stata compiuta da "persona cosciente e in situazione di spirito equilibrata". Attraverso tale intuzione del collegio peritale è stato possibile affermare Alberto Stasi aveva lavorato sulla tesi, dalle 10.17 alle 12.20.

Il secondo quesito che si è posto il collegio peritale riguardava la possibilità che l'imputato non fosse in casa mentre stava lavorando sulla tesi. La limitata autonomia del portatile (massimo due ore di attività utilizzando la batteria) ha indotto a escludere tale ipotesi, e le ridotte capacità informatiche di Stasi hanno convinto prima gli esperti e poi il Giudice che non ci si potesse trovare di fronte ad un'astuta falsificazione degli orari da parte di quest'ultimo.

Confermato l'*alibi* per il periodo di permanenza in casa più lungo (9.35, ora di accensione del personal computer; 12.20, ora di messa in *stand-by* dello stesso), sarebbero rimasti due scampoli di mattinata (prima delle 9.36 e tra le 12.46 e le

---

personal computer. V. Calabrò, G. Costabile, S. Fratepietro, M. Ianulardo, G. Nicosia, *L'alibi informatico. Aspetti tecnici e giuridici*, IISFA Memberbook 2010, Forlì, Experta.

[60] I metadati contengono le proprietà memorizzate direttamente all'interno del *file* di *Microsoft Word* a supporto delle procedure applicative. I metadati del *file* della tesi, visualizzabili nella versione di *Microsoft Word* posseduta da Alberto Stasi, contenevano le seguenti informazioni: titolo del documento, parole chiave, commenti, modello del documento, autore dell'ultimo salvataggio, numero di revisione, tempo totale di modifica del *file*, data e ora di ultima stampa, data e ora di creazione del documento, data e ora di ultimo salvataggio, numero di parole, numero di caratteri.

13.26) troppo brevi perché l'imputato potesse essere stato in grado di aver compiuto il breve tragitto fino a casa della vittima e aver consumato il delitto.

A questa deduzione i periti giungono tramite l'analisi forense dei metadati rimasti nel personal computer, nonostante le scorrettezze operative compiute dai Carabinieri sul personal computer dell'allora indagato.

Il caso in esame dimostra come la prova digitale possa essere di grande aiuto nella ricerca della verità processuale, ma anche come sia importante il rispetto di precisi *standard* nella fase investigativa, al fine di evitare che il Giudice, nella valutazione di una prova digitale raccolta in violazione dei criteri scientifici di riferimento, si trovi costretto a forzare l'ambito di operatività dell'art. 192 c.p.p..

CAPITOLO II – LA DIGITAL FORENSICS E LE INDAGINI PENALI

Il fine ultimo di ogni investigazione telematica consiste nel recupero di tutti i dati digitali che possano costituire una prova utilizzabile durante il processo.
Per raggiungere tale fine è necessario:
- individuare il supporto informatico che contiene il dato digitale utile all'indagine utile ad identificare il potenziale criminale;
- acquisire tale dato attraverso l'intercettazione nel caso di flussi di comunicazioni in Rete o attraverso il sequestro e la duplicazione del supporto di memorizzazione dove è archiviato il dato;
- conservare tutti i dati digitali acquisiti e duplicati in un luogo idoneo;
- effettuare, esclusivamente sulla copia del supporto informatico, le opportune analisi che consentano di recuperare le informazioni utili al Pubblico Ministero e all'avvocato, durante la fase delle indagini preliminari, e al Giudice, durante la fase dibattimentale.
- presentare i risultati dell'indagine durante la fase dibattimentale o nella relazione tecnica

In questo capitolo analizzeremo queste cinque fasi confrontando, ove possibile, la disciplina italiana con quella statunitense e con quella di altri paesi europei.

1. Individuazione della digital evidence

1.1 Indirizzo IP e file di log

Quando l'attività investigativa riguarda illeciti commessi in Rete da soggetti non identificati (pedopornografia *on line*, truffe telematiche o anche l'"italianissima" diffamazione *on line*) per l'individuazione dell'autore dell'illecito è necessaria la collaborazione degli *Internet Service Provider*.

I dati digitali che sono di norma richiesti in ambito investigativo possono generalmente dividersi fra quelli che consentono l'identificazione di un potenziale criminale (Indirizzo IP[61]) e quelli che ne determinano la sua attività *on line* (*file* di *log*[62]).

L'indirizzo IP si ottiene generalmente attraverso una richiesta da parte dell'autorità giudiziaria ai *providers* che offrono servizi di posta elettronica e/o ospitano contenuti generati dagli utenti. Una volta ottenuto tale dato, sarà possibile ottenere dai fornitori di connettività l'esatta ubicazione dell'intestatario della fattura da cui è avvenuta la connessione. I *file* di *log*, invece, sono richiesti agli *Internet Service Provider*, in base al tipo di esigenza investigativa.

In Italia tale richiesta è solitamente effettuata sotto la forma di "ordine di esibizione di documenti e atti rilevanti" ai sensi degli art. 256 c.p.p. e art. 132, comma 1 e 3, D.lgs 196/03.

E' interessante notare come, ad oggi, non sia ancora presente a livello nazionale una consolidata prassi circa gli aspetti formali di tale richiesta. Molto spesso, infatti, la richiesta di acquisizione di un indirizzo IP o di un *file* di *log* non proviene dal Pubblico Ministero, ma direttamente dalla Polizia Giudiziaria senza

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

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

alcuna delega da parte dell'autorità giudiziaria. Inoltre, non sempre la Polizia Giudiziaria è competente in materia: basti pensare che molto spesso gli investigatori confondono i *registration data*, ossia i dati di registrazione immessi da un utente che, ad esempio, crea un *account* di posta elettronica con gli indirizzi IP.

L'assenza di una prassi consolidata, ovviamente, non aiuta la collaborazione da parte degli *Internet Service Provider*, soprattutto se stranieri, che si trovano a dover rispondere a richieste molto differenti tra loro provenienti dall'Autorità Giudiziaria, dalla Polizia Giudiziaria e dagli avvocati, che svolgono attività d'indagine difensiva ai sensi dell'art. 132, comma 3, del D.lgs. 196/03[63].

Sul tema merita di essere ricordata una pronuncia del Tribunale di Chieti relativa ad un caso in cui la persona offesa aveva spontaneamente consegnato alla Polizia Giudiziaria i *file* di *log* in grado di dimostrare la colpevolezza dell'imputato. Il Tribunale ha rilevato come "il dato acquisito sia minimo e del tutto insufficiente a fondare qualsivoglia affermazione di responsabilità al di là del ragionevole dubbio". In particolare, secondo il Tribunale, le indagini non sarebbero state sufficientemente approfondite, "poiché ci si limitò ad interpellare la ditta senza alcuna formale acquisizione di dati e senza alcuna verifica circa le modalità della conservazione degli stessi allo scopo di assicurarne la genuinità e l'attendibilità nel tempo". Pertanto, il Tribunale ha ritenuto che mancassero le garanzie di genuinità ed integrità dei *file* di *log* acquisiti, definiti nella sentenza "dati tecnici di particolare delicatezza e manipolabilità", provenienti inoltre dalla stessa persona offesa e quindi da vagliare in modo ancor più rigoroso[64].

---

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

[64] Tribunale Chieti, 30 maggio 2006, n. 139, disponibile in versione integrale al seguente indirizzo: http://www.interlex.it/testi/giurisprudenza/ch060530.htm. Per un commento alla sentenza, si veda F. Cajani, *Alla ricerca del log (perduto)*, in *Rivista di Diritto dell'Internet*, 2006, p. 572.

La conservazione di questi dati da parte degli *Internet Service Provider* e dei fornitori di connettività (altresì definita "data retention"), è di fondamentale importanza sotto il profilo investigativo. L'Europa ha scelto di adottare una disciplina comunitaria molto dettagliata sulla *data retention* (Direttiva 06/24/CE fortemente voluta proprio dall'Italia), che prevede un minimo da 6 mesi fino ad un massimo di due anni di memorizzazione degli indirizzi IP e dei *file* di *log* di tutto il traffico internet[65].

Negli Stati Uniti, invece, anche se non è mancato chi ha ritenuto possibile una regolamentazione in tema di conservazione dei dati[66], non è stata mai emanata una normativa specifica sul tema anche grazie alle numerose e vibranti proteste mosse sia da EPIC[67] (*Electronic Privacy Information Center*) sia EFF[68] (*Electronic Frontier Foundation*). Una delle ragioni di tale forte opposizione è costituita dallo scandalo scoppiato durante l'amministrazione Bush circa l'accordo segreto della National Security Agency con i principali gestori di telefonia statunitensi, finalizzato a creare un *database* di tutte le telefonate e le attività *on line* compiute dai cittadini americani[69].

Ancora prima dell'emanazione della direttiva del 2006, inoltre, vi era chi sosteneva che, una volta introdotto un obbligo di conservazione dei dati, il rischio maggiore sarebbe stato quello di un abuso di tali informazioni anche per

[65] Si noti che in Italia la Direttiva 06/24/CE è stata recepita con il D.lgs. 30 maggio 2008, n. 109 che ha stabilito un periodo di conservazione del traffico telematico pari a 12 mesi.

[66] Da alcuni anni si discute, infatti, della possibilità di adottare una normativa specifica che preveda un determinato periodo di tempo di conservazione dei dati digitali. Tra le varie proposte si veda: http://www.pcmag.com/article2/0,2817,2341476,00.asp. Va ricordato, inoltre, che il *Sarbanes-Oxley Act* del 2002 obbliga a conservare le *e-mail* della propria società per un periodo non inferiore a 5 anni.

[67] Per un approfondimento si veda: http://epic.org/privacy/intl/data_retention.html.

[68] Tra gli ultimi si veda il commento di Eddan Katz, *The Beginning of the End of Data Retention Commentary*, in EFF, 10 marzo 2010, disponibile al seguente URL: http://www.eff.org/deeplinks/2010/03/beginning-end-data-retention.

[69] Per un approfondimento, si veda l'articolo del New York Times del 16 dicembre 2005, J. Risen, E. Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, disponibile al seguente URL: http://www.wired.com/threatlevel/2008/03/times-reporter/.

scopi diversi da quelli per cui tale normativa era stata pensata, come ad esempio la richiesta di dati di connessione in caso di violazione di *copyright*[70].

Le critiche non sono mancate anche in Europa: ne è una dimostrazione il fatto che, ad oggi, ben 16 Stati membri su 27 abbiano espressamente richiesto una dilazione, in alcuni casi fino a 36 mesi dall'emanazione della direttiva, per l'applicazione della stessa nel proprio Stato[71].

La Corte di Giustizia è dovuta intervenire nel marzo del 2009 rigettando il ricorso promosso da Irlanda e Slovacchia, che avevano chiesto l'annullamento della criticata direttiva[72].

La decisione della Corte di Giustizia della Comunità Europea su tale ricorso non ha impedito alla Corte Costituzionale tedesca di dichiarare, nel marzo del 2010, l'incostituzionalità della legge sull'archiviazione di massa di dati telefonici e di navigazione su Internet, derivante dell'implementazione della direttiva.

La Corte ha sostenuto che tale normativa viola la segretezza delle comunicazioni, archivia dati sensibili in mancanza di parametri di sicurezza per i cittadini ed è carente di informazioni precise in merito a come i dati verranno utilizzati[73]. La medesima decisione era stata raggiunta pochi mesi prima dalla Corte Costituzionale Romena[74].

---

[70] Jonathan Zittrain, *Beware the Cyber Cops*, in *Forbes,* 7 luglio 2002, disponibile al seguente URL: http://www.forbes.com/forbes/2002/0708/062.html; a livello europeo si veda P. Breyer, *Telecommunications Data Retention and Human Right: The compatibility of Blanket Traffic Data Retention with the ECHR*, in *European Law Journal*, 2005, p. 365, disponibile al seguente URL: http://www.tkg-verfassungsbeschwerde.de/data_retention_and_human_rights_essay.pdf.

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

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

[73] Per un approfondimento si consiglia il seguente articolo *Konkrete Ausgestaltung der Vorratsdatenspeicherung nicht verfassungsgemäss*, disponibile al seguente URL: http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.html.

[74] Decisione della Corte Costituzionale Rumena n. 1258 dell'8 ottobre 2009: http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html.

Sono chiare le conseguenze di questo scenario da un punto di vista pratico: un ufficiale di Polizia Giudiziaria delegato a svolgere un'indagine dove è coinvolto un *provider* di servizi statunitense, tedesco o rumeno, non potrà mai sapere a priori se i dati che sta cercando siano già stati cancellati oppure se siano ancora memorizzati e utilizzabili per le indagini.

Il contrasto in questo caso è ancora più insanabile, in quanto l'Autorità Giudiziaria e la polizia investita delle indagini, non solo ritengono fondamentale la direttiva sulla *data retention*, ma ne vorrebbero un'applicazione anche per i gestori non europei che offrono servizi in Europa[75].

Una possibile alternativa alla *data retention*, offerta dall'art. 16 della Convenzione Cybercrime sottoscritta a Budapest il 23 novembre 2001, consiste nella "data preservation". L'approccio è radicalmente diverso, in quanto non impone un obbligo a carico dei *provider* e dei fornitori di connettività di conservare tutti i dati di traffico, ma solo di conservare e congelare (da cui il termine *quick freeze procedure)*, i dati qualora sia espressamente richiesto dall'autorità giudiziaria.

L'art. 10 della legge 48/08 ha applicato l'art. 16 della Convenzione Cybercrime stabilendo che il Ministro dell'Interno o, su sua delega, le forze dell'ordine possono ordinare ai *provider*, anche in relazione alle eventuali richieste avanzate dalle autorità investigative straniere, ai *provider* di conservare e proteggere per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni. I provvedimenti adottati sono comunicati entro quarantotto ore al Pubblico Ministero del luogo di esecuzione che, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia. Se è indubbio che la *data preservation*

[75] Occorre rilevare che il 2 aprile del 2008 all'interno della *global Conference Cooperation Against Cybercrime*, gli Stati Membri del Consiglio d'Europa hanno redatto delle linee guida dal titolo: "*Guidelines for the cooperation between law enforcement and internet service provider against cybercrime*". Tale documento ha la finalità di fornire utili indicazioni per regolamentare il rapporto tra forze dell'ordine e *Internet Service Provider*. La versione integrale del testo è presente al seguente URL: http://www.ifap.ru/library/book294.pdf.

è meno invasiva della *data retention*, è altrettanto ovvio che la *data preservation* non consente di poter recuperare informazioni relative ad attività illecite accadute prima della richiesta di "congelamento".

Ma i problemi non sono solo di natura giuridica: anche dopo aver faticosamente ottenuto l'indirizzo IP dinamico[76] del soggetto, l'ufficiale di polizia giudiziaria si trova molto spesso di fronte a due ulteriori problemi di natura tecnica che rischiano seriamente di far indirizzare le indagini nei confronti della "persona sbagliata".

Ogni secondo si collegano ad Internet milioni di persone: gli *Internet Service Provider* e i fornitori di connettività conservano tutte le informazioni di accesso di attività svolta dagli utenti.

È evidente, quindi, che se la polizia giudiziaria effettua una richiesta riferendosi ad una data e ad un'ora errata anche di un solo secondo, le conseguenze a livello investigativo possono essere devastanti. Si correrebbe il rischio di indagare la persona sbagliata, che ha avuto la sola sfortuna di collegarsi un secondo prima o dopo l'autore dell'illecito.

Un altro serio problema è quello dell'occultamento dell'identità. Il più conosciuto sistema per rendere anonima la propria navigazione in Rete è dato dall'utilizzo di un *proxy server*[77]. Ciò non significa che questo sia l'unico. Gli "anonymous remailer", sono dei *server* che ricevono messaggi di posta elettronica e li inviano nuovamente seguendo apposite istruzioni incluse nei messaggi stessi, senza rivelare la loro provenienza originaria[78].

---

[76] Gli indirizzi IP possono essere assegnati in maniera permanente (per esempio un server che si trova sempre allo stesso indirizzo) oppure in maniera temporanea, da un intervallo di indirizzi disponibili. Nel primo caso vengono definiti indirizzi IP statici, mentre nel secondo caso, indirizzi IP dinamici. La grande maggioranza degli utenti della Rete, quando si collega, utilizzerà un indirizzo IP dinamico assegnato dal *Provider* di volta in volta sulla base degli "spazi disponibili".

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

[78] Per un approfondimento sul tema si veda G. Danezis, R. Dingledine, N. Mathewson, *Mixminion: Design of a Type III Anonymous Remailer Protocol*, in *IEEE Security & Privacy*, 2003, disponibile al

Particolarmente diffuse sono poi diverse tecniche di utilizzo fraudolento degli identificativi dell'elaboratore di un soggetto: in questi casi l'autore del comportamento illecito non soltanto nasconde la propria identità, ma addirittura crea le condizioni perché il comportamento sembri apparentemente attribuibile ad un altro utente davvero esistente. L'*hacker* acquisisce l'identificativo e la *password* di un utente ignaro, e si collega in Rete sotto mentite spoglie. L'acquisizione dell'identificativo e della *password* possono avvenire o in via "tradizionale" (riuscendo a carpirne gli estremi direttamente dall'utente o accedendo ad una Rete *wireless* non protetta), ovvero acquisendole per via telematica attraverso l'uso di specifici programmi denominati "trojan horses": si tratta di applicativi apparentemente innocui ed invisibili, che si installano sull'elaboratore con lo scopo di controllare e spiare il funzionamento del sistema, in modo da acquisirne i contrassegni identificativi[79].

1.2 Ispezione

Una volta trovato il luogo dove l'utente si è collegato per commettere l'attività illecita, è necessario individuare il supporto informatico che contiene la *digital evidence* e conseguentemente identificare l'autore dell'illecito.
Tale attività investigativa non è affatto banale: la *digital evidence*, vista la sua immaterialità, può trovarsi praticamente ovunque e assumere molteplici forme. Può essere un'immagine in un telefono, un *file* di testo in una *memory card*, un *record* in un database dipartimentale, un'immagine celata in un *file mp3* e così

---

seguente URL: http://www.mixminion.net/minion-design.pdf. Si vedano anche i progetti TOR (http://www.torproject.org/index.html.it) e Winston Smith (http://pws.winstonsmith.info/).

[79] F. Testa, *Cybercrime, intercettazioni telematiche e cooperazione giudiziaria in materia di attacchi ai sistemi informatici*, Incontro di Studio sul tema "Criminalità organizzata transnazionale: strumenti di contrasto e forme di cooperazione giudiziaria", 6-8 giugno 2005, Roma, p. 10, disponibile al seguente URL: http://appinter.csm.it/incontri/relaz/11794.pdf. Per un approfondimento sul tema si veda il rapporto annuale del CERT (Computer Emergency Response Team), 2006, disponibile al seguente URL: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

via[80]. Ma soprattutto e sempre di più, questa informazione si potrebbe trovare memorizzata "su una nuvola", visto il crescente investimento dei *provider* nel "cloud computing"[81]. Prima di affrontare questo delicato aspetto, tuttavia, è opportuno analizzare gli strumenti "tradizionali" che sono utilizzati a livello nazionale.

Il codice di procedura penale prevede come mezzi di ricerca della prova l'ispezione e la perquisizione. Anche se, nella prassi, l'Autorità Giudiziaria predilige sicuramente il secondo, è opportuno in questa sede soffermarci sul primo, in quanto nell'ambito delle investigazioni digitali potrebbe risultare uno strumento efficace senza essere particolarmente invasivo.

L'ispezione, disposta con un decreto motivato, consente all'Autorità Giudiziaria di percepire direttamente elementi utili alla ricostruzione del fatto e può avere ad oggetto persone, luoghi o cose. Se il reato non ha lasciato tracce o altri effetti materiali o se questi sono scomparsi o sono stati cancellati, dispersi, alterati o rimossi, l'Autorità Giudiziaria descrive lo stato attuale dei luoghi e se possibile quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni[82].

La Suprema Corte è intervenuta confermando che il difensore può assistere all'ispezione, ma non ha alcun diritto di far ritardare l'operazione per consentire la sua partecipazione[83].

Nel corso dell'ispezione l'autorità giudiziaria può ordinare che taluno non si allontani prima che le operazioni siano concluse e può far ricondurre coattivamente sul posto il trasgressore (art. 246 c.p.p.); l'Autorità Giudiziaria può

---

[80] A. Ghilardini, G. Faggioli, *op. cit.*, p. 45.

[81] Per un approfondimento sul tema si veda: UC Berkeley Reliable Adaptive Distributed Systems Laboratory, *Above the Clouds: A Berkeley View of Cloud Computing*, disponibile al seguente URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.150.628&rep=rep1&type=pdf.

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

[83] Cassazione Penale, 23 ottobre 1992, in *Cassazione Penale*, 1994, p. 676.

disporre inoltre che siano effettuati rilievi segnaletici, descrittivi, fotografici ed eventuali altre operazioni tecniche (art. 244 c.p.p.).

Tali attività, inoltre, sono per loro natura irripetibili ed è, pertanto, necessario che i relativi verbali siano dettagliati e che agli stessi sia allegata tutta la documentazione utile al fine di provare la commissione dell'illecito[84]. Il Tribunale di Savona ha assolto con formula piena un soggetto imputato del reato di duplicazione abusiva di software ai sensi dell'articolo 171-*bis* della legge sul diritto d'autore, in quanto l'indagine svolta appariva assolutamente lacunosa, non essendo stata effettuata né la duplicazione delle memorie dei computer, né un sequestro degli stessi, né le fotocopie delle licenze esibite. Le uniche prove erano pertanto costituite dalla relazione tecnica del Pubblico Ministero composta da due sole laconiche righe: "non essendo stata presentata alcuna documentazione comprovante il regolare possesso del software rinvenuto durante l'ispezione e indicato come sprovvisto di licenza d'uso, si conferma quanto precedentemente indicato nel verbale di ispezione"; nonché dal verbale di ispezione stesso che tuttavia non allegava alcuna documentazione attestante l'effettiva duplicazione del software.

Qualora siano adottate delle corrette metodologie operative, l'ispezione potrebbe risultare un utile strumento nel caso di indagini che richiedano l'analisi di materiale informatico[85]. La Polizia Giudiziaria, dopo aver trovato le tracce informatiche del reato commesso, ha la possibilità non solo di redigere il verbale di ispezione, ma anche di acquisire, attraverso una copia *bitstream* del supporto

[84] Tribunale di Savona, 17 gennaio 2004, disponibile al seguente URL: http://www.ictlex.net/?p=459.

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

di memorizzazione, i dati utili alla prosecuzione dell'indagine[86]. La copia *bitstream* è un particolare tipo di duplicazione che preserva anche l'allocazione fisica dei singoli *file* oltre che la loro posizione logica[87].

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

- la creazione di un impronta di *hash*, che permetterà di mostrare, al di là di ogni dubbio, se i contenuti del *file*, oppure del supporto, abbiano subito o meno modifiche;
- l'utilizzo di un "*write blocker*" che consente di bloccare ogni tipo di scrittura sul supporto ispezionato[88].

Tali operazioni sono caratterizzate dall'irripetibilità. Ciò significa che, solo se sono stati utilizzati i metodi di acquisizione idonei a garantire l'integrità e la genuinità dei dati e le garanzie del contradditorio, potranno essere pienamente utilizzati in dibattimento come fonte di prova.

La legge di ratifica della Convenzione Cybercrime (legge 48/08) ha modificato l'art. 244 c.p.p. disponendo espressamente che "in relazione a sistemi informatici o telematici, devono essere adottate misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione".

L'ispezione, particolarmente favorevole per l'indagato che non dovrà subire un eventuale spossessamento dei beni attraverso il sequestro, è un'attività che esige specifiche competenze informatiche ed un'adeguata strumentazione tecnica. Per questa ragione, tale mezzo di ricerca della prova appare consigliabile esclusivamente per reati facilmente identificabili e che impongano uno studio

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

[87] Sul tema si veda A. Ghilardini, G. Faggioli, *op. cit.*, p. 55; per maggiori informazioni sui requisiti tecnici si veda: The Computer Forensic Tool Testing (CFTT), disponibile al seguente URL: http://www.cftt.nist.gov/disk_imaging.htm.

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

superficiale dello strumento informatico. Sarebbe, infatti, molto complesso procedere, in un ragionevole arco temporale, all'analisi di supporti sempre più capienti (in pochi anni si è passati da gigabye ai terabyte) e di cui l'intero contenuto potrebbe risultare utile all'indagine. Basti pensare che, ad oggi, i tempi medi di copia sono di circa 2 giga al minuto: da ciò ne consegue che per un *hard disk* di un terabyte saranno necessarie 8 ore circa per effettuare una *bitstream image*[89].

Non va dimenticato, infine, che, da un punto di vista strettamente processuale, l'irripetibilità dell'ispezione impedirebbe all'indagato di poter effettuare, magari con l'ausilio di un perito di parte, una successiva analisi del supporto informatico ispezionato, lasciando spazio ad eventuali contestazioni sulla genuinità della prova da parte del difensore in sede dibattimentale[90].

1.3 Perquisizione

A differenza dell'ispezione, la perquisizione ha lo scopo di ricercare il corpo del reato o "le cose che ad esso si riferiscono", qualora si ritengano, con "fondati motivi", nascoste sulla persona o in un determinato luogo. La perquisizione locale è, inoltre, disposta anche quando deve eseguirsi l'arresto dell'imputato o dell'evaso e sussistono particolari motivi di urgenza che non consentono l'emissione di un tempestivo decreto di perquisizione[91].

La Suprema Corte ha precisato che per "fondati motivi" non si devono intendere congetture o sospetti, ma "indizi di un certo rilievo" in relazione ad una concreta

---

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

[90] Sul punto si veda F. Cajani, *La Convenzione di Budapest nell'insostenibile salto all'indietro del Legislatore italiano, ovvero: quello che le norme non dicono…*, in *Ciberspazio e Diritto*, 2010, p. 185.

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

figura di reato, previa una corretta individuazione del *thema probandum* della ricerca. Se così non fosse la perquisizione e il conseguente sequestro si "trasformerebbero da mezzo di ricerca della prova in mezzo di acquisizione di una *notitia criminis*, in quanto tale sarebbe inammissibile perché lesivo della libertà individuale *lato sensu*, che trova tutela negli articoli 13 e 14 della Costituzione"[92].

Qualora all'interno dell'indagine fosse necessario ricercare fonti di prova che coinvolgono l'elaboratore elettronico, saranno oggetto della perquisizione anche tutti i supporti ad esso dedicati e quelli contenenti dati potenzialmente utili ai fini dell'indagine.

Non si procede alla perquisizione se la cosa ricercata è consegnata spontaneamente dal soggetto, salvo che si ritenga utile procedervi per la completezza delle indagini.

Prima di iniziare la perquisizione viene notificato il decreto all'interessato che ha facoltà di farsi assistere da persona di fiducia, purché sia prontamente reperibile e sia idonea come "testimone" di un atto del procedimento.

Nella quasi totalità dei casi, il decreto di perquisizione comprende anche quello di sequestro: sebbene, infatti, siano due mezzi di ricerca della prova distinti, è evidente che, una volta trovato il corpo del reato o "le cose che ad esso si riferiscono" diventa necessario impedirne la disponibilità all'indagato al fine di evitare ogni possibile alterazione della prova.

Come nel caso dell'ispezione, la perquisizione richiede che ogni operazione avente ad oggetto lo strumento informatico, sia conforme ad una metodologia operativa che garantisca l'integrità e la genuinità dei dati, affinché non siano possibili contestazioni in sede dibattimentale sulle modalità di acquisizioni della prova avvenute durante le indagini[93].

---

[92] Cassazione Penale, 29 ottobre 1993, in *Cassazione Penale*, 1995, p. 134.

[93] Anche in questo caso è intervenuta la legge 48/08 che ha modificato l'art. 247 c.p.p. sancendo espressamente che: "quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici

Il Tribunale di Bologna, in un'interessante pronuncia in tema di accesso abusivo e danneggiamento a un sistema informatico (artt. 615 *ter* e 615 *quinquies* c.p.), ha dimostrato, tuttavia, uno scarso interesse verso l'utilizzo di tali protocolli[94]. Il caso riguardava un *hacker* che, dopo aver creato un *malware* denominato "Vierika", lo aveva diffuso tramite un noto *provider* a circa 900 utilizzatori. Il *malware*, inviato come allegato di una e-mail, una volta eseguito, andava ad agire sul registro di configurazione del sistema operativo Windows portando al livello minimo le impostazioni di protezione del browser Internet Explorer e inserendo come *home page* del predetto browser una determinata pagina web scelta dall'imputato. Quando l'utente accedeva in Rete, veniva automaticamente scaricato un comando che creava nella prima partizione del primo disco rigido del computer il *file* c:\Vierika.JPG.vbs, contenente la prima parte del codice, producendo un effetto di *mass-mailing*: veniva, infatti, inviata agli indirizzi contenuti nella rubrica di Outlook una e-mail contenente l'allegato sopra descritto, in modo che il malware si potesse autoreplicare. Il Giudice, per emettere la sentenza di condanna, si è fondato principalmente sul verbale di perquisizione e contestuale sequestro, in quanto in quella sede l'indagato aveva ammesso spontaneamente il fatto; inoltre egli aveva personalmente masterizzato un cd contenente i *file* incriminati, consegnandolo alla Polizia Giudiziaria.

Tale modalità operativa, come vedremo meglio nel prossimo paragrafo, non corrisponde, a nessuno dei protocolli scientifici ritenuti idonei a garantire l'effettivo contraddittorio all'imputato e, di conseguenza, la prova avrebbe dovuto essere ritenuta illegittimamente acquisita. Il Giudice, tuttavia, in assenza della allegazione di fatti dai quali si potesse astrattamente desumere verificata nel

---

o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione".

[94] Tribunale di Bologna, 22 dicembre 2005, disponibile al seguente URL: http://www.ictlex.net/?p=516; si noti che tre anni più tardi la Corte di Appello ha riformato parzialmente la sentenza, senza intervenire tuttavia sugli aspetti procedurali, ma limitandosi solo a una diversa qualificazione giuridica del fatto (Corte di Appello di Bologna, 30 gennaio 2008, disponibile al seguente URL: http://www.ictlex.net/?p=692).

caso concreto una qualsiasi forma di alterazione dei dati, ha sostenuto che non fosse suo compito determinare un protocollo relativo alla procedure informatiche forensi; pertanto, in forza del principio della libera valutazione della prova previsto dall'articolo 192 c.p., ha ritenuto alla luce del contesto probatorio complessivo che gli accertamenti compiuti dalla Polizia Giudiziaria fossero pienamente attendibili ed utilizzabili ai fini della decisione.

La dottrina ha criticato tale motivazione poiché di fatto ne è derivata un'inversione dell'onere della prova a carico dell'imputato. Rimane, tuttavia, il dubbio sulla decisione che il Giudice avrebbe adottato, se l'imputato non avesse immediatamente ammesso la sua piena colpevolezza circa i reati contestati.[95]

Il Tribunale di Pescara, diversamente da quello di Bologna, ha ritenuto non attendibili le indagini informatiche svolte dalla Polizia Giudiziaria nel caso di un procedimento relativo al reato di pubblicazioni e spettacoli osceni previsto dall'articolo 528 c.p.: l'imputato era accusato di aver messo in circolazione immagini dal contenuto pornografico senza adottare nessun tipo di restrizione (*password* o altri sistemi) "attraverso apposita strumentazione informatica, *server*, che permetteva il reindirizzamento al sito Internet denominato www.vallecupa.com"[96]. La giurisprudenza in materia, infatti, prevede che il commercio di materiale pornografico, purché realizzato nei confronti di acquirenti adulti, non integra alcuna fattispecie di reato, ove il Giudice di merito accerti che in relazione a tali modalità il comune senso del pudore non risulti offeso[97].

---

[95] L. Lupária, *Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova finale digitale – Profili processuali*, in *Diritto dell'Internet*, 2006, p. 153. e F. Catullo, *Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova finale digitale – Profili sostanziali*, in *Diritto dell'Internet*, 2006, p. 160.

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

[97] Cassazione Penale, Sezione III, 12 maggio 1994, n. 5630.

Le indagini erano consistite nell'identificazione del titolare del sito, tramite il fornitore di servizi di *web hosting* statunitense e dalla stampa di alcune pagine di esso.

Nel corso della perquisizione erano stati rinvenuti su un personal computer utilizzato come server DNS due *file* di *log*, che erano stati acquisiti mediante copia su supporto CD ed un *file* identificabile con il nome "vallecupa.con.dns", contenente il reindirizzamento della pagina web vallecupa.com, allocata presso il server della società "50megs.com". Nessuna immagine relativa al sito vallecupa.com era presente, tuttavia, sul personal computer.

Durante la perizia disposta in dibattimento, il perito ha dovuto concludere di essere impossibilitato ad ogni considerazione, non essendo riuscito ad acquisire le pagine web nel formato digitale, al fine di valutarne contenuto e caratteristiche tecniche ed ha criticato, inoltre, la mancata acquisizione di copia certificata dei documenti informatici, con eventuale sottoscrizione (firma digitale), come previsto dalla normativa tecnica già all'epoca emanata dall'AIPA (Autorità per l'Informatica nella Pubblica Amministrazione, ora CNIPA centro Nazione per l'Informatica nella P.A.), in tema di creazione, diffusione e conservazione della documentazione informatica. Ha rimarcato, infine, la scarsa valenza probatoria delle riproduzioni a stampa (difficilmente classificabili, alla stregua della stessa normativa tecnica, quali "documenti analogici originali"), che, peraltro, riportavano date di consultazione delle pagine all'indirizzo www.vallecupa.com successive all'epoca di commissione del reato.

In questo caso, il Giudice, ritenendo il contesto probatorio insufficiente a fondare una condanna, ha assolto l'imputato per insufficienza di prove ai sensi dell'articolo 530 co. 2 c.p.p..

Se la Polizia Giudiziaria avesse acquisito l'intero sito web in formato digitale e avesse certificato la data dell'acquisizione attraverso alcuni opportuni accorgimenti tecnici (firma digitale del *file*, utilizzo della funzione di *hash*,

videoripresa delle operazioni compiute durante l'acquisizione), avrebbe sicuramente fornito al Giudice degli elementi idonei per valutare diversamente l'intera vicenda. È opportuno segnalare che alcuni informatici italiani hanno recentemente realizzato un *software* denominato hashbot (www.hashbot.com), in cui viene fornita la possibilità gratuita di validare ogni prova digitale reperita in Rete, attraverso l'utilizzo della funzione di hash di cui si parlerà diffusamente nel paragrafo relativo al sequestro della *digital evidence*. L'utilizzo di questo software rappresenta sicuramente una soluzione efficace e sicura alla validazione di prove digitali acquisite in Rete.

1.4 Accertamenti urgenti sui luoghi, cose e persone. Sequestro

Qualora vi sia il concreto rischio che le cose, le tracce e i luoghi pertinenti al reato si alterino e il Pubblico Ministero non possa intervenire tempestivamente o non abbia ancora assunto la direzione delle indagini, gli ufficiali di Polizia Giudiziaria compiono i necessari accertamenti sullo stato dei luoghi e delle cose e, se del caso, sequestrano il corpo del reato e le cose a questo pertinenti[98].
Questa importante facoltà, concessa alla Polizia Giudiziaria ai sensi dell'art. 354 c.p.p., ha un impatto notevole nell'ambito di un'investigazione digitale, poiché può accadere che la prova digitale divenga difficilmente recuperabile nel caso si sia necessario attendere un provvedimento *ad hoc* del Pubblico Ministero. Ad esempio, se durante un accertamento urgente l'elaboratore fosse trovato in funzione, potrebbe essere utile o addirittura indipensabile recuperare tutti i dati volatili presenti all'interno della *RAM*[99], che verrebbero persi con l'arresto del

[98] Anche se rileva marginalmente nell'ambito delle investigazioni digitali, l'accertamento urgente può essere anche nei confronti delle persone. In questo caso, gli ufficiali di Polizia Giudiziaria compiono i necessari accertamenti e rilievi sulle persone.
[99] R.A.M.: acronimo usato nell'informatica per *Random Access Memory*, è il supporto di memoria su cui è possibile leggere e scrivere informazioni con un accesso "casuale", ovvero senza dover rispettare un determinato ordine , come ad esempio avviene per un nastro magnetico. Caratteristica comune a tutti i tipi di *RAM* utilizzati per la memoria principale è quella di perdere il proprio contenuto nel momento in cui viene a mancare la corrente elettrica che le alimenta.

sistema operativo. Allo stesso modo potrebbe essere utile verificare preliminarmente il contenuto dell'*hard disk* attraverso un'attività di *preview,* che è possibile svolgere attraverso una distribuzione *live* dei vari software di *digital forensics,* che saranno descritti nei prossimi paragrafi.

Il legislatore, conscio dell'importanza di questo strumento processuale nelle investigazioni digitali, ha precisato con la legge 48/08 che "in relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità".

Sarà quindi necessario che la Polizia Giudiziaria adotti tutte le necessarie cautele per evitare il rischio di alterare il dato digitale, in assenza di una precisa delega del Pubblico Ministero.

1.5 La disciplina statunitense in tema di "search and seizure"

Gli Stati Uniti costituiscono un modello di confronto particolarmente interessante, in quanto il tema della individuazione e acquisizione della prova digitale è stato oggetto di un'ampia e dettagliata analisi giurisprudenziale.

La fonte primaria che regola tale materia è il quarto emendamento il quale sancisce che: "il diritto dei cittadini ad essere sicuri nelle loro persone, case, carte ed effetti personali contro perquisizioni e sequestri non ragionevoli, non potrà essere violato, e non potranno essere emessi mandati se non sulla base di motivi fondati, sostenuti da giuramenti o solenni affermazioni e con una dettagliata descrizione del luogo da perquisire e degli oggetti da sequestrare"[100].

[100] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause,

Occorre preliminarmente sottolineare che, a differenza della disciplina normativa italiana sui mezzi della ricerca della prova, la disciplina statunitense non distingue tra ispezione, perquisizione e sequestro, ma si limita ad identificare un unico mezzo che comprende la ricerca della prova e il successivo sequestro ("search and seizure").

La norma che regola la disciplina del "search and seizure" della *digital evidence* è la *Rule* 41 delle *Federal Rules of Criminal Procedure*[101], mentre la *Section* 18 U.S.C. §§ 2701-12 dello *Stored Communication Act*[102] si applica in caso di sequestro presso un *provider*.

La *Rule 41* chiarisce che per ottenere un mandato (*warrant)* di perquisizione e sequestro (*search and seizure*) è necessario che l'agente che ha svolto le indagini sottoscriva una dichiarazione (*affidavit*) che dovrà essere sottoposta (*application*) al vaglio di un Giudice competente in materia (*magistrate*). L'*affidavit* deve:

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

Il richiedente deve indicare nell'*affidavit* quali attività di indagini hanno permesso di identificare l'abitazione del potenziale criminale. La giurisprudenza al riguardo ha ritenuto che costituiscano validi presupposti per la concessione del *warrant* l'acquisizione dell'indirizzo IP del soggetto indagato fornito dai

---

supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".

[101] *Rule 41 Federal Rules of Criminal Procedure (Search and Seizure)*: […] "After receiving an affidavit or other information, a magistrate judge — or if authorized by Rule 41(b), a judge of a state court of record — must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device […]". La norma per esteso è disponibile al seguente URL: http://www.law.cornell.edu/rules/frcrmp/Rule41.htm.

[102] *Section* 18 U.S.C. §§ 2701-12 *Stored Communication Act*: "(a) A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction […]". La norma per esteso è disponibile al seguente URL: http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002701----000-.html.

provider[103] o le credenziali delle carta di credito raccolte nel caso di un acquisto *on line*[104].

La descrizione dei dati digitali da sequestrare dovrà essere fatta in modo preciso al fine di evitare che siano sequestrati oggetti non rilevanti[105] e, in ogni caso, dovrà essere limitata agli oggetti per cui è stata ritenuta necessaria tale richiesta. Un precedente storico è quello relativo da due società statunitensi (Solid State Devices e Unisem Internation), indagate per aver fornito al Dipartimento della Difesa semiconduttori non conformi a quanto previsto dal contratto. La Corte di Appello degli Stati Uniti ritenne illegittimo il provvedimento di *search and seizure*, in quanto il *warrant* non era dettagliato e l'attività svolta nella fase di indagine aveva violato i principi del 4° emendamento della Costituzione[106].

Esattamente come accade in Italia, negli Stati Uniti non vi sono chiare indicazioni sull'opportunità di procedere al sequestro del dato digitale attraverso la copia *bit-stream* dell'*hard disk* direttamente nel luogo dove è rinvenuto il supporto informatico, tuttavia nel caso in cui vi sia il rischio che si protraggano le conseguenze del reato o qualora la copia *bit stream* dell'immagine del disco dovesse comportare un eccessivo dispendio di tempo, è necessario il sequestro dell'hardware[107].

In presenza di determinate circostanze, la Corte può ritardare la notifica del *warrant* fino a 30 giorni dopo la perquisizione. Lo *Stored Communications Act*

---

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

[104] Nel caso *United States v. Kelley, 482 F3d 1047, 1053 (9th Cir. 2007)*, i soggetti avevano usufruito del servizio America On Line, acquistando immagini pedopornografiche con la loro carta di credito.

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

[106] *In re Grand Jury Investigation Concernine Solid State Devices, Inc., 130 F.3d 853, 957 (9th Cir. 1997)*.

[107] *United States v. Hay, 231 F3d 630, 637 (9th Cir. 2000)*; *United States v. Blake, No. 1:08-cr-0284 OWW (E.D.Cal. 02/24/2010)*. In questo caso, la Corte della California aveva ritenuto legittimo il sequestro di un personal computer, 2 hard disk removibili, alcuni cd e uno "zip disk", in quanto sarebbe stato impossibile effettuare una copia forense di tutto il material in tempi brevi.

(18 U.S.C. §§ 3103a) prevede che ciò possa avvenire qualora la notifica all'interessato dell'atto possa pregiudicare la salute o la vita di una persona, compromettere la prova o mettere in pericolo l'intera indagine. Nel caso *United States v. Grubbs* , il Giudice ritenne legittimo un *warrant* effettuato sulla futura consegna di un video contenente immagini pedo-pornografiche ordinato on line dall'indagato[108].

Nel caso in cui gli agenti avessero ragione di credere che i dati siano stati memorizzati in due o più luoghi all'interno del territorio degli Stati Uniti, essi dovranno ottenere un mandato per ogni luogo dove il dato risiede[109].

Sebbene i principi fissati dal quarto emendamento della Carta Costituzionale statunitense appaiano particolarmente stringenti e garantisti, è ammessa la perquisizione e il sequestro della prova digitale anche senza mandato, qualora il soggetto si trovi in una condizione in cui non si possa ragionevolmente pretendere che venga rispettata la sua privacy[110].

La giurisprudenza statunitense alla fine degli anni ottanta ha più volte affrontato il principio della "expectation of privacy constitutionally reasonable" chiarendone i limiti: in un'indagine legata al traffico di stupefacenti la Polizia Giudiziaria aveva ispezionato i rifiuti lasciati fuori dall'abitazione dell'indagato[111]. La Suprema Corte statunitense ha stabilito che tale attività di indagine non viola i principi previsti dal quarto emendamento e non è quindi ragionevole ritenere che sia stata violata la privacy dell'indagato. Analogamente la Suprema Corte in un caso in cui un poliziotto aveva scoperto una piantagione di *marijuana* situata in un terreno distante alcune centinaia di

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

[109] Tuttavia, ove vengano in possesso delle informazioni da un altro Stato, il sequestro sarebbe comunque valido, salvo che non abbiano deliberatamente violato la *Rules* 41 *del Federal Criminal Procedural Code* (*United States v. Burke, 517 F2d 377, 386 2d Cir. 1975*).

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

[111] *California v. Greenwood, 486 U.S. 35, 40-41 1988*.

metri dall'abitazione dell'imputato, ha statuito che la tutela offerta del quarto emendamento riguarda solo l'abitazione e, al massimo, il giardino adiacente a essa[112].

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

- la prova digitale sia inviata a una terza persona (*Third-Party Possession*)[113];
- la prova digitale sia stata scoperta e comunicata all'autorità giudiziaria da parte di un privato (*Private Search*)[114];
- vi sia il consenso dell'indagato, della moglie/marito dello stesso[115], dei genitori se l'indagato è minorenne[116] o, anche di una persona che condivide lo stesso personal computer[117] (*Consent*);
- vi sia una situazione di pericolo e la prova digitale rischi di essere compromessa o distrutta[118];
- un *provider* e la polizia trovino un accordo per lo scambio di informazioni (*Exigent Circumstances)*[119];
- sia stato effettuato il legittimo arresto del soggetto indagato (*Search after a lawful arrest*)[120];

---

[112] *Oliver v. United States, 466 U.S. 170, 177 1984*.

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

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

[115] Nel caso *Trulock c. Freeh, 275 E.3d, 391, 398, 403-404 (4th Cir. 2001)* un ex agente dell'FBI che aveva più volte criticato l'operato dell'Agenzia presso cui aveva lavorato, subì una procedura di *search and seizure* del suo computer, in quanto lo condivideva, pur avendo diverse password di accesso, con la propria compagna.

[116] *United States v. Andrus, 483, F.3d 711, 720-21 (10th Cir. 2007)*.

[117] *United States v. Matlock, 415 U.S. 164 (1974)*.

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

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

- la prova digitale emerga *ictu oculi* (*Plain View*)[121];
- la prova sia scoperta durante un controllo alla frontiera (*Border Search*)[122];
- i soggetti siano sottoposto a regimi di libertà controllata (*Probation and Parole*)[123];
- sia ricercata la prova all'interno di un ufficio pubblico (*Public-Sector Workplace Searches*)[124].

1.6 Modalità operative durante la fase di individuazione del dato digitale

La *digital evidence* presenta un'intrinseca caratteristica di fragilità tale per cui può essere facilmente alterata, danneggiata o distrutta, anche per colpa degli stessi investigatori o esaminatori.
Per questi motivi è necessaria, oltre ad un'ottima conoscenza dello strumento informatico, anche il rispetto di una corretta metodologia delle operazioni di raccolta degli elementi probatori che dovrà comprendere sia le tecniche prettamente informatiche (analisi *hos*t, analisi *file* di *log*), che le tecniche investigative tradizionali (verbale di sommarie informazioni con le persone coinvolte, esame dello stato dei luoghi).
È stato correttamente osservato da alcuni autori che la creazione di linee guida sulle modalità operative da utilizzare in caso di un'indagine informatica limitano l'attività investigativa sia perché potrebbero in breve tempo diventare

[120] *Arizona v. Gant, 129 S. Cr. 1710 (2009)*.
[121] Nel caso *Horton v. California, 496 U.S. 128, 136 (1990),* un agente che non aveva ottenuto un mandato per ricercare delle armi, ma solo della merce rubata, una volta arrivato presso l'abitazione, trova in bella mostra le armi.
[122] Nel caso *United States v. Boucher, 2007 WL 4246473,* che verrà descritto nel terzo capitolo, un Giudice dello Stato del Vermont (Jerome Niedermeier) ha ordinato all'imputato (Sebastien Boucher) di rivelare la password per decifrare un hard disk crittografato sequestrato durante un controllo alla frontiera.
[123] *United States v. Knights, 534 U.S. 112, 122 (2001)*.
[124] *United States v. Mancini, 8 F.3d 104, 109 (1st Cir. 1997)*.

obsolescenti, sia perché l'analisi di uno strumento così complesso come l'elaboratore elettronico è difficilmente riconducibile in rigidi schemi[125].

In questo senso la giurisprudenza statunitense ha affermato che "l'investigazione digitale deve essere considerata più un'arte che una scienza", criticando ogni forma di limitazione alle metodologie investigative in ambito informatico[126].

Ciò non significa, tuttavia, che non sia necessario stabilire regole e principi che consentano di garantire l'autenticità, l'accuratezza e l'attendibilità delle prove raccolte durante l'attività d'indagine, senza tuttavia specificare le tecniche investigative che sarebbero comunque soggette a una rapida obsolescenza[127].

Durante la fase dell'individuazione della prova digitale, sono necessarie tre operazioni preliminari: la corretta descrizione dell'ambiente, l'individuazione dei soggetti utilizzatori di tali supporti e la valutazione del grado di competenza tecnica dell'indagato.

L'analisi dell'ambiente in cui è collocato il personal computer, attraverso una documentazione fotografica e, ove possibile, riprese video, riveste una grande importanza, in quanto molto spesso chi effettuerà la successiva perizia del materiale sequestrato, potrebbe non aver partecipato alla relativa fase della perquisizione.[128] Anche in questo caso, tuttavia, si potrebbero porre dei legittimi dubbi su quali debbano essere le condizioni necessarie per ritenere scientifiche e non alterate le immagini e le riprese digitali effettuate durante la perquisizione[129].

---

[125] G. Costabile, *Scena criminis, documento informatico e formazione della prova penale*, disponibile al seguente URL: http://www.penale.it/page.asp?mode=1&IDPag=72.

[126] *United States v. Brooks, 427 F.3d 1246, 1252 (10th Cir. 2005)*

[127] Onofrio Signorile, Computer Forensics Guidelines: *un approccio metodico-procedurale per l'acquisizione e l'analisi della digital evidence*, in *Ciberspazio e diritto*, 2009, p. 197.

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

[129] Sull'ampio tema della *image forensics* che, per motivi di brevità, non si può approfondire in questa sede, si veda: S. Battiato, G. Messina, S. Rizzo, *Image Forensics*. *Contraffazione Digitale e identificazione della camera d'acquisizione: status e prospettive*, 2009, Forlì, in IISFA Memberbook, Experta, disponibile al seguente URL: http://iplab.dmi.unict.it/download/Elenco%20Pubblicazioni%20%28PDF%29/Capitoli%20di%20Libri/2009_IISFA_Image_Forensic.pdf; A. Swaminathan, K. J. Ray Liu, *Digital Image Forensics via Intrinsic Fingerprints*, in *IEEE Transactions on Information Forensics and Security*, marzo 2008, disponibile al seguente URL: http://www.cspl.umd.edu/sig/publications/Swaminathan_TIFS_200803.pdf.

Successivamente, sarà necessario comprendere, tramite l'ausilio dei verbali di sommarie informazioni testimoniali fornite da persone informate sui fatti o di spontanee dichiarazioni da parte dell'indagato, quali soggetti avevano la concreta possibilità di accedere ai supporti informatici oggetto di indagine[130].

L'autorità giudiziaria, infatti, in vista di una corretta attribuzione delle responsabilità, non deve mai escludere l'ipotesi che il legittimo proprietario del personal computer possa essere assolutamente all'oscuro dell'illecito commesso[131].

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

La presenza o meno di appunti, diari, note dai quali si possano eventualmente ricavare password o chiavi di cifratura o di riviste specializzate nel settore informatico potrebbero essere degli utili indici per escludere o avvalorare l'ipotesi che il computer sia stato violato attraverso l'utilizzo di strumenti informatici e che quindi il reato non sia stato compiuto dal soggetto indagato, ma da una terza persona che si è introdotta nel suo computer[132]. Allo stesso modo, tali elementi possono consentire di valutare la reale volontà dell'utente di commettere l'illecito: il Tribunale di Brescia, ad esempio, in una pronuncia in tema di detenzione illecita di materiale pedopornografico, ha ritenuto che non vi

---

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

[131] L. Chirizzi, *Computer Forensic. Il reperimento della fonte di prova informatica*, 2006 ,Roma, Laurus Robuffo, p. 20.

[132] Gli strumenti utilizzati per controllare da remoto un computer sono molti: a titolo esemplificativo si citano la *botnet* e il *rootkit*. La *botnet* è una rete di computer collegati a Internet controllato da un'unica entità, il *botmaster*. Ciò può essere causato da falle nella sicurezza o mancanza di attenzione da parte dell'utente e dell'amministratore di sistema, per cui i computer sono infettati da *trojan* i quali consentono ai loro creatori di controllare il sistema da remoto. Il *rootkit* è un *software* che consente di assumere il controllo dell'utente *root*, ossia dell'amministratore del sistema. Dopo che un *hacker* ha installato un *rootkit* sul computer, potrà accedere in qualsiasi momento, senza temere di essere rilevato.

fosse consapevolezza da parte dell'imputato di aver scaricato materiale pedopornografico, in quanto il *file*, protetto da *password*, poteva essere ragionevolmente scambiato per l'aggiornamento di un videogioco[133]. Questo esempio dimostra l'importanza di una seria verifica, durante la fase dell'ispezione e della perquisizione, di tutti gli elementi che possono dimostrare l'effettiva conoscenza dello strumento informatico da parte dell'indagato al fine di portare utili elementi di valutazione durante la successiva fase dibattimentale.

Dopo aver terminato queste tre importanti operazioni preliminari, sarà possibile concentrarsi sui supporti informatici oggetto della perquisizione. In questa fase è opportuno verificare preliminarmente se l'elaboratore elettronico sia acceso oppure spento.

Qualora l'elaboratore fosse trovato spento, sarà necessario aprire il relativo carrello, per verificare la presenza, all'interno di eventuali supporti ottici (cd o dvd), utilizzando l'apposito foro presente nella quasi totalità dei lettori ottici.

Si dovrà successivamente aprire l'elaboratore per identificare il numero e le caratteristiche tecniche dei dischi fissi presenti al suo interno e, ove possibile, avere conferma da parte dell'indagato che i dati presenti in esso contenuti siano esclusivamente riconducibili alla sua persona.

Nel caso, invece, in cui l'elaboratore venisse trovato in funzione, l'indagine diventa più delicata, in quanto potrebbe essere utile o addirittura necessario recuperare tutti i dati volatili presenti all'interno della *RAM* che verrebbero persi con l'arresto del sistema operativo. Le soluzioni possibili per l'acquisizione della *RAM* sono due:

- arrestare il sistema attraverso l'interruzione della corrente ed effettuare una immediata analisi forense dell'*hard disk* dell'indagato (*guillotine method*)[134];

---

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

[134] Per un approfondimento sulle modalità di acquisizione della RAM, si veda J. Rutkowska, *Beyond The CPU: Defeating Hardware Based RAM Acquisition*, disponibile al seguente URL: http://www.first.org/conference/2007/papers/rutkowska-joanna-slides.pdf.

- utilizzare, a computer acceso, particolari software che consentono di acquisire la memoria volatile senza alterare la prova digitale.

Sempre nel caso in cui l'elaboratore fosse acceso, potrebbe essere determinante l'analisi dell'attività di *download* e delle informazioni relative agli utenti connessi nel caso di utilizzo di software di *file-sharing*[135].

In tutti questi tipo di operazioni, la Polizia Giudiziaria può avvalersi, ai sensi dell'articolo 348, III comma, c.p.p., di consulenti tecnici. La loro presenza è particolarmente utile poiché alcune tracce sfuggono agli operatori non professionali: è il caso, ad esempio, dei residui di memoria che hanno subito solo una parziale reimpressione (*slack*), i *file* cancellati (per l'utente, non per il sistema), quelli temporanei ancora presenti in memoria, gli *swap* (aree di disco rigido intervenute a supporto della *RAM*) e i *dump* (foto della *RAM* in caso di malfunzionamento).

Durante un'ispezione, qualora fosse necessario acquisire alcuni messaggi di posta elettronica che non sono presenti all'interno dei normali *client* utilizzati per la loro gestione (*Microsoft Outlook, Eudora*), dovrà essere contattato il *provider* al fine di bloccare tempestivamente l'accesso all'indirizzo di posta elettronica, per poi richiedere l'estrazione delle *e-mail* presenti sul *server*. Diversamente, l'indagato potrebbe accedere, anche tramite terzi, all'indirizzo di posta elettronica al fine di cancellare i messaggi "sospetti".

Al termine di tali operazioni si procederà allo spegnimento dell'*hard disk* staccando la spina dell'alimentazione elettrica in modo da ottenere il più possibile una fotografia del sistema così come era, evitando la cancellazione e l'alterazione di tutti i dati temporanei[136].

---

[135] Per un approfondimento si veda E. Huebner, D. Bema, F. Henskensb, M. Wallisb, *Persistent System Techniques in forensic acquisition of memory,* in *Digital Investigation*, 2007, p. 129.

[136] Vi è, addirittura, chi suggerisce, specie se l'indagato è soggetto particolarmente esperto nell'uso degli strumenti informatici, di disporre con separato provvedimento la temporanea interruzione dell'energia elettrica presso i locali da perquisire, sì da impedire che durante l'atto l'utente alteri i dati oggetto di ricerca. F. Testa, *Cybercrime, intercettazioni telematiche e cooperazione giudiziaria in materia di attacchi ai sistemi informatici*, *op. cit.*, p. 10.

Ogni operazione dovrà essere documentata dettagliatamente: alcuni esperti suggeriscono di utilizzare due distinti documenti: uno per la descrizione cronologica di tutte le operazioni compiute (*timeline* degli eventi) e l'altro per identificare i supporti informatici e riportare tutte le azioni intraprese per preservare la "catena di custodia" (*chain of custody)* di ogni singolo supporto[137].
È consigliabile, infine, che la redazione del verbale documenti le operazioni compiute con appositi *screenshot*: tutte le attività svolte durante l'eventuale analisi forense devono essere accuratamente registrate in un *file* di *log* che consenta di evidenziare se siano state avviate alterazioni dei dati originali.

2. Aquisizione della digital evidence

Nel precedente capitolo sono state analizzate le modalità di individuazione della *digital evidence* e di identificazione dell'autore dell'illecito presente in Italia e negli Stati Uniti. Anche se non mancano le analogie tra i due Paesi, è apparso evidente come, negli Stati Uniti La disciplina della *digital forensics* abbia raggiunto un grado di maturità ben diverso rispetto a quello italiano. Nel prossimo capitolo analizzeremo l'acquisizione del dato digitale sia attraverso il "tradizionale" mezzo di ricerca della prova del sequestro, sia attraverso le possibili soluzioni tecnologiche (tra tutte la *remote forensics*) che, se da un lato semplificano la vita all'investigatore, dall'altro rischiano di minare alcuni diritti costituzionalmente protetti a tutela dell'indiduo.

2.1 Il sequestro

[137] Onofrio Signorile, Computer Forensics Guidelines: *un approccio metodico-procedurale per l'acquisizione e l'analisi della digital evidence*, *op. cit.*, p. 201.

Il codice di procedura penale prevede tre distinte forme di sequestro: il sequestro "probatorio"[138] (art. 253 c.p.p.), il sequestro preventivo[139] (art. 321 c.p.p.) ed il sequestro conservativo[140] (art. 316 c.p.p.). Il primo è collocato tra i mezzi di ricerca della prova, mentre gli altri due sono le misure cautelari.

Caratteristica comune ai tre tipi di sequestro è quella di creare un vincolo di indisponibilità su una cosa mobile od immobile, attraverso uno spossessamento coattivo[141].

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

Il sequestro preventivo, durante la fase delle indagini, invece, è disposto dal Giudice per le indagini preliminari su richiesta del Pubblico Ministero (art. 321 c.p.p.). Anche in questo caso, il Pubblico Ministero e la Polizia Giudiziaria possono disporre il sequestro in casi di urgenza (art. 321 comma 3-bis c.p.p.). Il Pubblico Ministero, tuttavia, dovrà chiedere al Giudice la convalida del provvedimento entro quarantotto ore dal sequestro o dalla ricezione del verbale se il sequestro è stato eseguito su iniziativa della Polizia Giudiziaria.

---

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

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

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

[141] P. Tonini, *Manuale di procedura penale*, 2004, Milano, Giuffrè, p. 287.

Il sequestro conservativo, come nel caso precedente, è emesso dal Giudice competente con ordinanza su richiesta dal Pubblico Ministero o della parte civile.
Oggetto del sequestro sono, come già detto, il corpo del reato e le cose pertinenti al reato necessarie per l'accertamento dei fatti.
Il corpo del reato è configurato, secondo la definizione data dall'articolo 253 comma 2, c.p.p., non solo dalle cose sulle quali o mediante le quali il reato è stato commesso, ma anche da quelle che ne costituiscono il prodotto, il profitto o il prezzo. Questa seconda locuzione comprende sia le cose acquisite direttamente con il reato o da questo create, sia qualsiasi vantaggio patrimoniale e non patrimoniale ricavato dal reato.
Sono pertinenti al reato, invece, le cose che, per la particolare relazione intercorrente fra cosa e reato, sembrano dotate di una specifica potenzialità probatoria e consentono di accertare, anche indirettamente, la consumazione dell'illecito, il suo autore e le circostanze del reato[142]. In un'indagine informatica, il corpo del reato o le cose pertinenti a esso sono nella gran parte dei casi costituiti dai dati digitali contenuti all'interno di un dispositivo di memorizzazione. Ciò pone un problema, in quanto l'art. 253 comma 2 c.p.p. presuppone la materialità del corpo del reato o delle cose pertinenti ad esso, mentre la *digital evidence*, è connotata dall'immaterialità[143].
Alcuni autori hanno agevolmente superato tale assunto, sostenendo che il dato contenuto all'interno di un computer è assimilabile a quello presente in un documento cartaceo con l'unica differenza del tipo di supporto in cui tale dato è stato impresso[144].
L'art. 19 della Convenzione Cybercrime chiarisce espressamente che il sequestro di strumenti informatici può riguardare indistintamente sia l'*hardware* (sistema

[142] D. Siracusano, A. Galati, G. Tranchina, E. Zappalà, *Diritto processuale penale,* 1996, Milano, Giuffrè, p. 421.
[143] S. Aterno, *La* computer forensics *tra teoria e prassi*, in *Ciberspazio e diritto*, 2006, fasc. 4, p. 427.
[144] L. Chirizzi, *op. cit.*, p. 18.

informatico, o supporto di memorizzazione) sia dati digitali in esso contenuti e presenti all'interno del territorio nazionale[145].

La giurisprudenza di merito, non soffermandosi neppure sulla *vexata quaestio* dell'immaterialità del dato informatico, ha considerato l'*hard disk*, l'unico elemento utile da acquisire durante la fase di indagine[146]. Nella stessa pronuncia, il Giudice aveva chiarito, inoltre, che tra *hard disk* e software in esso contenuto "sussiste un rapporto di stretta pertinenza, in quanto il software necessita dell'*hard disk* per funzionare. Non rileva che il software possa funzionare su un altro *hard disk*: sarebbe come dire che un furgone utilizzato dagli autori del furto per trasportare i mobili della casa derubata non sia cosa pertinente al reato, perchè gli autori avrebbero potuto usare un altro furgone o semmai un autoveicolo".

La giurisprudenza di legittimità si è concentrata sulla distinzione tra il sequestro probatorio della memoria fissa di un computer e quello del materiale informatico "neutro" rispetto alle indagini in corso: il Tribunale del Riesame di Siracusa, in un'indagine legata alla diffusione di materiale pedo-pornografico, aveva qualificato come "cosa pertinente al reato", il materiale informatico utilizzato per "scaricare" i *file* in questione tra cui lo schermo, la stampante e lo scanner dell'indagato[147].

---

[145] L'art. 184 dello Explanatory Report disponibile al seguente URL: http://conventions.coe.int/treaty/en/reports/html/185.htm chiarisce che l'articolo 19 della Convenzione Cybercrime è stato scritto proprio perché in molti giurisdizioni è previsto esclusivamente il sequestro di "oggetti fisici". "This article aims at modernising and harmonising domestic laws on search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law includes powers for search and seizure of tangible objects. However, in a number of jurisdictions stored computer data per se will not be considered as a tangible object and therefore cannot be secured on behalf of criminal investigations and proceedings in a parallel manner as tangible objects, other than by securing the data medium upon which it is stored. The aim of Article 19 of this Convention is to establish an equivalent power relating to stored data".

[146] La sezione del Riesame del Tribunale di Torino, ha osservato che "*l'hard-disk* è certamente (e quanto meno) cosa pertinente al reato, in quanto in atti vi è il *fumus* che, anche tramite quell'*hard-disk*, sia stato utilizzato il *software* necessario per porre in essere i fatti contestati" (Tribunale di Torino, 7 febbraio 2000, disponibile al seguente URL: http://www.ictlex.net/?p=889). Per un commento si veda, A. Monti, *Sequestri di computer. Dal Tribunale di Torino un provvedimento controtendenza*, 15 aprile 2000, disponibile al seguente URL: http://www.ictlex.net/?p=626.

[147] Cassazione Penale, 7 marzo 2003, disponibile al seguente URL: http://www.ictlex.net/?p=119.

Nel successivo ricorso in Cassazione, l'indagato aveva, da un lato, sostenuto che uno *scanner* o uno schermo non potevano avere alcuna utilità sotto il profilo probatorio e, dall'altro, aveva lamentato l'illegittimità del sequestro dello stesso *hard disk*, in quanto sarebbe stato sufficiente prelevare una copia forense del suo contenuto[148].

La Suprema Corte ha parzialmente accolto il ricorso, in quanto la motivazione data dal Tribunale di Siracusa sulla sussistenza, in concreto, delle finalità proprie del sequestro probatorio di cose pertinenti al reato, non era adeguata a quella richiesta: non venivano, infatti, minimamente indicate le esigenze probatorie che legittimassero il permanere del vincolo su parte del materiale informatico sequestrato. La stessa Corte, tuttavia, ha ritenuto legittimo il vincolo sulla memoria fissa del computer, non prendendo in considerazione l'ipotesi fornita dall'indagato di effettuare una copia dei dati in esso contenuti[149].

Sotto questo ultimo aspetto, il Tribunale di Torino, nell'ordinanza sopra citata, aveva deciso diversamente, in quanto "nulla avrebbe potuto impedire agli agenti di Polizia Giudiziaria, per di più appartenenti a Sezione specializzata nell'ambito dei reati informatici, di procedere a copia integrale dell'*hard disk*, con specificazione verbale di ogni singola operazione.

Il tema è particolarmente dibattuto anche dalla dottrina e vede due differenti orientamenti.

Da un lato vi è chi sostiene che potrebbe essere sufficiente apporre, in presenza di testimoni e con le dovute cautele, un sigillo elettronico (impronta di *hash*)

[148] Per una definizione approfondita di "copia forense" si rimanda al paragrafo 2.4

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

sulle cartelle incriminate o sull'intero *hard disk*, per poi procedere alla copia sicura (*bit stream image)* del suo contenuto, lasciando al legittimo proprietario l'originale[150].

Altri autori, tuttavia, sostengono che una simile procedura non tiene conto delle innumerevoli variabili che costituiscono l'espletamento delle indagini e che richiedono di avere a disposizione le cose sotto sequestro per un tempo necessario a un'adeguata ricerca delle fonti di prova[151].

La legge di ratifica della Convenzione Cybercrime ha introdotto l'articolo 254-*bis* c.p.p., il quale prescrive che, quando l'Autorità Giudiziaria dispone un sequestro presso i fornitori di servizi informatici, telematici o di telecomunicazioni dei dati da questi detenuti, compresi quelli di traffico e di ubicazione, può stabilire per esigenze di regolare fornitura dei servizi medesimi, di acquisire tali dati mediante copia lasciando al fornitore l'onere della conservazione degli originali.

Tale norma sembra propendere per l'adozione di una procedura meno invasiva in caso di sequestro di dati digitali; tuttavia va rilevato che tale procedura è solo facoltativa ed è limitata ad una determinata categoria di soggetti (*provider* di servizi e fornitori di connettività).

Nella prassi, tre ragioni portano l'autorità giudiziaria a propendere per un sequestro integrale dell'*hard disk* senza alcuna copia *bit stream image* del supporto.

La prima risiede nel fatto che, molto spesso, si procede al sequestro di materiale informatico nell'ambito di indagini legate al contrasto della pirateria informatica (legge 633/41 e successive modifiche) o della pedo-ponografia (artt. 603 *ter* e *quater* c.p.): in entrambe i casi è prevista, in caso di condanna, la confisca degli

[150] A. Monti, *La formazione della prova nei processi di criminalità informatica*, intervento del 5 marzo 2003, presso il Master in Diritto delle nuove tecnologie, organizzato dal Centro Studi Informatica Giuridica. Una breve relazione dell'intervento è disponibile al seguente URL http://www.avvocatiacqua vivacassano.it/convegni-contributi/post-eventum-formazione_prova.htm.

[151] L. Chirizzi, *op. cit.*, p. 20.

strumenti e dei materiali utilizzati per compiere i relativi reati (art. 171 *sexies* legge 633/31 e art. 600 *septies* c.p.).

La seconda è che l'indagato, ai sensi dell'articolo 258 c.p.p., ha diritto di chiedere all'Autorità Giudiziaria che sia estratta gratuitamente la copia dei dati contenuti all'interno dell'*hard disk*, a condizione che sia in grado di dimostrare la legittimità del possesso del supporto: in questo modo viene meno anche il possibile pregiudizio che scaturisce nel momento in cui all'interno del computer fossero presenti anche dati indispensabili, ad esempio, per la prosecuzione della propria attività lavorativa[152]. Sul tema è opportuno rilevare che la giurisprudenza di legittimità ha rienuto ammissibile l'istanza di riesame del sequestro, anche qualora sia stata precedentemente fornita una copia di dati digitali all'indagato. Infatti, permane nel richiedente, "l'interesse a far verificare che il sequestro sia stato disposto nei casi ed entro i limiti previsti dalla legge"[153].

La terza, già menzionata, è che un procedimento di copia forense di un *hard disk* può avere una durata incompatibile con l'esecuzione, in tempi ragionevoli, del mezzo di ricerca della prova[154].

L'incertezza sulle modalità operative del sequestro di supporti informatici sembra, comunque, destinata a proseguire: emblematica, in tal senso, è l'ordinanza del Tribunale del Riesame di Venezia, con la quale è stato rigettato il ricorso proposto dall'indagato avverso il decreto di sequestro probatorio emesso dal Pubblico Ministero in relazione al reato di divulgazione di materiale pedo-pornografico[155]. Tre le argomentazioni a sostegno del ricorso, il difensore ha contestato la sussistenza della finalità probatoria del sequestro esteso a

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

[153] Cassazione Penale, Sez. VI, 31 maggio 2007, n. 40380.

[154] S.D. Williger, R.M. Wilson, *Negotiating the Minefields of Electronic Discovery*, in *Richmond Journal of Law and Technology*, 2004, Vol. X, Issue 5, disponibile al seguente URL: http://jolt.richmond.edu/v10i5/article52.pdf.

[155] Tribunale di Venezia, 31 marzo 2005, disponibile al seguente URL: http://www.interlex.it/testi/giurisprudenza/ve050331.htm.

componenti ulteriori rispetto all'*hard disk*, con richiesta di limitare il sequestro solo a questo. Il Tribunale, non aderendo all'indirizzo della giurisprudenza di legittimità in precedenza descritto, ha rigettato la richiesta ritenendo che il decreto del Pubblico Ministero avesse spiegato sufficientemente che "nel personal computer, nelle relative periferiche nonché nei supporti informatici si sarebbero potuto trovare le immagini di pornografia infantile costituenti prova dell'ipotizzato reato sub indagine". A tal fine, il Tribunale ha giudicato necessario "un approfondito esame tecnico della strumentazione informatica [...] non potendosi escludere che la disponibilità di tutto il materiale sequestrato possa consentire, o comunque facilitare, operazioni tecniche più complesse quali, ad esempio, la ricerca di tracce di *file* già scaricati e, successivamente, cancellati".
Sostenere che all'interno di un monitor o di un mouse possano annidarsi delle immagini di natura pedopornografica non vuol dire, come è stato sostenuto da alcuni autori[156], "negare la civiltà del diritto", ma è solo un esempio concreto di quanto la cultura delle nuove tecnologie sia ancora del tutto sconosciuta agli operatori del diritto.
Molto più rassicurante la giurisprudenza di legittimità che ha ritenuto illegittimo il sequestro di un intero "server" aziendale disposto in relazione al reato di turbata libertà dell'industria o del commercio sostenendo che "il Giudice del riesame di un sequestro probatorio deve accertare l'esistenza del vincolo di pertinenzialità tra il reato ipotizzato ed i diversi beni o le diverse categorie di beni oggetto del provvedimento di sequestro"[157].
L'altalenante casistica giurisprudenzale descritta ha, tuttavia, una sua ragion d'essere: ogni indagine è diversa dall'altra e, per questa ragione, le modalità operative del sequestro informatico sono da valutare caso per caso. A questo proposito è consigliabile l'utilizzo di una distribuzione live di alcuni software di

[156] M. Cammarata, *Sequestri: se la polizia viola il domicilio informatico*, 22 aprile 2005, in Interlex, http://www.interlex.it/regole/tribvebz.htm.
[157] Cass. Pen., sez. III, 18 novembre 2008, n. 12107.

foensics (Helix o Caine) al fine di verificare preliminarmente, senza alterarlo, il contenuto di un *hard disk* prima di decidere se sequestrarlo o meno[158].

2.2 Sequestro di corrispondenza

Sempre sul tema dell'oggetto del sequestro probatorio è opportuno rilevare come la giurisprudenza prima e il codice di procedura penale poi abbiano equiparato la corrispondenza tradizionale alla posta elettronica. In altre parole, si è ritenuta applicabile la disciplina dell'art. 254 c.p.p., in forza del quale le carte e gli altri documenti sequestrati che non rientrano fra la corrispondenza sequestrabile sono immediatamente restituiti all'avente diritto e non possono comunque essere utilizzati.

Sul punto il Tribunale di Torino ha sostenuto come l'inviolabilità della corrispondenza sia espressione di un principio generale che trova la sua legittimazione nell'art. 15 della nostra Carta Costituzionale[159]. Lo stesso Tribunale ha osservato, tuttavia, che il concetto d'immediatezza, previsto dall'articolo 254 c.p.p., debba considerarsi come un concetto relativo, soprattutto qualora il numero delle *e-mail* non consenta un'agevole individuazione di quelle da restituire.

Sullo stesso tema è intervenuto il Tribunale del Riesame di Brescia sostenendo che "il sequestro di un intero *hard disk* consente certamente l'acquisizione di elementi probatori, ma implica anche l'acquisizione di dati che esulano dal contesto per il quale l'atto è disposto, sicché, come è immediatamente percepibile, tale genere di sequestro esige un ambito di corretta e ristretta operatività per evitare connotazioni di spropositata afflittività e di lesione di beni costituzionalmente protetti. Sotto questo profilo merita particolare attenzione la compressione della libertà e segretezza della corrispondenza conservata nel disco

[158] G. Costabile, *op. cit.*, p. 497.
[159] Tribunale di Torino, 7 febbraio 2000, disponibile al seguente URL: http://www.ictlex.net/?p=889.

fisso, con conoscenza di tutti i messaggi inviati o ricevuti, compresi quelli destinati a soggetti del tutto estranei alle indagini"[160]. Tale decisione è stata avallata dalla Suprema Corte che ha ritenuto illegittimo il sequestro del computer in uso ad una giornalista e dell'area del "server" dalla stessa gestita, con la conseguente acquisizione dell'intero contenuto dell'*hard disk* e di un'intera cartella personale presente nell'area del sistema operativo. Le motivazioni della Corte di Cassazione richiamano quelle del Tribunale del Riesame di Brescia: "il sequestro probatorio disposto nei confronti di un giornalista professionista deve rispettare con particolare rigore il criterio di proporzionalità tra il contenuto del provvedimento ablativo di cui egli è destinatario e le esigenze di accertamento dei fatti oggetto delle indagini, evitando quanto più è possibile indiscriminati interventi invasivi nella sua sfera professionale"[161].

Alcuni autori hanno rilevato che lo strumento investigativo del sequestro di corrispondenza sia, da un punto di vista pratico, un'attività molto più simile ad un'intercettazione che non a un provvedimento ablativo[162]. Dietro un apparente provvedimento di sequestro si celerebbe, infatti, una vera e propria attività captativa di comunicazioni epistolari, che non rispetta, però, le regole stabilite a pena di nullità o inutilizzabilità dagli artt. 266 e ss. c.p.p., né, ancor prima, la riserva di giurisdizione di cui all'art. 15 Cost. così come attuata dal codice di rito. L'art. 8 della legge di ratifica della Convenzione Cybercrime ha comportato la modifica del primo comma dell'art. 254 c.p.p., prevedendo, in capo all'Autorità Giudiziaria, di procedere al sequestro presso "i fornitori di servizi postali, telegrafici, telematici o di telecomunicazioni di lettere, pieghi, pacchi, valori,

[160] Tribunale di Brescia, 4 ottobre 2006, disponibile al seguente URL: http://www.ictlex.net/?p=566. Tale decisione è stata confermata dalla Suprema Corte (Cass. pen., sez. VI, 31 maggio 2007, n. 40380).
[161] Cassazione penale, Sez. VI Sent., 31-05-2007, n. 40380, in *Dir. Pen. e Processo*, 2008, 11, p. 1416.
[162] A. Manchìa Chelo, *Acquisizione di corrispondenza o "intercettazione epistolare"?*, in *Dir. Pen. Proc.*, 2007, 8, p. 1049; Sul tema si veda anche, Cassazione Penale, Sez. II, 23 maggio 2006, n. 20228. Per una opinione contraria si veda: Consiglio Superiore della Magistrature, Atti dell'incontro di studio tenutosi a Roma il 22-23 maggio 2006 dal titolo, *Le intercettazioni telefoniche, telematiche ed ambientali: normativa, prassi e nuove tecnologie*, p. 12, disponibile al seguente URL: http://appinter.csm.it/incontri/relaz/13134.pdf.

telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica".

Anche se il dettato letterale del nuovo art. 254 c.p.p. sembra estendere al sequestro di corrispondenza cartacea quella telematica, parte della dottrina ritiene ancora preferibile ricorrere alle intercettazioni telematiche, poiché tale secondo strumento risulta essere più garantito per l'indagato, essendo necessario l'intervento del Giudice per le Indagini Preliminari[163].

2.3 Le modalità operative nel caso di sequestro della prova digitale

Negli ultimi anni le competenze della Guarda di Finanza (che dal 2001 ha istituito il "G.A.T.", Gruppo Anticrimine Tecnologico[164]), dei Carabinieri (con alcuni reparti del "R.O.S." Raggruppamento Operativo Specializzato[165]) e della Polizia Postale (specialmente per quanto riguarda le indagini in tema di pedofilia e truffe telematiche[166]) sono notevolmente cresciute ed hanno raggiunto un livello adeguato ai più alti standard previsti in campo internazionale.

Al grado di eccellenza raggiunto dai citati nuclei specializzati non sempre corrisponde uno standard di conoscenza minimo dello strumento informatico da parte di tutti gli altri componenti delle Forze dell'Ordine. Il risultato è che i nuclei specializzati si trovano talvolta a dover investire del tempo prezioso in indagini che potrebbero essere svolte anche da altri pubblici ufficiali che, se adeguatamente formati, potrebbero raggiungere gli stessi risultati, soprattutto nei casi dove il pericolo sociale non è particolarmente elevato (ad esempio nei casi di diffamazioni on line o di violazione penale della normativa sulla privacy).

---

[163] F. Testa, *op. cit.*, p. 47.

[164] Per ulteriori informazioni sul Gruppo Antricrime Tecnologico si veda: http://www.gat.gdf.it/

[165] Per ulteriori informazioni sul Raggruppamento Operativo Specializzato si veda: http://www.carabinieri.it/Internet/Arma/Oggi/Reparti/Organizzazione+Mobile+e+Speciale/ROS

[166] Per ulteriori informazioni sulla Polizia Postale si veda: http://poliziadistato.it/articolo/978-Attivita_ed_organizzazione

Sempre più spesso, la Polizia Giudiziaria si avvale di consulenti nominati in qualità di propri ausiliari, qualora si debbano compiere atti od operazioni che richiedono specifiche competenze tecniche (art. 348 c.p.p.). Questo comporta un potenziale aggravio di costi e di risorse per lo Stato e non sempre garantisce un'esperienza investigativa "tradizionale" che è necessario mantenere anche nel mondo del *cybercrime*.

Le operazioni che dovrebbero essere compiute durante la fase del sequestro per garantire la tutela dell'integrità e della genuinità del dato informatico ed evitare successive contestazioni da parte dell'indagato o del suo difensore, sono principalmente due[167].

In primo luogo, una volta individuati i supporti da sequestrare, è necessaria una loro identificazione attraverso le loro caratteristiche tecniche (marca, modello, numero seriale ed etichette apposte). In questa fase, oltre a far siglare dall'indagato il singolo supporto sequestrato, è consigliabile effettuare anche alcune fotografie o una ripresa video, in modo da rendere il più possibile esaustiva la fase della identificazione. I supporti devono successivamente essere opportunamente imballati e conservati; su di essi devono essere apposte etichette e sigilli indicando il soggetto che ha raccolto le prove e le modalità ed il luogo in cui esse sono state reperite.

---

[167] Per un ulteriore approfondimento a livello statunitense sul tema si veda: E. Casey, *Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence Investigation,* 2004, p. 39, disponibile a seguente URL: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F43490_43FD3A9.pdf; O. Kerr, *Searches and Seizures in a digital world*, in *Harvard Law Review*, 2005,Vol. 119, p. 531; R. Nolan, C. O'Sullivan, J. Branson,C. Waits, *First Responders Guide to Computer Forensics, 2005*, disponibile al seguente URL: http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf; State of Maryland, Maryland State Police, Criminal Enforcement, Command, Computer Crime Unit, Computer Forensics Laboratori, *General Guidelines for Seizing Computers and Digital Evidence*, Disponibile al seguente URL: http://ccu.mdsp.org/Guidelines%20-%20Seizure%20of%20Digital%20Evidence.htm; State of New Jersey, Department of Law and Public Safety, Division of Criminal Justice, *New Jersey Computer Evidence Search and Seizure Manual*, disponibile al seguente URL: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf. A livello Europeo, si consiglia la lettura delle linee guida inglesi della Association of Chief Police Officers disponibili al seguente URL: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf.

In secondo luogo sarà necessario distinguere tra supporti non alterabili (cd e dvd non riscrivibili) e supporti soggetti a modifiche quali *hard disk*, *pen drive*, cd e dvd riscrivibili.

Il sequestro di supporti alterabili presuppone il compimento di un'operazione preliminare che costituisce requisito indispensabile al fine di garantire l'intangibilità dei dati in essi contenuti: l'impronta di *hash*[168]. L'*hash* è una funzione univoca operante in un solo senso (ossia, che non può essere invertita), attraverso la quale viene trasformato un documento di lunghezza arbitraria in una stringa di lunghezza fissa, relativamente limitata. Tale stringa rappresenta una sorta di "impronta digitale" del testo in chiaro, ed è detta valore di *hash* o *Message Digest*. Se il documento fosse alterato anche in minima parte, cambierebbe di conseguenza anche l'impronta. In altre parole, calcolando e registrando l'impronta, e successivamente ricalcolandola, è possibile mostrare al di là di ogni dubbio che i contenuti del *file*, oppure del supporto, abbiano subito o meno modifiche, anche solo accidentali. Pertanto, la registrazione e la ripetizione costante del calcolo degli *hash* sui reperti sequestrati costituiscono l'unico metodo scientificamente valido per garantire l'integrità e la catena di custodia dei reperti.

La Polizia Giudiziaria, prima di apporre i sigilli al materiale informatico, ha il compito di collegare il supporto oggetto del sequestro a un computer portatile su cui dovrà essere eseguito il comando che consente il calcolo dell'impronta di *hash*. Al termine dell'analisi del supporto sarà generata una sequenza di caratteri (tipicamente 16 oppure 20) che dovrà necessariamente venire trascritta sul verbale di sequestro, al fine di garantire la massima trasparenza nella successiva fase di analisi. Nella pratica gli algoritmi di *hash* più utilizzati, sono l'MD2, Md4, MD5 e SHA1; in particolare il calcolo dell'algoritmo MD5 (*Message*

[168] Per un approfondimento sul tema si veda, V. Klima, *Tunnels in Hash Functions: MD5 Collisions Within a Minute*, ricerca del marzo 2006, disponibile al seguente URL: http://eprint.iacr.org/2006/105.pdf.

Digest 5) permette di generare una stringa di 128-*bit*, mentre l'algoritmo SHA1 genera una stringa a 160-*bit*. L'abbinamento di questi due algoritmi dovrebbe evitare qualsiasi contestazione da parte del difensore, anche se sono stati riscontrati problemi di vulnerabilità, che rendono assai più facile del previsto la scoperta di collisioni al suo interno.[169]

Per tutte le operazioni di *hashing*, sarebbe opportuno utilizzare software *open source*, ovvero programmi di cui sia conosciuto il "codice sorgente" del software, al fine di consentire al consulente o al perito la verifica passo per passo delle operazioni di analisi, validazione ed eventuale confutazione.[170]

È consigliabile, inoltre, conservare una copia del software usato nella fase dell'acquisizione, perché solitamente i programmi sono aggiornati di frequente e potrebbero non essere più reperibili durante la fase del dibattimento.

Una procedura adottata molto raramente, ma non per questo meno utile, è quella di filmare, con almeno due telecamere, tutte le operazioni effettuate utilizzando un riferimento orario certo, in modo che sia le telecamere sia l'*hardware* usato per l'estrazione dei dati siano sincronizzati con tale riferimento. Inoltre, sarebbe utile effettuare una registrazione digitale dell'*output* dello schermo (*screencast*) di ogni operazione di acquisizione utilizzando uno dei numerosi software *open source* facilmente reperibili in Rete[171].

Ove non fossero adottate le procedure per garantire una corretta "catena di custodia" nella fase investigativa, i dati informatici contenuti nel supporto non avranno più i requisiti di certezza, genuinità e paternità. E', quindi, necessario

---

[169] C. Giustozzi, Hash *sempre più vulnerabili*, in *Nightgaunt*, disponibile al seguente URL: http://www.nightgaunt.org/testi/interlex/sha1.htm

[170] S. Zanero, E. Huebner, *The Case for Open Source Software in Digital Forensics*, in *Open Source Software for Digital Forensics*, 2010, Springer, p. 3. Il codice sorgente (spesso abbreviato sorgente) è un insieme di istruzioni appartenenti ad un determinato linguaggio di programmazione, utilizzato per realizzare un programma per computer. Lo scopo del codice sorgente è quello di essere eseguito, cioè di far compiere al computer le azioni descritte nel codice sorgente.

[171] Alcuni dei software più utilizzati sono: RecordMyDesktop (http://recordmydesktop.sourceforge.net/about.php) in caso di sistema operativo Linux, Windows Media Encoder (http://www.microsoft.com/windows/windowsmedia/forpros/encoder/default.mspx) in caso di sistema operativo Windows e Screen Movie Recorder (http://alphaomega.software.free.fr/screenmovierecorder/Screen%20Movie%20Recorder.html) in caso di sistema operativo Mac OS X.

avere un'elevata conoscenza informatica e disporre di una strumentazione tecnica adeguata, pianificando correttamente le attività di indagine da compiere, definendo in modo circostanziato gli obiettivi , il flusso di lavoro e le varie fasi.
Un cenno a parte meritano i casi in cui debbano essere acquisite interamente o meno siti *web*. Si è già detto in precedenza del progetto di ricerca denominato *hashbot* che consente di effettuare non solo il *download* delle pagine web, ma anche di validare la prova digitale attraverso l'utilizzo della funzione di *hash*.
Alternativamente sarà sempre possibile acquisire il sito *web* attraverso appositi *tools* liberamente disponibili in Rete (*HTTrack o Wget*) oppure accedendo al *file system* del server del sito da remoto.

2.4 Remote Forensics

Sia in Europa che negli Stati Uniti si è molto discusso circa la possibilità di introdurre un mezzo di ricerca della prova che consenta alle forze di polizia l'accesso remoto sugli strumenti informatici (*notebook, server, smartphone*) della persona sotto indagini.
Sempre più spesso accade che la Polizia Giudiziaria non conosce il luogo in cui è collocato il server che contiene i dati incriminati, in quanto l'indagato ha utilizzato risorse *hardware* o *software* distribuite in remoto per memorizzare e elaborare i dati digitali[172]. La popolarità del fenomeno del *cloud computing*[173], inoltre, ha reso ancor più difficile l'investigazione tradizionale: se è vero, infatti, che, grazie al *cloud computing*, chiunque può accedere a un determinato dato da qualunque parte del mondo o utilizzare un determinato applicativo senza averlo installato nel proprio computer, è anche vero che un criminale informatico può

[172] O. Kerr, *op. cit.*, p. 531.
[173] Per un approfondimento sulla tecnologia "Cloud Computing", si suggerisce una ricerca del centro di ricerca Pew, della Elon University, dal titolo *The Future of cloud computing*, disponibile al seguente URL: http://www.elon.edu/docs/e-web/predictions/expertsurveys/2010survey/PIP_Future_of_internet_2010_cloud.pdf.

decidere di memorizzare i suoi dati all'interno di un *server* dislocato al di fuori del territoriale nazionale e, magari, in uno Stato che non ha accordi di cooperazione giudiziaria con quello in cui risiede.

Gli Stati firmatari della Convenzione Cybercrime hanno dettato numerose disposizioni per contrastare tale fenomeno, tra cui vanno ricordati gli articoli 18 (*Production order*), 19 (*Search and seizure of stored computer data*) e 20 (*Real-time collection of traffic data*).

L'art. 18 della Convenzione Cybercrime[174] ha introdotto la possibilità per l'Autorità Giudiziaria di ordinare (*production order*) a qualunque soggetto (inclusi quindi i *provider*) di fornire i dati digitali presenti all'interno di un sistema informatico o di un *server* in suo possesso o sotto il suo controllo[175].

La convenzione utilizza i termini 'possession' e 'control' per indicare che sono obbligati a fornire i dati sia i soggetti che possono accedere fisicamente agli stessi, sia quelli che hanno la possibilità di accedervi da remoto[176]. L'ordine di produzione riguarda sia le informazioni di registrazione dell'utente a un determinato servizio (indirizzi IP e i *file* di *log*) sia i contenuti dei dati.

---

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

[175] Per un approfondimento sul tema, Marco Gercke, *Understanding Cybercrime: A Guide For Developing Countries*, p. 192, disponibile al seguente URL: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.

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

È stato osservato che tale misura potrebbe riguardare dati relativi a soggetti che si trovano al di fuori del territorio dello Stato, purché essi risultino abbonati con un fornitore che offre i propri servizi (anche) nello Stato richiedente[177].

Questa interessante interpretazione, tuttavia, è in contrasto con il principio di sovranità e in ogni caso potrebbe applicarsi ai soli dati di registrazione dell'utente (art. 18 sub b), poiché, per quanto riguarda i contenuti dei suoi *file* (art. 18 sub a), emerge chiaramente che l'ordine può eseguito solo nei confronti di *provider* presenti all'interno del territorio dello Stato richiedente[178].

L'art. 19 stabilisce che, nel caso in cui la Polizia Giudiziaria scopra che i dati digitali ricercati risiedono all'interno di un altro *server*, è autorizzata a estendere la ricerca su di esso, salvo che non si trovi al di fuori del territorio nazionale[179].

Tutavi anche nel caso in cui i dati siano memorizzati in un *server* che si trova all'interno del confine nazionale, si possono incontrare notevoli difficoltà nel trovare il dato ricercato a causa del volume di dati in esso contenuti.

In questo caso la Convenzione Cybercrime ha stabilito che gli investigatori possono ordinare all'amministratore di sistema di quel *server* di collaborare con la Polizia Giudiziaria e di fornire, ove possibile ("as is reasonable"[180]), le informazioni necessarie[181].

---

[177] F. Licata, *La Convenzione del Consiglio d'Europa sul cybercrime e le forme della cooperazione giudiziaria: una risposta globale alle nuove sfide della criminalità transnazionali*, in *Atti dell'incontro di Studio del Consiglio Superiore della Magistratura tenutosi a Roma il 19 settembre 2005*, p. 17, disponibile al seguente URL: http://appinter.csm.it/incontri/relaz/12009.pdf.

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

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

[180] Sul tema si veda l'art. 202 dell'*Explanatory Report* della Convenzione Cybercrime: "The provision of this information, however, is restricted to that which is "reasonable". In some circumstances, reasonable

L'art. 20 infine prevede la possibilità di raccogliere in tempo reale i *traffic data*[182]: i "dati di traffico" servono a monitorare in tempo reale l'attività dell'indagato in Rete (siti web visitati, intestazione delle *e-mail* scambiate, *downloads* effettuati).

La Convenzione Cybercrime indica due distinte metodologie operative per implementare la normativa nazionale: la prima è quella di prevedere che i *provider* siano obbligati a fornire un'interfaccia software alla Polizia Giudiziaria, che gli consenta di prelevare direttamente i dati utili all'indagine; la seconda è quella di stabilire uno specifico obbligo per i *provider* di raccogliere i *traffic data* su richiesta della Polizia Giudiziaria.

Come già osservato per il caso del sequestro della corrispondenza telematica, le misure previste dagli articoli 18 ("Production order") e 20 ("Real-time collection of traffic data") presentano delle caratteristiche molto simili all'attività di intercettazione, per la quale sono previste specifiche limitazioni conformemente all'articolo 8 della Convenzione europea per la tutela dei diritti dell'uomo[183].

Questi tre importanti strumenti offerti dalla Convenzione Cybercrime non sono stati presi in considerazione dalla normativa italiana in modo adeguato. Se è vero

---

provision may include disclosing a password or other security measure to the investigating authorities. However, in other circumstances, this may not be reasonable; for example, where the disclosure of the password or other security measure would unreasonably threaten the privacy of other users or other data that is not authorised to be searched. In such case, the provision of the "necessary information" could be the disclosure, in a form that is intelligible and readable, of the actual data that is being sought by the competent authorities".

[181] Un approccio simile è stato trovato durante gli incontri effettuati nel 2002 da un gruppo di esperti in crimini informatici che hanno redatto un modello legislativo per l'applicazione della Convenzione Cybercrime in tutti i Paesi aderenti al *Commonwealth*. Per ulteriori approfondimenti si veda la *section* 11 del "Model Law on Computer and Computer Related Crime", n. 202, disponibile al seguente URL: http://www.thecommonwealth.org/shared_asp_file/uploadedfile/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf.

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

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

che le attuali previsioni del codice di procedura penale offrono gli strumenti processuali per raggiungere i medesimi risultati (nomina dell'ausiliario di Polizia Giudiziaria ai sensi dell'art. 348 IV comma, richiesta di consegna ai sensi dell'art. 248 c.p.p. e intercettazione telematica ai sensi dell'art. 266-*bis* c.p.p.), è pur vero che la legge di ratifica della Convenzione Cybercrime ha perso un'importante occasione per poter effettuare alcune doverose precisazioni in materia. Ad esempio, l'obbligo per i *provider* di fornire un'interfaccia software alla Polizia Giudiziaria avrebbe potuto velocizzare l'attività di indagine e garantire un minor rischio di alterabilità del dati. Nella prassi attuale, infatti, i *provider* forniscono le informazioni relativi ai *file* di *log* o all'indirizzo IP dell'indagato, estrapolando i dati richiesti, senza nessun accorgimento previsto dalle *best practice* di *digital forensics.*

Oltre agli strumenti citati, in molti Paesi europei sono al vaglio progetti di legge per garantire l'accesso remoto da parte della Polizia Giudiziaria sui computer degli indagati[184]. Negli Stati Uniti, il *Federal Bureau of Investigation* (FBI), invece, ha già sperimentato con successo l'utilizzo di un particolare tipo di *spyware* (*CIPAV*[185]) che ha la funzione di raccogliere informazioni riguardanti le attività *on line* dell'indagato e di ritrasmetterle in tempo reale agli investigatori[186].

Da queste breve panoramica sulla *remote forensics,* emerge chiaramente come la possibilità di effettuare l'attività investigativa rimanendo davanti allo schermo di un computer e senza che l'indagato ne sia a conoscenza, rappresenti un indiscutibile vantaggio e una garanzia di successo per l'indagine.

---

[184] J. Blau, *Debate rages over German government spyware plan*, 5 maggio 2007, in *Computerworld Security*, disponibile al seguente URL: http://www.computerworld.com/s/article/print/9034459/Debate_rages_over_German_government_spyware_plan?taxonomyName=Security&taxonomyId=17

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

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

Tuttavia, i vantaggi di questa metodologia investigativa non possono far passare inosservato il fatto che un'attività così invasiva potrebbe pregiudicare alcuni diritti fondamentali del soggetto sottoposto all'indagine. È necessario, pertanto, prestare la massima attenzione alla tutela di tutti gli interessi in gioco, bilanciando attentamente le esigenze di prevenzione e di sicurezza con la tutela dei diritti fondamentali, come quello della privacy e delle garanzie dell'indagato.
In questo senso è interessante notare come la giurisprudenza di legittimità non si sia posta il problema di ritenere valido il decreto del Pubblico Ministero, ai sensi dell'art. 234 c.p.p., di acquisizione in copia attraverso l'installazione di un captatore informatico della documentazione informatica memorizzata nel personal computer in uso all'imputato e installato presso un ufficio pubblico. La Suprema Corte ha, infatti, evidenziato come il provvedimento del Pubblico Ministero non avesse riguardato un flusso di comunicazioni, ma la semplice estrapolazione di dati già formati e contenuti nella memoria del "personal computer" ossia "un flusso unidirezionale di dati" confinati all'interno dei circuiti del computer[187].
La Corte ha, altresì, escluso che, nella specie, "dovesse essere osservata la disciplina prevista per gli accertamenti tecnici irripetibili, atteso che l'attività di riproduzione dei *file* memorizzati non aveva comportato l'alterazione, nè la distruzione dell'archivio informatico, rimasto immutato, quindi consultabile ed accessibile nelle medesime condizioni, anche dopo l'intervento della polizia giudiziaria". Secondo gli Ermellini si è trattato di un'attività sempre reiterabile, alla cui esecuzione non era necessaria la partecipazione del difensore, poichè la stessa avrebbe potuto essere compiuta una seconda volta qualora si fosse approdato ad uno sviluppo dibattimentale del procedimento, cosa che poi non avvenne poiché fu scelto il "rito abbreviato".

[187] Cass. Pen., Sez. V, 14 ottobre 2009, n. 16556 (rv. 246954).

La difesa, invece, aveva eccepito che il decreto del Pubblico Ministero, pur autorizzando una mera acquisizione in copia di atti, avrebbe costituito, di fatto, la premessa per condurre un'attività di intercettazione di comunicazioni informatiche ai sensi dell'art. 266-*bis* c.p.p.. Il decreto, infatti, aveva disposto la registrazione non solo dei *file* esistenti, ma anche dei dati che sarebbero stati inseriti in futuro nel personal computer, in modo da acquisirli periodicamente. A conferma di tale tesi, sono state evidenziate le concrete modalità esecutive del decreto, consistite nell'installazione, all'interno del sistema operativo del personal computer, di un captatore informatico (ghost) in grado di memorizzare i *file* già esistenti e di registrare in tempo reale tutti i *file* in via di elaborazione, in tal modo innescando un monitoraggio occulto e continuativo del computer dell'indagato (protrattosi per oltre otto mesi).

Due osservazioni sorgono spontanee: in primo luogo, la Corte non sembra considerare come la presunta ripetibilità presupponga l'assenza di un intervento sul personal computer da parte del soggetto indagato in un momento successivo alla fase di captazione. In secondo luogo, la Corte, per escludere la disciplina delle intercettazioni telematiche, si limita a evidenziare come il flusso di comunicazioni acquisito non abbia riguardato una conversazione telematica tra due soggetti, ma solo un "flusso di comunicazioni unilaterale". Pur condividendo tale impostazione, non si può non rilevare, da un lato, come l'art. 266-*bis* non sia chiaro sul punto, poichè prevede che la captazione riguardi "un flusso di comunicazione relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi" e, dall'altro, come sia estremamente delicata la scelta di stabilire che un'operazione così invasiva come il monitoraggio occulto di un personal computer per un periodo prolungato di tempo possa essere autorizzato senza il vaglio del Giudice per le indagini preliminari.

2.5 Le intercettazioni telematiche: disciplina italiana e statunitense a confronto

Se le intercettazioni telefoniche sono state lo strumento di indagine più proficuo ed efficace in tutte le grandi indagini di questi ultimi anni, è facile prevedere il ruolo che avranno le intercettazioni telematiche nel prossimo futuro: attraverso di esse è possibile controllare, infatti, l'intero flusso di dati (*e-mail* inviate e ricevute, siti *web* visitati, comunicazioni *VoIP* non criptate, *download* ed *upload* di *file,* conversazioni in *chat room*) di un dato sistema informatico.

Le recenti statistiche dimostrano che, a livello europeo, l'Italia è il paese che fa più largo uso dell'intercettazione come mezzo di ricerca della prova nelle indagini[188]. Basti pensare che negli ultimi quattro anni il Ministero di Giustizia italiano ha speso un miliardo e 800 milioni di dollari (1,3 miliardi di euro) per poter conseguire il seguente primato europeo: un cittadino ogni 500 abitanti è intercettato per un totale di quasi 150.000 richieste di intercettazioni all'anno.

Questi dati riguardano principalmente le intercettazioni telefoniche e non quelle telematiche, in quanto, in Italia, anche se ogni giorno sono scambiate 464 milioni di *e-mail*, non sono ancora sufficientemente note le enormi potenzialità di questo tipo di intercettazioni[189].

Negli Stati Uniti, le statistiche relative alle intercettazioni sono molto diverse, in quanto le richieste autorizzate di intercettazione all'anno sono 1861 di cui 386 a livello federale e le restanti 1475 a livello statale[190]. Solo un cittadino su 165.000 abitanti è intercettato.

Una *e-mail*, a differenza di una telefonata, può essere immediatamente indicizzata con chiavi di ricerca determinate, contiene spesso allegati potenzialmente utili, e rende più facile la comprensione del contesto del discorso.

---

[188] John Leyden, Italy tops global wiretap league, in http://www.theregister.co.uk/2007/03/07/wiretap_trends_ss8/; per un approfondimento sui costi delle intercettazioni in Italia: http://punto-informatico.it/1860408/Telefonia/News/intercettazioni-governo-vuole-risparmiare.aspx

[189] Fonte contactlab: http://www.en.contactlab.com/download/CONR09/CONR09_europe_extract_en.pdf.

[190] Fonte U.S. Courts: http://www.uscourts.gov/wiretap08/Table2.pdf.

Se due commercianti di droga dovessero darsi via telefono un appuntamento in un determinato luogo ad una certa ora, come è possibile sapere se durante quell'incontro sarà consegnato un ingente quantitativo di droga oppure se i due andranno soltanto a bere un caffé per ricordare "i vecchi tempi"? Intercettando una singola *e-mail*, invece, vi è la possibilità di raccogliere un numero maggiore di informazioni utili all'indagine anche perché, sempre più spesso, accade che essa contenga anche tutti i precedenti messaggi che gli utenti si sono scambiati tra loro.

Negli Stati Uniti le intercettazioni telematiche sono regolate dall'*Electronic Privacy Communications Act* emanato nel 1986[191]. Con l'emanazione di questo atto, è stato chiarito che ogni intercettazione che non rispetti le condizioni previste dalla legge, deve essere considerata illegale e, oltre a comportare l'inutilizzabilità delle informazioni così acquisite all'interno del processo, può determinare un'azione di risarcimento del danno rivolta nei confronti del responsabile.

Questa normativa è divisa in tre atti normativi distinti: il primo è dedicato specificamente alle intercettazioni delle comunicazioni telematiche (*Electronic Privacy Communications Act*, 18 U.S.C. § 2510), il secondo regola la possibilità di accedere ai contenuti memorizzati all'interno di un computer o di un server (*Stored Communications* Act, 18 U.S.C. § 2701) e il terzo riguarda la possibilità di monitorare gli accessi alla Rete da parte degli utenti, senza tuttavia poter conoscere il contenuto delle loro comunicazioni (*Pen Register Act*, 18 U.S.C. § 206).

Teoricamente, tra questi tre atti, solo il primo riguarda specificamente le captazioni in tempo reale di informazioni digitali; tuttavia, ritengo opportuna una trattazione congiunta, in quanto, come già detto per il caso della corrispondenza elettronica, è molto sottile la differenza tra l'intercettazione di una *e-mail*

[191] *Electronic Privacy Communications Act*, 18 U.S.C. § 2510, disponibile al seguente URL: http://www.law.cornell.edu/uscode/18/usc_sup_01_18_10_I_20_119.html.

attraverso un sistema di duplicazione della casella di posta elettronica e un accesso alla casella di posta elettronica nella forma prevista dallo *Store Communications Act*.

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

Infatti, nel caso delle informazioni memorizzate all'interno di un computer o di un *server* (*Stored Communication Act*), vi sono alcune specifiche eccezioni: nel caso in cui il *provider* si renda conto, per circostanze casuali, di un concreto e serio pericolo di vita di un soggetto, nel caso in cui debba tutelare i suoi diritti qualora fosse vittima di una frode[192] o nel caso in cui debba informare il *National Centre for Missing and Exploted Kids* per un'ipotesi di pedofilia *on line*, può accedere ai contenuti memorizzati dal suo utente senza alcun mandato.

Inoltre è possibile che le sole informazioni relative all'identità di un determinato utente (e non quindi i contenuti) possano essere ottenute anche attraverso una diffida (*subpoena*) che, tuttavia, non può essere fatta da un privato, ma deve comunque essere richiesta dall'Autorità Giudiziaria.

Nel caso del monitoraggio, invece, il *Pen Register Act*, ha subito sensibili modifiche con il *Patriot Act* e con l'introduzione della *National Security Letter*, che hanno consentito una deroga notevole al principio generale.

La *National Security Letter* è una forma di *subpoena* di natura amministrativa, utilizzata dal *Federal Bureau of Investigation*, in forza della quale viene concessa a tale organo investigativo la possibilità di richiedere il monitoraggio di alcune informazioni (nome dell'utente, indirizzo, registro delle transazioni, intestazioni

[192] *United States v. Harvey,* 540 F.2d 1345, 1350-52 (8th Cir. 1976)

delle *e-mail*), senza sostanzialmente alcuna previa autorizzazioni da parte del Giudice[193].

In Italia, la legge n. 547, del 23 settembre 1993, oltre ad aver introdotto la disciplina relativa ai reati informatici, ha previsto anche uno specifico mezzo di ricerca della prova, vale a dire le intercettazioni del flusso di comunicazioni relativo a sistemi informatici o telematici[194].

Preliminarmente occorre chiarire cosa si intende per sistema informatico e sistema telematico, in quanto, ad oggi, a livello nazionale non esiste alcuna definizione normativa. Al di là delle definizioni che la giurisprudenza di legittimità ha cercato di elaborare con risultati non sempre soddisfacenti[195], possiamo dire che:

- per sistema informatico si intende ogni elaboratore elettronico che utilizzi un microprocessore per l'elaborazione di dati binari per l'esecuzione di una qualsiasi operazione in grado di esprimere un particolare significato per l'utente.
- per "sistema telematico", si intende l'insieme di più sistemi informatici collegati tra loro per lo scambio di informazioni, purché siano connessi in

[193] La *National Security Letter* dava anche la facoltà al *Federal Bureau of Investigation* (FBI) di segretare l'attività di monitoraggio fino alla dichiarazione di incostituzionalità avvenuta con il caso Ashcroft v. ACLU, 542 U.S. 656, 665-66 (2004).

[194] Tale legge, infatti, ha aggiunto al codice di procedura penale l'art. 266-*bis* ed il comma 3-*bis* dell'art. 268, accostando alle intercettazioni telefoniche ed ambientali questo nuovo tipo di intercettazione. Non essendo questa la sede per un approfondimento sui profili processuali delle intercettazioni, si suggeriscono i seguenti volumi: E. Aprile e F. Spiezia, *Le intercettazioni telefoniche ed ambientali. Innovazioni tecnologiche e nuove questioni giuridiche,* 2004, Milano, Giuffrè; Atti del Convegno tenutosi a Milano il 5-7 ottobre 2007: "*Le intercettazioni di conversazioni e comunicazioni. Un problema cruciale per la civiltà e l'efficienza del processo e per le garanzie dei diritti*, 2009, Giuffrè, Milano; C. Parodi, *La disciplina delle intercettazioni telematiche*, in *Dir. pen. e proc.*, 2003, p. 889; L. Filippi, *L'intercettazione di comunicazioni*, 1997, Milano, Giuffrè; C. Maioli e R.Cugnasco, *Profili normativi e tecnici delle intercettazioni. Dai sistemi analogici al voice over IP*, 2008, Milano, Gedit.

[195] Cass. Pen., Sez. V, n. 31135 del 6.7.2007. per la quale "deve ritenersi 'sistema informatico', […] un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di 'codificazione' e 'decodificazione' - dalla 'registrazione' o 'memorizzazione', per mezzo di impulsi elettronici, su supporti adeguati, di 'dati', cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare 'informazioni', costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente".

modo permanente e lo scambio di informazioni sia il mezzo necessario per conseguire i fini operativi del sistema.

La convenzione Cybercrime, sottoscritta a Budapest il 23 novembre del 2001 e recentemente ratificata in Italia con la legge 48/08, non distingue invece tra sistema informatico e telematico stabilendo che per sistema informatico si intende qualsiasi apparecchiatura, dispositivo, gruppo di apparecchiature o dispositivi, interconnesse o collegate, una o più delle quali, in base ad un programma, esegue l'elaborazione automatica di dati"[196].

Partendo dal presupposto che oggi un personal computer è un oggetto privo di utilità se non connesso alla Rete, non si può non condividere tale definizione.

In Italia, l'intercettazione è disciplinata dal codice di procedura penale all'articolo 266-*bis*, mentre l'accesso ai dati digitali, contenuti in un *server* o in un computer, avviene (o dovrebbe avvenire, vista la recente giurisprudenza citata nel paragrafo precedente) attraverso il sequestro.

Dal punto di vista procedurale la disciplina non si differenzia in modo significativo da quella statunitense. Infatti, il Pubblico Ministero chiede al Giudice delle indagini preliminari (o al Giudice nel corso del dibattimento o al Giudice di pace in caso di reati di sua competenza) di emettere il decreto di autorizzazione allo svolgimento delle operazioni. Ove, invece, vi fossero ragioni di urgenza (art. 267 c.p.p.), sarebbe legittimo un provvedimento di autorizzazione del Pubblico Ministero: questi, tuttavia, deve tassativamente richiedere la convalida al Giudice competente entro 24 ore dal suo provvedimento e il Giudice deve autorizzazione tale intercettazione entro 48 ore dalla richiesta.

Una volta autorizzato, il Pubblico Ministero dispone l'intercettazione con decreto, indicando modalità e tempi di esecuzione delle operazioni (massimo quindici giorni, che diventano quaranta in caso di intercettazioni preventive).

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

Proprio sui tempi di esecuzione potrebbe porsi un problema nell'applicazione delle intercettazione telematica. Se, infatti, l'arco temporale in cui è ammissibile compiere delle intercettazioni è di 40 giorni, come si può considerare l'intercettazione di una email che contiene al suo interno una precedente *e-mail* di due mesi prima?

Come già anticipato sopra, nella comunicazioni telematiche si è soliti, attraverso il comando "rispondi" o "rispondi a tutti", conservare le *e-mail* precedentemente inviate. Se è indubbio che tale prassi favorisce gli investigatori, ne è meno certa la legittimità da un punto di vista procedurale.

Nella scarsa giurisprudenza sul tema delle intercettazioni telematiche un problema del genere non si è ancora posto, ma merita di non essere sottovalutato.

Tornando alle intercettazioni telematiche *tout cout*, l'articolo 266 *bis* c.p.p., quanto al reato che giustifica tale mezzo istruttorio, fa espressa menzione di due tipologie di fattispecie penali: da un lato vi sono i reati previsti specificamente dall'articolo 266 c.p.p. [197] e dall'altro quelli commessi mediante l'impiego di tecnologie informatiche o telematiche.

Quanto al secondo gruppo, la dottrina ha fornito due interpretazioni: secondo alcuni la norma considera solo i *computer crime* (crimini introdotti dalla legge 547/1993, in cui lo strumento informatico è elemento costitutivo della

[197] Quanto al primo gruppo, trattasi dei seguenti reati:
a) delitti non colposi per i quali è prevista la pena dell'ergastolo o della reclusione superiore nel massimo a quattro anni determinata a norma dell'articolo 4 c.p.p.;
b) delitti contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni determinata a norma dell'articolo 4 c.p.p.;
c) delitti concernenti sostanze stupefacenti o psicotrope;
d) delitti concernenti le armi e le sostanze esplosive;
e) delitti di contrabbando;
f) reati di ingiuria, minaccia, usura, abusiva attività finanziaria, abuso di informazioni privilegiate, manipolazione di mercato, molestia o disturbo alle persone col mezzo del telefono;
f-bis) delitti previsti dall'articolo 600 ter, terzo comma, del codice penale, anche se relativi al materiale pornografico di cui all'articolo 600 quater del medesimo codice.

descrizione normativa); secondo altri si applica a tutti i *computer related crime* (crimini d'ogni sorta purché commessi mediante tecnologie informatiche)[198].

Secondo i sstenitori dell'interpretazione restrittiva[199], non vi sarebbe altra possibilità ermeneutica dal momento che il canone costituzionale delle intercettazioni, ossia l'articolo 15 della Costituzione, impone un'interpretazione necessariamente restrittiva della disposizione in esame. Ne deriva che le intercettazioni non sono ammissibili se non nel rispetto di tre criteri fondamentali, conformemente all'articolo 8 della Convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali del 4 novembre 1950, e all'interpretazione di tale disposizione data dalla Corte europea dei diritti dell'uomo:

(i) una normativa di dettaglio che precisi limiti e strumenti di applicazione;

(ii) l'esigenza del provvedimento dell'autorità giurisdizionale che verifichi il rispetto di tale fondamento giuridico;

(iii) la conformità ad uno degli scopi legittimi, tra cui il fine di prevenire e reprimere i reati, indicati nella Convenzione.

Affermare che l'intercettazione informatica è esperibile in riferimento a qualsiasi reato vorrebbe dire rilevare un preoccupante vuoto normativo in tale (necessaria) regolamentazione. Ad esempio, si dubita del rispetto del principio di uguaglianza, stante il fatto che detta regolamentazione fa si che per certi reati di pari gravità commessi con lo strumento informatico, ma non ricompresi nel sopra riportato elenco dell'art. 266 c.p.p., è possibile per l'Autorità Giudiziaria disporre intercettazione telematica e non intercettazione telefonica o ambientale.

---

[198] L. Lupária, *La disciplina processuale e le garanzie difensive,* in L. Lupária - G. Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, 2007, Milano, Giuffrè, p. 163

[199] L. Filippi, *op. cit.*, p. 82.

Secondo l'interpretazione estensiva[200], invece, la lettera della norma non lascia spazio ad alcuna limitazione riguardo al titolo del reato, ma soltanto, come già ribadito, riguardo al mezzo attraverso cui l'illecito è commesso: sarebbe tale uso del mezzo telematico o informatico a giustificare una risposta investigativa di pari livello. Ne discenderebbe, come detto, la possibilità di disporre intercettazioni telematiche ed informatiche e non telefoniche o ambientali in relazione ad una pluralità di reati non catalogati ai sensi dell'articolo 266 c.p.p. Tale disparità troverebbe giustificazione proprio nell'uso, da parte del reo, dello strumento informatico che qualificherebbe come particolarmente insidiosa la sua condotta. In sostanza, i sostenitori della tesi estensiva ritengono irragionevole, nel momento in cui detto strumento è utilizzato per offendere, non utilizzarlo anche per reprimere tale offesa. L'uso dello strumento informatico diviene allora di per sé solo portatore di uno specifico disvalore o, meglio, di una specifica offensività che giustifica particolari strumenti di indagine.

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

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

[200] C. Parodi, *op. cit.,* p. 889; A. Camon, *Le intercettazioni nel processo penale*, 1996, Milano, Giuffrè, p. 67.

Un discorso a parte merita il *Foreign Intelligence Surveillance Act* del 1978[201] che definisce le procedure per la sorveglianza elettronica e la raccolta di informazioni, relative a cittadini americani, al fine di proteggere gli Stati Uniti contro attuali e potenziali attacchi, sabotaggi o possibili atti terroristici.

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

Da menzionare, infine, il *Communications Assistance for Law Enforcement Act* 47 U.S.C. § 1001-1021)[202], che impone alle compagnie telefoniche di implementare la propria infrastruttura tecnologica per poter favorire eventuali attività di sorveglianza elettronica da parte delle forze dell'ordine[203].

In estrema sintesi, la vera differenza tra la disciplina italiana delle intercettazioni e quella americana non è tanto nella procedura, quanto nell'effettiva applicazione. Negli Stati Uniti vi è una massiccia applicazione dei sistemi di monitoraggio preventivo, mentre in Italia vi è un ampio utilizzo delle intercettazioni per ora solo telefoniche, ma che diventeranno sicuramente telematiche nei prossimi anni.

Nonostante vi siano numerose somiglianze nella procedura, esse non bastano per creare una forma di cooperazione che possa risultare più efficace di quella prevista dagli "Accordi sulla mutua assistenza giudiziaria tra gli Stati Uniti e

---

[201] *Foreign Intelligence Surveillance Act* (50 U.S.C. § 1801-1885C) disponibile al seguente URL: http://www.law.cornell.edu/uscode/50/usc_sup_01_50_10_36.html.

[202] Communications Assistance for Law Enforcement Act (47 U.S.C. § 1001-1021) disponibile al seguente URL: http://www.law.cornell.edu/uscode/uscode47/usc_sup_01_47_10_9_20_I.html.

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

l'Italia del 3 maggio 2006", che sostituiscono gli accordi del 1982, al fine di adeguarli al trattato sottoscritto dagli Stati Uniti con l'Unione europea il 25 giugno 2003[204].

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

Per un paese come l'Italia affrontare un processo rogatoriale per ottenere tali informazioni potrebbe diventare molto complesso: ogni giorno, mediamente, in Italia vengono autorizzate 464 intercettazioni, mentre negli Stati Uniti ne vengono autorizzate 6.

Sulla difficoltà di trovare una forma di cooperazione su questo tema, già il Consiglio d'Europa, nel 2001, in sede di ratifica della Convenzione Cybercrime, aveva evidenziato il problema, nella sua relazione illustrativa all'articolo 32 , che copre la materia dell' "accesso transfrontaliero ai contenuti memorizzati all'interno di un computer". Il Consiglio affermava laconicamente che permettere ad un Stato membro della Convenzione di accedere ai dati contenuti in un computer, memorizzati da un utente o da una società di un altro Stato membro, è "questione particolarmente complessa che non è possibile affrontare in carenza di esperienze consolidate in materia"[205].

2.6 Modalità operative delle intercettazioni telematiche

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

---

[204] Il testo del trattato è disponibile al seguente URL: http://www.giustizia.it/giustizia/it/mg_1_3.wp;jsessionid=EA2996918987F14F07198599BB365BD9.ajpAL02?detail=y&tabait=y&tab=a&ait=AIT32552&aia=AIA32731

[205] Per un approfondimento sul tema, M. Gercke, *Understanding Cybercrime: A Guide For Developing Countries*, disponibile al seguente URL: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.

Da un punto di vista tecnico, la possibilità di utilizzare tecniche di crittografia per nascondere le informazioni che transitano in Rete abbinate a sistemi *peer to peer* per la comunicazione vocale, rende estramente difficile anche per i consulenti più esperti poter intercettare e conseguentemente decifrare i pacchetti di informazioni che vengono scambiati tra gli utenti[206].

Dal punto di vista giuridico, la collocazione fisica fuori dal territorio nazionale dei *servers* dei principali gestori di servizi *VoIP* (*Skype, Gtalk, Windows Live Messenger*) e di posta elettronica (*@gmail.com*, *@yahoo.com*, *@live.com*) comporta per l'Autorità Giudiziaria la necessità di avviare un procedimento rogatoriale che molto spesso non coincide con i tempi di un'indagine penale.

Da un punto di vista pratico, la conseguente impossibilità di poter intercettare i dati direttamente presso il *provider*, obbliga la Polizia Giudiziaria ad utilizzare sistemi molto più elaborati che comportano un notevole dispendio economico sia in termini di *hardware* (*sistemi embedded* da utilizzare come sonde[207]), che in termini di risorse umane (consulenti tecnici qualificati).

Le modalità operative sono condizionate dalle caratteristiche del sistema, dal tipo di comunicazioni e dall'oggetto delle stesse. I punti più vulnerabili di un'intercettazione sono i punti di gestione e di concentrazione del traffico di Rete come i *routers*[208], le *gateways*[209] o i *servers* di rete [210].

---

[206] T. Berson, *Skype Security Evaluation*. *Anagram Laboratories 18 october 2005*, ricerca disponibile al seguente URL: http://www.anagram.com/berson/skyeval.pdf.Va rilevato, tuttavia che vi sono autori che sostengono invece la possibilità di utilizzare strumenti tecnici per intercettare conversazioni VoIP anonime: S. Chen, X. Wang, S. Jajodia, *Tracking anonymous peer-to-peer VoIP calls on the Internet*, in *Conference on Computer and Communications Security archiveProceedings of the 12th ACM conference on Computer and communications security*, 2005, ACM, New York, p. 81-91.

[207] In informatica, con il termine sistema *embedded* (generalmente tradotto in italiano con sistema immerso o incorporato) si identificano genericamente tutti quei sistemi elettronici a microprocessore progettati appositamente per una determinata applicazione (special purpose) ovvero non riprogrammabili dall'utente per altri scopi, spesso con una piattaforma hardware *ad hoc*, integrati nel sistema che controllano ed in grado di gestirne tutte o parte delle funzionalità. Alcuni di questi modelli sono commercializzati dalla società statunitense Win Enterprise (www.win-ent.com) o dalla società Lex System di Taiwan (www.lex.com.tw).

[208] Il *Router* (dall'inglese instradatore) è un dispositivo responsabile dell'instradamento di pacchetti di dati attraverso una Rete.

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

In generale, l'intercettazione telematica può avvenire:

- attraverso la collaborazione dei *provider* di servizi: qualora il gestore del servizio abbia una sede operativa in Italia, l'Autorità Giudiziaria, una volta emesso il decreto di intercettazione, consegna alla Polizia Giudiziaria l'eventuale delega e un documento ("griglia") contenente i dati tecnici. La Polizia Giudiziaria consegna la "griglia" al *provider*, il quale ha l'obbligo di mettere a disposizione un collegamento dedicato (RES[211]) che porta i dati sul *server* della sala ascolto della Procura della Repubblica, in cui avvengono tecnicamente le intercettazioni. Un esempio di questa forma di collaborazione avviene nel caso dell'intercettazione di corrispondenza elettronica: il gestore del servizio, una volta ricevuta la "griglia", provvederà a duplicare la casella di posta elettronica dell'indagato e inoltrerà tutte le *e-mail* direttamente sul *server* della Procura della Repubblica;
- presso i privati o presso i *provider* di servizi: questo tipo di intercettazione avviene nel caso in cui non vi sia la collaborazione del gestore del servizio di *hosting* in cui sono memorizzati i dati o qualora sia necessario effettuare un'intercettazione dell'intero flusso di dati trasmesso dal soggetto indagato. In questo caso, viene svolto un filtraggio sull'indirizzo IP[212]. Qualora l'utente

---

[210] J. F. Korose e K. W. Ross, *La sicurezza nelle reti,* in *Reti di calcolatori e internet,* 2005, Milano, Pearson Addison Wesley, pp. 592-593.

[211] Alcuni chiarimenti sul funzionamento della linea RES sono stati dati durante la seduta della Commissione Giustizia del 29 novembre 2006. Il resoconto stenografico della seduta è disponibile al seguente URL: http://www.senato.it/documenti/repository/commissioni/stenografici/15/comm02/02a-20061129p-IC-0194.pdf. Occorre, inoltre, segnalare che, per quanto riguarda gli impianti e le attrezzature utilizzabili per procedere alle intercettazioni, l'articolo 268, comma 3 bis, c.p.p. prevede espressamente che la regola sia affidare a privati l'effettuazione delle operazioni, laddove tale ipotesi è considerata una eccezione nei casi di intercettazioni telefoniche. Pertanto è possibile effettuare attività di intercettazione telematica, mediante impianti appartenenti a privati, allorché ricorra l'esigenza di disporre di peculiari strutture o di speciali apparecchiature.

[212] Se il computer da cui sono originate le conversazioni è connesso ad una LAN, avrà un IP privato interno alla stessa, e un IP pubblico, ma in questo caso tutti i dati in transito dalla rete LAN utilizzeranno lo stesso IP pubblico e non sarà possibile, durante l'intercettazione, dividere il traffico dei vari terminali attivi. V. S. Destito, G. Dezzani, C. Santoriello, *Il diritto penale delle nuove tecnologie*, 2007, Padova, Cedam, p. 445.

utilizzi linee fisse come ADSL, al posto dello *switch*[213] viene messa una sonda detta *Front End* collegata ad una porta denominata *span port*[214] che riceve in copia tutto il traffico scambiato (in entrambe le direzioni quindi) dall'apparato di accesso che gestisce la connessione finale dell'utente. La sonda filtra solo il traffico rilevante per il decreto di intercettazione in base all'indirizzo IP del soggetto indagato. Il flusso viene poi scaricato localmente su disco e trasferito tramite la linea RES ad alta velocità verso la postazione di decodifica (*Back End*)[215]. La postazione di decodifica ha un modulo che interpreta e ricostruisce i protocolli in modo che l'addetto alla postazione possa vedere, ad esempio, i messaggi di posta elettronica inviati e ricevuti, le pagine web visitate, la comunicazione *VoIP* nel caso in cui non sia criptata[216].

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

[213] Uno *switch* (dall'inglese commutatore) è un dispositivo di rete che inoltra selettivamente i frame ricevuti verso una porta di uscita.
[214] A. Ghilardini, G. Faggioli, *op. cit.*, p. 72.
[215] Qualora non si riesca ad avere accesso fisico allo *switch* è possibile procedere con un attacco "man in the middle": Se "X" e "Y" sono i due interlocutori "Z" che è l'*attacker* cercherà di deviare il flusso tra X e Y al fine di trovarvisi in mezzo per poterlo intercettare comodamente. Per attuare un attacco "man in the middle" è necessario utilizzare delle tecniche di *ARP spoofing*. Per un approfondimento si veda A. Ghilardini, G. Faggioli, *op. cit.*, p. 73; D. D'Agostini, *Le indagini sulle reti informatiche*, in *Diritto penale dell'informatica*, 2007, Forlì, Experta Edizioni, p. 212.
[216] La Polizia Giudiziaria dispone anche di uno strumento *hardware* denominato "tele-monitor" che consente di intercettare l'utente nel caso egli decida di accedere alla Rete da diversi punti e con diverse tipologie di collegamento. Per un approfondimento sul tema si consiglia di consultare il sito dell'ufficiale dei Carabinieri Marco Mattiucci (Comandante della Sezione Telematica del RIS di Roma che svolge attività scientifico forense nello specifico settore dei crimini ad alta tecnologia) disponibile al seguente URL: www.marcomattiucci.it.

della maggioranza dei dati che ai fini delle indagini è generalmente inutile) ed eventuale correlazione dei dati acquisiti con l'utente intercettato.

Il sistema operativo utilizzato per effettuare un'intercettaziona telematica è, generalmente, *Linux,* in quanto tale sistema ha subito una rapidissima evoluzione nel campo del *networking*. Molte delle funzioni necessarie ad effettuare una captazione di dati digitali, infatti, sono già incorporate nel sistema operativo[217].

L'applicativo più importante è invece l'analizzatore di rete (*sniffer*). Esso è un software adatto all'analisi dei dati (pacchetti) che transitano su una rete, in quanto fornisce una panoramica dettagliata di tutto ciò che accade nella rete locale ed è in grado di individuare i protocolli di rete utilizzati per i vari tipi di comunicazione. Alcuni analizzatori di protocollo permettono di acquisire i *log* da altri programmi per i prodotti di libero accesso e di applicare dei filtri per rendere selettiva la cattura del traffico.

Gli *sniffer* intercettano i singoli pacchetti, decodificano i dati contenuti, e rendono disponibili le informazioni sul mittente, il destinatario, il tipo di protocollo, l'applicazione e, soprattutto, il contenuto in forma di testo, audio e video[218]. Tra quelli più utilizzati si ricordano *Ethereal*[219] (), Wireshark[220] (http://www.wireshark.org/) e *Tcpdump*[221].

Vi sono, inoltre, appositi programmi che estraggono dal flusso di comunicazioni alcune informazioni, come ad esempio, *login*, *password* e *file* trasferiti[222].

Come già osservato[223], l'intercettazione dei sistemi *VoIP* criptati, costituisce uno dei maggiori problemi sia da un punto di vista giuridico (i gestori del servizio

---

[217] A. Ghilardini, G. Faggioli, *op. cit.*, p. 75;

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

[219] Ulteriori informazioni su Ethereal sono disponibili al seguente URL: http://www.ethereal.com.

[220] Ulteriori informazioni su Wireshark sono disponibili al seguente URL: http://www.wireshark.com.

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

[222] Due programmi che svolgono a tale funzione sono: *Chaos reader* (http://chaosreader.sourceforge.net) e *Ettercap-ng* (http://ettercap.sourceforge.net/).

non hanno sede nel territorio del soggetto intercettato e non accettano di collaborare con le forze di polizia), sia da un punto di vista tecnico (i gestori del servizio sostengono di non essere in grado di penetrare nel loro stesso sistema[224]).

La soluzione potrebbe essere quella di installare nel computer del soggetto indagato, a sua insaputa, un software di *remote forensics* attraverso, ad esempio, l'invio di un *trojan horse*[225].

Un software di *remote forensics*[226] potrebbe permettere alla Polizia Giudiziaria di ricercare le informazioni sul computer del soggetto, registrare le conversazioni effettuate tramite i sistemi *VoIP*[227], recuperare le chiavi di decifratura utilizzate per criptare i *file*[228] e addirittura attivare le periferiche audio/video per identificare il sospettato e il luogo in cui si trova[229]:

---

[223] Sul tema si veda ancora: D. Bem, F. Feld, E. Huebner, and O. Bem, *Computer Forensics - Past, Present And Future*, in *The Journal of Information Science & Technology*, 2008, Vol. 5, p 43; M. Bates, T. Min, *Problems With Wiretapping of VoIP Services*, disponibile al seguente URL http://www.colorado.edu/policylab/Papers/Secure_Voip_writeup%20v3_2%20_2_.pdf

[224] La società Skype, ad esempio, sostiene di non riuscire a fornire la chiave di decifratura a causa della complessità dell'algoritmo di criptazione la cui chiave, oltretutto, viene cambiata ad ogni sessione di comunicazione; per un approfondimento si veda A. Ghilardini, *Intercettazioni Telematiche: Case Study su Skype*, intervento al Convegno IISFA Forum 2008, tenutosi a Bologna il 18 Aprile 2008 reperibile al seguente URL: http://www.iisfa.it/forum2008/IISFA_Forum_2008_Andrea_Ghirardini.pdf. Tutto ciò contrasta con il principio espresso dalla *Organisation for Economic Co-operation and Development* (OECD), nelle *Guidelines* sulla crittografia: "National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible". Il testo è disponibile al seguente URL: http://www.oecd.org/document/11/0,3343,en_2649_34255_1814731_1_1_1_1,00.html.

[225] Un *trojan horse* (dall'inglese: Cavallo di Troia), è un tipo di *malware*. Deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice *trojan* nascosto.

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

[227] Per ottenere questo risultato sarebbe sufficiente installare da remoto uno dei tanti *software* disponibili in rete (tra i molti si veda http://voipcallrecording.com/).

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

[229] M. Gercke, *Secret Online Search*, in *Computer und Recht*, 2007, p. 246.

L'utilizzo di questi programmi, ovviamente, dovrebbe avvenire sotto il costante controllo dall'Autorità Giudiziaria, che avrebbe il preciso compito di delimitare il tipo di attività del sistema controllante, filtrando le informazioni utili alle indagini e quelle che invece non hanno alcuna attinenza.

Se questa metodologia è in grado di consentire di superare il problema delle intercettazioni *VoIP*, è evidente che genera non poche perplessità dal punto di vista giuridico[230].

Anticipando nuovamente un tema che verrà meglio approfondito nel prossimo capitolo, è necessario trovare un punto di equilibrio tra le esigenze di prevenzione dei reati e di tutela dell'ordine pubblico con quelle di tutela dei dati personali e del rispetto del principio di sovranità[231].

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

[231] Sul principio di sovranità, basti pensare alle problematiche che potrebbero sorgere nel momento stesso in cui il proprietario del computer è installato un software di *remote forensics*, decida di partire in un altro stato portando con sè il computer "infetto". In questo caso, si potrebbe ipotizzare che la polizia giudiziaria stia svolgendo un'attività investigativa al di fuori del territorio nazionale. M. Gercke, *op. cit.*, p. 192.

3. Conservazione della *digital evidence*

Un aspetto estremamente importante in tema di *digital forensics* è la conservazione del dato digitale dopo la sua acquisizione. Come abbiamo visto, la dottrina italiana[232], statunitense[233] e le *best practices* internazionali[234] hanno prestato la massima attenzione alla fase di acquisizione e copia del dato digitale suggerendo le più idonee modalità operative al fine di non alterare la prova (*bit-stream image*, algoritmo di *hash*, *write blocker, live forensics*, corretta e puntuale elencazione e descrizione di tutti il materiale sequestrato).

Tuttavia, vi è una sorta di limbo in cui la prova digitale spesso viene a trovarsi tra la fase delle indagini e l'inizio del processo. Dove sono custoditi gli *hard disk* e le relative copie *bit-stream* e tutte le altre possibili prove digitali dopo che sono state sequestrate ed eventualmente analizzate?

A livello italiano, il codice di procedura penale (artt. 259, 260 e 261 c.p.p.) prevede che le cose sottoposte a sequestro siano affidate in custodia alla cancelleria o alla segreteria del Pubblico Ministero. Quando ciò non sia possibile o opportuno, l'Autorità Giudiziaria dispone che la custodia avvenga in luogo diverso, determinandone le modalità e nominando un altro custode.

All'atto della consegna, il custode è avvertito sia dell'obbligo di conservare e di presentare gli oggetti ad ogni richiesta dell'Autorità Giudiziaria, sia delle pene previste dalla legge penale per chi trasgredisce i doveri della custodia. Al custode può anche essere imposta una cauzione.

Le cose sequestrate si assicurano con il sigillo dell'ufficio giudiziario e con le sottoscrizioni dell'Autorità Giudiziaria, dell'ausiliario che la assiste e dell'indagato ovvero, in relazione alla natura delle cose, con altro mezzo idoneo a indicare il vincolo imposto a fini di giustizia.

---

[232] Tra tutti G. Ziccardi, *La procedura di analisi della fonte di prova digitale*, *op. cit.*, p. 73.
[233] Tra tutti E. Casey, *op. cit.,* p. 108.
[234] Tra tutte le linee guida inglesi della Association of Chief Police Officers disponibili al seguente URL: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf.

Nel caso di oggetti sequestrati di difficile custodia è necessario fare copia dei documenti ed eseguire fotografie o altre riproduzioni; ove, invece, tali oggetti siano soggetti ad alterazione può esserne ordinata la distruzione o la vendita.

L'esperienza di chi scrive non è delle più rassicuranti. Per stessa ammissione di alcuni ufficiali di Polizia Giudiziaria si stanno formando all'interno degli uffici giudiziari dei veri e propri "cimiteri informatici": depositi di *hard disk, monitor*, tappetini del *mouse* (sic) e altre amenità tecnologiche sequestrate nel corso degli anni.

Alcune di queste *digital evidences* sono accatastate in attesa di essere distrutte o, come è stato opportunamente tentato di proporre, di essere riutilizzate da parte della Polizia e dell'Autorità Giudiziaria[235]; altre, invece, potrebbero diventare la prova decisiva per l'assoluzione o la condanna in un procedimento penale.

In questo secondo caso, le metodologie di conservazione del supporto informatico diventano necessariamente importanti. Immaginiamo il seguente caso: un soggetto indagato per il reato di pedofilia subisce una perquisizione presso la propria abitazione con contestuale sequestro del suo personal computer.

La Polizia Giudiziaria avvalendosi di un esperto esegue degli accertamenti tecnici ripetibili sulla copia *bit-stream* dell'*hard disk* e predispone una relazione tecnica che sarà successivamente acquisita nel fascicolo del Pubblico Ministero.

Dopo sei mesi, all'indagato è notificato l'avviso di conclusione delle indagini preliminari e dopo altri sei mesi viene fissata l'udienza preliminare. Durante la fase dibattimentale, l'avvocato della difesa chiede che sia effettuata una nuova perizia sull'*hard disk* dell'imputato, in quanto potrebbero emergere degli elementi idonei a dimostrare la sua totale estraneità ai fatti.

---

[235] F. Cajani, *La destinazione dei beni informatici e telematici sequestrati o confiscati. Spunti per una modifica normativa in tema di contrasto al cybercrime*. Testo presentato all'I.I.S.F.A. Forum a Milano nel maggio del 2010 e disponibile al seguente URL: http://www.iisfa.it/atti_siracusa_F.Cajani.pdf.

A questo punto potrebbero essere passati da un minimo di un anno e mezzo ad un massimo di tre anni circa dal momento in cui l'*hard disk* è stato sigillato dopo il suo sequestro.

Alcune ricerche scientifiche[236] dimostrano che la durata media di un *hard disk* in condizioni non ottimali di temperatura è di tre anni (per non parlare della polvere che rischia di accumularsi ove il supporto sia sigillato semplicemente all'interno di una busta di carta).

È chiaro quindi che se il *bit* è eterno, il suo supporto non lo è affatto. I supporti digitali durano meno di quelli analogici e i dispositivi per leggere i supporti durano ancora meno[237].

Senza nessuna pretesa di voler entrare nel merito di quale siano le metodologie più adatte per conservare il dato digitale, ritengo, tuttavia, che una maggiore riflessione sul tema sia doverosa e imprescindibile, qualora si voglia garantire una corretta catena di custodia della *digital evidence*.

---

[236] E. Pinheiro, W.D. Weber, L. A. Barroso, *Failure Trends Large Disk Drive Population*, Ricerca presentata alla quinta edizione della conferenza USENIX sulle tecnologie di memorizzazione dei *file*, tenutasi a Madison presso l'University of Wisconsin, disponibile al seguente URL: http://static.googleusercontent.com/external_content/untrusted_dlcp/research.google.com/it//archive/disk_failures.pdf; ulteriori informazioni sul tema sono disponibili all'intero del sito USENIX: http://www.usenix.org/events/byname/fast.html.

[237] Il *Domesday Book* è un antico volume del 1086 che contiene un censimento (ossia un *database*) fatto realizzare da Guglielmo il Conquistatore nel 1086 con lo scopo di descrivere le terre, i beni e le persone del suo regno. Il libro è leggibile anche oggi. Nel 1983 è stato deciso di digitalizzare il *Domesday Book* utilizzando come supporto di memorizzazione il video disco. Il supporto è diventato osboleto dopo 15 anni e quindi non è più possibile accedere al *Domesday Book* attraverso quel supporto. P. Attivissimo, *Di chi sono i miei dati? Come i nostri dati rischiano di perdersi: casi vissuti e semplici tecniche di difesa*, disponibile al seguente URL: http://www.slideshare.net/disinformatico/di-chi-sono-i-miei-dati.

4. Analisi della digital evidence: accertamenti tecnici, incidente probatorio e perizia

L'Autorità Giudiziaria, dopo aver acquisito la prova informatica attraverso la copia *bit-stream* o attraverso il sequestro dell'*hard disk*, dovrà procedere all'analisi dei dati in essa contenuti.

Il codice di procedura penale offre tre differenti strumenti: in sede di indagine preliminare sarà possibile alternativamente procedere ad accertamenti tecnici[238] (artt. 359 e 360 c.p.p.) o ad incidente probatorio[239] (artt. 392 e ss. c.p.p.); in sede dibattimentale, invece, sarà possibile utilizzare lo strumento della perizia[240] (artt. 220 e ss. c.p.p.).

L'accertamento tecnico, in mancanza di una precisa definizione codicistica, si potrebbe definire come lo studio e la relativa elaborazione critica dei dati, necessariamente soggettivi e per lo più su base tecnico scientifica.

Durante le indagini preliminari, infatti, può assumere rilievo la necessità di ricorrere a specifiche competenze, soprattutto in campo informatico, che esorbitano dalla scienza privata dell'inquirente e per le quali il Pubblico Ministero potrà nominare, ai sensi dell'articolo 359 c.p.p., un consulente tecnico, che non potrà rifiutare di prestare la sua opera. In questo caso, le attività compiute dal consulente tecnico non sono direttamente utilizzabili a fini di prova, a meno che lo stesso non venga escusso come testimone durante il dibattimento e, quindi, in contraddittorio tra le parti.

A tale regola vengono apportati alcuni temperamenti, poiché determinate categorie di accertamenti possono essere valutati come prova anche in giudizio, tanto che vengono *ab initio* inseriti nel fascicolo del dibattimento, come previsto

[238] F. Giunchedi, *Gli accertamenti tecnici irripetibili*, 2009, Torino, Utet, p. 63.
[239] L. Cuomo, F. Scioli, *L'incidente probatorio*, 2007, Torino, Giappichelli, p. 25.
[240] S. Aterno, P. Mazzotta, *La perizia e la consulenza tecnica*, 2008, Padova, Cedam, p. 20.

dall'articolo 431 c.p.p., ove questi presentino un certo grado di urgenza e, dunque, di indifferibilità[241].

Trattandosi di atti destinati sicuramente ad esplicare efficacia di prova, il legislatore ha predisposto alcune garanzie, previste dall'articolo 360 c.p.p., rappresentate dalla partecipazione dei difensori, delle parti ed, eventualmente, dei loro consulenti tecnici.

È, infine, opportuno segnalare che la legge n. 397, del 7 dicembre 2000, in materia di indagini difensive, ha garantito un maggior rispetto del principio di parità tra accusa e difesa, introducendo l'articolo 327 *bis* c.p.p. e quelli compresi tra il 391 *bis* e 391 *decies* c.p.p..

L'articolo 391 *decies*, terzo comma c.p.p., infatti, specifica la possibilità per il difensore di ricorrere agli accertamenti tecnici non ripetibili, qualora, nelle more del giudizio, vi sia pericolo che la prova venga modificata. In tale eventualità la norma prevede che "il difensore deve darne avviso, senza ritardo, al Pubblico Ministero per l'esercizio delle facoltà previste, in quanto compatibili, dall'articolo 360 c.p.p." [242].

In tema di accertamenti tecnici nell'ambito di un'indagine digitale, la dottrina si è chiesta se l'analisi forense di un supporto informatico costituisca atto ripetibile o irripetibile[243].

È evidente che nel momento stesso in cui venga rispettata la procedura di acquisizione *bit-stream* dell'immagine del disco e sia verificata attraverso il calcolo dell'algoritmo di *hash* la perfetta identità della copia, non vi sono ragioni per ritenere irripetibile tale accertamento tecnico.

---

[241] Un esempio di scuola è quello dei rilievi segnaletici o fotografici disposti in occasione di un sinistro stradale. È evidente, infatti, che per effetto delle condizioni atmosferiche e del transito degli altri veicoli, le tracce di frenata o i detriti dell'impatto finirebbero, nel caso del sinistro stradale, per disperdersi e non potrebbero, fino al dibattimento, essere in altro modo conservati.

[242] O. Busi, *I Rilievi e gli Accertamenti tecnici nell'attività della polizia Giudiziaria e nell'esercizio delle investigazioni difensive*, in Atti del Convegno di Polizia Locale del 14 settembre 2005, in *Lex Ambiente*, http://www.lexambiente.it/acrobat/Busi.pdf

[243] L. Lupária, *La disciplina processuale e le garanzie difensive, op.cit.*, p. 153.

Sul punto è intervenuta recentemente anche la S.C. relativamente ad un caso in cui gli ufficiali di Polizia Giudiziaria avevano prelevato, ai sensi dell'art. 258 c.p.p.[244], dei *file* dall'*hard disk* dell'indagato e senza il rispetto di alcuna procedura di *digital forensics*. La Corte ha affermato il principio secondo cui "è da escludere che l'attività di estrazione di copia di *file* da un computer costituisca un atto irripetibile [...], atteso che non comporta alcuna attività di carattere valutativo su base tecnico-scientifica né determina alcuna alterazione dello stato delle cose, tale da recare pregiudizio alla genuinità del contributo conoscitivo nella prospettiva dibattimentale, essendo sempre comunque assicurata la riproducibilità di informazioni identiche a quelle contenute nell'originale"[245].

Il principio affermato in questa sentenza, in linea con l'orientamento prevalente[246] conferma la ripetibilità dell'accertamento tecnico su un supporto informatico. Lascia perplessi, invece, il totale disinteresse verso il mancato rispetto delle procedure di *digital forensics* idonee a garantire la non alterazione del dato così come prescritto dalle modifiche introdotte dalla legge di ratifica della Convenzione Cybercrime.

A distanza di pochi mesi, tuttavia, gli Ermellini hanno sostenuto che "l'esame dell'*hard disk* di un computer in sequestro e la conseguente estrazione di copia dei dati ivi contenuti non sono attività che le parti possono compiere durante il termine per comparire all'udienza dibattimentale senza contraddittorio e alla sola presenza del custode, in quanto implicano accertamenti ed interventi di persone qualificate e l'utilizzo di appositi strumenti, sì che devono essere

[244] Art. 258 c.p.p. "Copie dei documenti sequestrati. 1. L'autorità giudiziaria può fare estrarre copia degli atti e dei documenti sequestrati, restituendo gli originali, e, quando il sequestro di questi è mantenuto, può autorizzare la cancelleria o la segreteria a rilasciare gratuitamente copia autentica a coloro che li detenevano legittimamente […]".

[245] Cass. pen. Sez. I, 5 marzo 2009, n. 14511; conforme Cass. pen. Sez. I, 26 febbraio 2009, n. 11863. Per un commento si veda, F. Bravo, *Indagini informatiche e acquisizione della prova nel processo penale*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, Vol. III - N. 3, Vol. IV – N. 1, Settembre 2009–Aprile 2010, disponibile al seguente URL http://www.vittimologia.it/rivista/articolo_bravo_2009-03_2010-01.pdf.

[246] Cass. pen., Sez. I, 26 febbraio 2009, n. 11863; Cass. Sez. I, 25 febbraio 2009, n. 11503. Sono conformi a questo indirizzo anche: Cass. pen. Sez. III, 02 luglio 2009, n. 38087 (rv. 244928).

necessariamente svolti in dibattimento, nel contraddittorio, e sotto la direzione del giudice"[247]. Anche se una rapida lettura della massima potrebbe far ipotizzare un *revirement* giurisprudenziale, deve essere osservato che, in questa seconda pronuncia, l'attività compiuta dalla Polizia Giudiziaria non è stata solo quella di una mera acquisizione del dato digitale, ma è stata compiuta anche un'analisi dello stesso. Da ciò ne consegue che la mera copia *bit stream* dell'*hard disk* costituisce attività ripetibile, salvo che non sia preceduta da un'analisi preliminare del dato digitale. In attesa di una pronuncia che possa definitivamente sciogliere i legittimi dubbi avanzati dalla dottrina[248], ritengo sia difficile predeterminare la possibile ripetibilità o irripetibilità delle attività di acquisizione del dato digitale, perché essa può variare in base allo "stato di fatto" in cui trova ad operare la Polizia Giudiziaria.

L'incidente probatorio, disciplinato dagli articoli 392 e ss. c.p.p., garantisce, a differenza dell'accertamento tecnico, l'esercizio di un vero e proprio contraddittorio tra le parti. Nato per operare esclusivamente durante le indagini preliminari, a seguito di un significativo intervento della Corte Costituzionale [249], è stato reso esperibile anche nel corso dell'udienza preliminare e, quindi, successivamente all'esercizio dell'azione penale.

Con tale istituto, il codice offre la possibilità alle parti di chiedere un'assunzione anticipata della prova, in modo tale da poterla poi utilizzare nel futuro dibattimento; per fare ciò è necessario aprire, nel corso delle indagini, una "incidentale" parentesi accusatoria, celebrando un'apposita udienza, con le formalità del dibattimento, finalizzata non alla definizione del porcedimento, ma

[247] Cass. pen. Sez. III, 09 giugno 2009, n. 28524 (rv. 244594)

[248] L. Luparia, *"Sull'ipotesi di una irripetibilità intrinseca delle attività di Computer Forensics"*, *op. cit*., 152.

[249] Corte Costituzionale, 10 marzo 1994, n. 77. Tale pronuncia ha messo fine ad una disparità di trattamento tra Pubblico Ministero ed imputato: essendo le indagini preliminari segrete, solo il primo aveva modo di avanzare richiesta di incidente. L'indagato poteva valutare per la prima volta l'utilità dell'incidente probatorio dopo la *discovery* sugli atti e cioè dopo la richiesta di rinvio a giudizio e la conseguente fissazione dell'udienza preliminare. Per questo motivo la Corte Costituzionale ha consentito di richiedere l'incidente probatorio anche nel corso dell'udienza preliminare.

all'assunzione della specifica prova richiesta, affinché possa essere pienamente utilizzabile nel dibattimento; si pensi, ad esempio, ad un teste importante che, colpito da una grave malattia, corra il rischio di morire in pochi giorni e, quindi, di non poter testimoniare durante il processo.

Le ipotesi tassative che consentono di ricorrere all'incidente probatorio previste dall'articolo 392 c.p.p. possono essere suddivise in tre distinte macroaree: la prima riguarda i casi in cui l'assunzione della prova è indifferibile perché soggetta a modificazione e, quindi, non è possibile attendere il dibattimento, la seconda è quella in cui l'assunzione della prova viene chiesta dalle parti secondo valutazioni di strategia processuale, come quella di esaminare l'indagato su fatti concernenti la responsabilità di altri e, infine, la terza ha come obiettivo quello di non allungare i tempi del dibattimento, garantendo la sua concentrazione durante la fase delle indagini e può verificarsi qualora l'espletamento di una perizia possa avere una durata superiore ai sessanta giorni.

In estrema sintesi, l'incidente probatorio è un istituto del tutto eccezionale il cui esperimento risulta condizionato non solo dalla presenza di rigidi presupposti soggetti al vaglio del Giudice, ma anche alla possibile richiesta di differimento da parte del Pubblico Ministero.

A dimostrazione di tale assunto, il Tribunale di Arezzo ha rigettato la richiesta di incidente probatorio avente ad oggetto la perizia di un disco fisso ritenuto soggetto a "modificazione non evitabile". La richiesta era stata formulata dai difensori del proprio assistito indagato in un procedimento per duplicazione abusiva di *software*[250].

Nella motivazione si legge che "il pericolo di modificazione non evitabile della cosa deve dipendere dalla natura della cosa in sé e non dalle modalità di custodia della stessa, evitabili con ordinari ed elementari accorgimenti tecnici, autorizzando, ad esempio, l'effettuazione di piccoli fori di areazione sul cartone

[250] Ufficio del Giudice delle Indagini Preliminari di Arezzo, 26 maggio 2003, disponibile al seguente URL: http://www.ictlex.net/?p=55

in cui è custodito il computer sequestrato". Sia consentito rilevare, con rispettoso sarcasmo, che un supporto informatico non è un essere vivente (almeno fino ad ora) e che la modificazione non evitabile di un supporto non custodito adeguatamente è un rischio da prendere in seria considerazione.

Il terzo e ultimo strumento di analisi del dato informatico è la perizia, che viene disposta dal Giudice autonomamente o su richiesta delle parti "quando occorre svolgere indagini o acquisire dati e valutazioni che richiedono specifiche competenze tecniche, scientifiche o artistiche".

Il nuovo e diverso impianto del codice di procedura penale ha notevolmente modificato la disciplina della perizia: in precedenza il Giudice vagliava la necessità del ricorso allo strumento penale e stabiliva il quesito da porre al merito. Ora, invece, l'ammissibilità della perizia è preclusa solo nei casi in cui "non occorra" l'indagine, mentre il quesito viene posto "sentiti i periti, i consulenti tecnici, il Pubblico Ministero ed i difensori presenti".

Le operazioni peritali si sviluppano in tre fasi: conferimento dell'incarico, attività del perito ed enunciazione del parere. Durante la prima fase il perito, la cui scelta non è vincolata alla iscrizione in appositi albi, ma si effettua sulla base della concreta idoneità a svolgere l'incarico, riceve il quesito concordato dalle parti; contestualmente il Giudice lo autorizza "a prendere visione degli atti, dei documenti e delle cose prodotte dalle parti dei quali la legge prevede l'acquisizione al fascicolo del dibattimento".

Nella seconda, il perito compie la sua attività entro il periodo di tempo fissato dal Giudice che, comunque, non deve superare i novanta giorni prorogabili fino al limite massimo di sei mesi; nella terza ed ultima fase, oltre all'enunciazione del parere e all'eventuale presentazione di una relazione scritta, il perito viene esaminato dalle parti con le stesse regole previste per i testimoni.

L'articolo 511 c.p.p. spiega in modo sufficientemente chiaro il rapporto tra perito e perizia sancendo il principio che la lettura della relazione peritale è disposta

solo dopo l'esame del perito: da ciò si deduce che la relazione peritale può diventare prova solo dopo l'esame del perito e che le parti possono utilizzare tale relazione per formulare domande e muovere contestazioni[251].
Sia nel caso della perizia che dell'incidente probatorio, le parti possono controllare l'operato del perito avvalendosi di consulenti tecnici in numero non superiore a quello dei periti con la facoltà di assistere a tutte le operazioni, al fine di salvaguardare gli interessi di tutti i soggetti coinvolti nel processo.

4.1 Le modalità operative nel caso di analisi del dato informatico

L'utilizzo del reperto informatico a fini probatori di qualunque reato richiede la consapevolezza, negli operatori, del suo carattere puramente indiziario e sempre ripudiabile e genera la necessità di avere un approccio metodologico nelle operazioni da eseguire e negli strumenti da analizzare.
Il problema consiste, infatti, nella pratica impossibilità di dimostrare, al di là di ogni ragionevole dubbio, che il dato stesso non sia stato manipolato ad arte: chiunque debba utilizzarlo come elemento probatorio deve ricostruire con ragionevole certezza tutte le fasi che hanno contraddistinto il contesto relazionale in cui il dato in questione si è formato.
La metodologia che contraddistingue l'accesso al reperto informatico e la sua successiva utilizzazione richiede una serie precisa e ben definita di fasi operative.
Dal punto di vista del metodo, come si è evidenziato in precedenza, un'indagine di informatica forense non avviene mai sul sistema informatico originale, ma viene effettuata una copia dei supporti sui quali lavorare in un secondo tempo.
Questa è una delle fasi più delicate per le successive finalità processuali, in quanto incorpora i maggiori rischi di futuro ripudio del dato stesso. L'acquisizione, qualora non sia già stata effettuata durante l'esperimento di uno

[251] D. Siracusano, A. Galati, G. Tranchina, E. Zappalà, *op. cit.*, p. 407

dei mezzi di ricerca della prova, deve essere condotta in modo da assicurare la massima coerenza fra originale e copia attraverso l'utilizzo dell'algoritmo di *hash*, possibilmente documentando, anche con riprese video le diverse azioni compiute e la correttezza della procedura seguita dall'inquirente e/o dai suoi consulenti.

È, inoltre, opportuno ribadire che le analisi forensi di dati digitali hanno sempre di meno come oggetto, il personal computer e sempre di più altre tipologie di supporti (*smartphone*, lettori mp3, *console* di videogiochi, navigatori satellitari).

Dopo l'apertura dei sigilli apposti sui supporti informatici sequestrati, è utile un controllo per verificare la presenza di cd rom o *flash drive* ancora inseriti all'interno dell'*hardware*, oltre che una corretta descrizione delle macchine da analizzare. Può capitare infatti che, durante la fase di sequestro, non siano stati inseriti all'interno del verbale supporti o caratteristiche tecniche del supporto potenzialmente utili alle indagini in corso.

La successiva operazione da compiere sarà quella di rimuovere in modo certo tutti i dati presenti sul supporto di destinazione attraverso l'operazione di *wiping*; all'interno dei supporti di memorizzazione presenti in commercio sono presenti degli elementi di tipo magnetico, che potrebbero impedire un'acquisizione perfettamente identica del supporto originale.

Utilizzando, poi, un *write blocker*, si procede all'acquisizione vera e propria che consiste nella copiatura su un altro supporto di quello del supporto da analizzare.

I *software* per effettuare tale operazione, senza perdere eventuale dati presenti all'interno del supporto di memorizzazione non acquisibili con una semplice copia di *back up*, possono essere sia *open source* che di natura proprietaria (*closed source*).[252]

I software *open source* sono caratterizzati dalla possibilità di visionare il codice sorgente, ossia l'insieme di istruzioni appartenenti ad un determinato linguaggio

[252] Tra i software proprietari il più conosciuto è il già citato *Encase* della *Guidance Software Inc*, mentre tra quelli *Open Source* è possibile utilizzare, tra i molti, la funzione "DD" del sistema operativo Linux.

di programmazione utilizzato per realizzare un programma per computer. Per questo motivo, garantiscono una maggiore trasparenza, in quanto è possibile verificare tutte le operazioni compiute dal *software* durante la fase di acquisizione.

Alcuni autori[253] hanno, inoltre, osservato che i *software open source* sono in grado di garantire un maggior rispetto dei criteri previsti dalla citata "sentenza Daubert" in tema di validazione della prova scientifica[254]. La possibilità di poter visionare, modificare e controllare il codice sorgente, infatti:

- garantisce un enorme vantaggio epistemologico rispetto ai *closed source* che possono essere solo testati;
- rende agevole e verificabile la *peer review*;
- rende agevole la misurazione del tasso di errore;
- favorisce una costante discussione dalla Comunità Scientifica e, quindi, per definizione, un costante miglioramento.

Da convinto sostenitore del "movimento" *open source* in tutti i settori del diritto, non posso che concordare con quanto scritto, tuttavia, occorre rilevare che, stante l'attuale giurisprudenza in tema di *digital forensics*, questo tema appare, a mio modesto parere, un po' troppo raffinato per "il palato" di Magistrati che ancora considerano la stampa di una pagina *web* una fonte di prova[255].

---

[253] E. Huebner, S. Zanero, *op. cit.*, p. 3.

[254] *Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579*, syllabus disponibile al seguente URL: http://www.law.cornell.edu/supct/html/92-102.ZS.html); Per un approfondimento si veda: M. Taruffo, *Le prove scientifiche nella recente esperienza statunitense*, in *Riv. trim. dir. proc. civ.*, 1996, p. 219; L. Dixon, B. Gill, *Changes in the Standards for Admitting Expert Evidence in Federal Civil Cases since the Daubert Decision*, 2001, RAND Institute for Civil Justice; D.J. Faigman, D.H. Kaye, M.J. Saks, J. Sanders, *Modern Scientific Evidence. The Law and Science of Export Testimony*, St. Paul, 2002; K.R. Foster, P.W. Huber, *Judging Science. Scientific Knowledge and the Federal Courts*, Cambridge, 1999, M.I.T. Press.

[255] Sul tema è interessante osservare che alcuni autori hanno ritenuto che sia, oggi, necessario trovare un meccanismo per certificare la *digital evidence*. In altri campi, come la contabilità, ciò è avvenuto, con l'utilizzo di riconosciute strutture di certificazione dei bilanci. La stessa cosa sarebbe ipotizzabile anche in ambito *digital forensics*. Allo stesso modo, la seconda area di preoccupazione è data dalla qualificazione dell'esperto, in quanto la caratteristica del settore è l'assenza di procedure univoche di qualificazione rendono molto incerta e "fumosa" la carriera del consulente tecnico.

Un aspetto molto importante, a parte il *software* utilizzato, è dato dalla qualità della *workstation* su cui si effettua l'acquisizione. Vista la complessità delle operazioni da eseguire, è necessario che questa abbia delle adeguate caratteristiche tecniche sia sotto il profilo della potenza di calcolo (processore) che della memoria (RAM).

Dopo aver provveduto ad effettuare l'acquisizione della copia *bit-stream* del supporto di memorizzazione, è possibile passare alla fase dell'analisi e della valutazione del dato digitale.

Anche in questa fase, sono disponibili sia software *open source* che *closed source*[256] per supportare questo tipo di analisi. Questi strumenti consentono, in particolare, l'analisi dei *file* cancellati, l'identificazione dei *file* noti e presenti all'origine nel sistema indagato, nonché l'individuazione della *timeline*, ossia del momento in cui è stato eseguita l'ultima modifica del *file*.

Le operazioni da compiere possono essere di varia natura e dipendono strettamente dalla tipologia del reato oggetto di indagine. È, comunque, opportuno effettuare sempre una descrizione accurata della parte logica del supporto e del tipo di sistema operativo, verificando il numero e le dimensioni logiche delle "partizioni" e dei "volumi" del disco fisso.

Successivamente dovranno essere analizzati tutti i dati potenzialmente rilevanti: dai *file* audio e video ai *file* compressi, dalla posta elettronica salvata all'interno del computer ai *link* locali e remoti contenuti nella cartella preferiti, dalla cronologia della navigazione Internet con i relativi *cookies*[257], fino ad arrivare ai *file* steganografati, criptati e protetti da *password*.

---

[256] I più noti sono sicuramente *Encase* della *Guidance Software Inc.* (http://www.guidancesoftware.com/), *FTK Imager* della *software-house* Access Data Group Inc. (http://www.accessdata.com/downloads.html), *ILook* Investigator della *software-house* Perlustro L.P. (http://www.ilook-forensics.org), *HELIX* della *software-house E-fense* (http://www.e-fense.com/), *Maresware The Suite* della *software-house Mares and company* (http://www.dmares.com), *Live View* della Carnegie Mellon University (http://liveview.sourceforge.net/). Grande importanza rivestono, inoltre, i progetti *open source* DEFT (http://www.deftlinux.net/) e CAINE (http://www.caine-live.net/).

[257] I *cookies* (letteralmente "biscottini") sono piccoli file di testo che i siti web utilizzano per immagazzinare alcune informazioni nel computer dell'utente. I *cookies* sono inviati dal sito web e

Particolare attenzione meritano anche i software di *file-sharing* che possono fornire informazioni statistiche sul numero dei *file* scaricati o immessi in rete o i programmi di *chat* e di *instant messaging* che, spesso, conservano un *file* di *log* contenente le registrazioni delle conversazioni telematiche effettuate[258].

Tutti i *file* o i *software* analizzati dovranno essere oggetto di una precisa valutazione che consiste in un giudizio sintetico sulla loro attendibilità (rispetto ai rischi di manipolazione) e sulla loro autenticità (possibilità di accertarne l'autore).

Anche se non è possibile prevedere in modo esaustivo quale tipo di analisi dovrà essere effettuata sul dato digitale, le principali attività sono le seguenti:

1. *Text searching*: consiste nel condurre ricerche di tipo testuale all'interno dei *file* o delle *directory* e si estende a tutte le strutture del *file system*. L'analisi del contenuto di *file* con applicazione ignota viene effettuata con l'impiego di visualizzatori forensi in grado di interpretare numerosi formati.
2. *Image searching*: consiste nella ricerca delle immagini digitali su *file* di vario formato, inclusi i fotogrammi di *file* video e riveste grande importanza nei casi di pedopornografia e di violazione del diritto d'autore.
3. *Data recovery and identification*: questa fase dell'analisi è di grande utilità per la quantità di informazioni che può fornire all'operatore ed è costituita dalla *data recovery* (procedimento per recuperare dati presenti, cancellati o danneggiati da memorie di massa), *data discovery* (procedimento per scoprire dati nascosti da una memoria o da un *file* cifrati o protetti in altro modo), *data carving* (tentativo di ricostruire un *file* danneggiato attraverso il recupero di porzioni di *file*).
4. *Metadata recovery e Identification*: i metadati sono dei dati che rivestono particolare importanza e comprendono informazioni di sistema o applicazioni a

---

memorizzati sul computer. Sono quindi re-inviati al sito web al momento delle visite successive. Le informazioni all'interno dei *cookies* sono spesso codificate e non comprensibili. I file steganografati, invece, sono quei file nascosti all'interno di file di "copertura" (filigrana elettronica), che due utenti possono utilizzare per inviare messaggi.

[258] Per un ulteriore approfondimento si veda L. Chirizzi, *op. cit.*, p. 66.

corredo della struttura di *file system*, *file*, cartelle, partizioni. Il recupero e l'identificazione di tali dati (es. date e orari, attributi di *file*) e sono di particolare importanza per determinare la *timeline* di accesso e di modifiche di un *file*[259].

[259] Per un approfondimento si veda, tra i molti, R. Cannavò, Computer Forensics*: aspetti tecnici e legali*, in *Teutas,* 20 dicembre 2009, disponibile al seguente URL: http://www.teutas.it/societa-informazione/prova-elettronica/740-computer-forensics-aspetti-tecnici-e-legali.html

5. Presentazione della *digital evidence*

Fino ad ora è stato analizzato il livello ontologico dell'analisi del dato digitale. Un aspetto fondamentale dell'attività di *digital forensics*, tuttavia, è il livello epistemologico che si estrinseca nella relazione tecnica: questo documento deve descrivere tutte le operazioni compiute per il raggiungimento del risultato dell'analisi del dato digitale; in tale sede, sarà necessario operare uno sforzo di sintesi e di semplificazione, tale da abbattere ogni potenziale *digital divide* tra inquirenti e giudicanti. Questa fase, infatti, sebbene sia spesso la più noiosa per un informatico, è di fondamentale importanza per Pubblici Ministeri, Giudici e avvocati, in quanto l'esito del processo dipenderà non solo dai risultati raggiunti, ma anche dal grado di chiarezza e di comprensione di tale documento.

La relazione tecnica potrà essere redatta in fase di accertamento tecnico preventivo, incidente probatorio e perizia. Negli ultimi due casi viene instaurato un vero e proprio contraddittorio davanti al Giudice, nel primo, invece, il consulente lavorerà a stretto contatto con la Procura e la Polizia Giudiziaria, salvo che egli non sia incaricato da un avvocato a controllare il loro operato o ad effettuare delle autonome indagini difensive.

Indipendentemente dalla fase in cui viene richiesta, la relazione tecnica deve necessariamente contenere una completa ed esaustiva descrizione dei sistemi informatici analizzati, un elenco degli strumenti (*tools*) utilizzati e un dettagliato resoconto dei risultati raggiunti[260].

La dottrina statunitense sul tema consiglia di considerare la relazione tecnica, come un documento *in itinere*: prima ancora di scriverla, è necessario aver raccolto tutto il materiale attraverso appunti scritti, oltre che documentazione fotografica e video di tutte le operazioni compiute a partire dalla fase dell'individuazione del dato.

[260] A. Reyes, K. O'Shea, R. Brittson, J. Steel, *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors*, 2007, Elsevier Science, p. 255.

Se la relazione tecnica è lunga, è preferibile inserire un indice e iniziare il documento con un breve *abstract,* che sintetizzi i risultati raggiunti e le più importanti operazioni tecniche compiute.
Nel caso in cui i termini tecnici siano molti e non di immediata comprensione, potrebbe essere utile realizzare un glossario per i termini meno noti e immediatamente comprensibili.
Uno dei modi migliori per presentare i dati è quello di utilizzare una *timeline table* che, tra le altre cose, consentirà di mostrare la data e l'ora dell'accesso di quel determinato *file* da parte dell'utente. Alla stessa stregua, si consiglia un diagramma di flusso delle principali operazioni compiute.
Quasi tutti i *software* di analisi forense hanno, infatti, dei *tools* che consentono di registrare tutte le attività compiute dall'esperto e successivamente di inserire le prove digitali direttamente nel *report* con un semplice *clic* del *mouse*. Tuttavia, l'elenco delle operazioni compiute, creata autonomamente da *software* proprietari come *Encase* e *FTK* o *open source* o come *Helix*, *Deft* o *Caine* è scritta in inglese: ciò rende più difficile l'utilizzo di tali strumenti all'ufficiale Polizia Giudiziaria o al consulente tecnico.
Se la consulenza è incompleta o non accurata il rischio di una pronuncia sfavorevole per l'imputato è molto alto e anche lo stesso consulente potrebbe fare fatica a distanza di anni a ricostruire esattamente il tipo di attività svolta.
La sfida più delicata, comunque, è quella di presentare il caso in modo che non vi possano essere contestazioni di sorta. Da un lato, infatti, la presentazione deve essere di immediata e facile comprensione anche per chi non è esperto, ma dall'altro non deve prestare il fianco a contestazioni sulla validità del metodo eseguito. Gli standard della *digital forensics* cambiano con estrema rapidità e

l'utilizzo di un *software* non idoneo o sul quale sono stati riscontrati dei difetti, potrebbe costituire un elemento determinante per l'esito di un processo[261].

Non bisogna dimenticare, inoltre, che la relazione tecnica viene spesso redatta con largo anticipo rispetto alla fase in cui verrà effettivamente analizzata: è necessario, quindi, conformarsi alle *best practices* in materia.

Anche se la consulenza non nasce per essere prodotta in giudizio o ha portato ad un risultato negativo, è comunque opportuno redigerla in modo che possa essere garantito il suo successivo ed eventuale utilizzo all'interno del processo.

Infine, sarebbe opportuno redigere delle relazioni tecniche interattive, che contengano al loro interno alcune *slides* di presentazione del caso oltre ad immagini e video, che possono essere aperti con un collegamento ipertestuale dall'interessato.

Quest'ultima considerazione nasce da una riflessione di fondo: la cultura audiovisiva sta cambiando il mondo e la giustizia. È difficile dire se questo sia un bene, ma è sicuramente un dato di fatto. Stiamo assistendo, attraverso il computer, ad una moltiplicazione del concetto di immagine: abbiamo video e foto digitali, scene del crimine elaborate digitalmente, animazioni al computer, presentazioni multimediali, *slides* e molto di più[262].

La combinazione delle immagini con la voce duplica le capacità recettive dello spettatore e il progresso tecnologico è ancora in corso: si intravedono all'orizzonte realtà virtuali in tre dimensioni.

Questo cambiamento influenza la cultura legale: pensare con le immagini è molto diverso che pensare con le parole. Pertanto, sono richieste nuove professionalità.

---

[261] M. Scheetz, *Computer Forensics: an essential guide for accountants, lawyers, and managers*, 2007, John Wiley & Sons, p. 52; si veda anche H. Silverstone, M. Scheetz, *Forensic Accounting and Fraud Investigation for Non-Experts*, 2004, John Wiley & Sons.

[262] Per un approfondimento sul tema si veda, N. Feigenson, C. Spiesel, *Law on Display. The Digital Transformation of Legal Persuasion and Judgement*, 2009, New York University Press; S. M. Kassin and Meghan A. Dunn, *Computer-Animated Displays and the Jury: Facilitative and Prejudicial Effects*, in *Law and Human Behaviour*, 1997, Vol. 21, N. 3, p. 269.

Se gli operatori del diritto non compiranno uno sforzo per fare propri i nuovi *media*, saranno sempre più in difficoltà di fronte ad avvocati o Pubblici Ministeri capaci di far propri gli strumenti digitali.

In sintesi, non esiste prova digitale senza una relazione tecnica: ma la relazione tecnica non può e non potrà in futuro che essere espressa nel nuovo linguaggio della comunicazione, quello che integra le parole con le immagini, e che, anzi, tende a privilegiare le seconde. Basti pensare che negli Stati Uniti, molti avvocati si avvalgono con regolarità non solo del consulente tecnico, ma anche del consulente della "comunicazione processuale". Per chiarire meglio questa considerazione, è opportuno descrivere sinteticamente il caso *SEC v. Buntrock*.

Prima del "caso Enron", una delle più importanti indagini finanziarie fu condotta dalla Securities and Exchange Commission (SEC) contro James Koenig (Direttore finanziario di Waste Management)[263]. Dal 1992 al 1996 James Koenig aveva elaborato una serie di complessi schemi contabili per sottostimare le spese e incrementare quindi i profitti ufficiali.

James Koenig aveva violato i principi contabili del GAAP (General Acceptable Accountable Principle) nel trattamento degli ammortamenti, nella capitalizzazione degli interessi e in una serie di violazioni minori.

Nel marzo del 2002 la SEC citò in giudizio Koenig, cercando di dimostrare a giurati senza alcuna competenza in materia che attraverso alcuni sottili artifizi contabili questi aveva falsificato i bilanci e conseguentemente truffato gli azionisti.

SEC decise di usare un consulente di comunicazione processuale: Christopher Ritter e la sua società The Focal Point[264]. Il processo si svolse nel 2006, ossia 10 anni dopo gli eventi. Ritter preparò 180 *slides* per le dichiarazioni di apertura e più di 100 per l'argomentazione conclusiva.

---

[263] *SEC v. Koenig,* 2009 U.S. App. LEXIS, 3725.

[264] All'interno del sito web della società è possibile visionare le *slides* realizzate per questo e altri importanti casi: http://www.thefocalpoint.com/cases_spotlight.

Le *slides* di Ritter seguivano la logica del confronto e contrasto. Prima una normale azienda che seguiva i corretti principi contabili, poi le piccole deviazioni di Koenig e le conseguenze sempre più clamorose del falso.

Con semplici animazioni ogni esempio era drammatizzato. Al termine di ogni serie era mostrata un'immagine in cui si diceva che cosa Mr. Koenig avrebbe dovuto fare.

In sintesi, il meccanismo adottato da Ritter consentì di realizzare una formidabile operazione didattica, ottenuta proprio con l'uso integrato dei canali audio e video, riconducendo al suo essenziale connotato illecito quella che avrebbe potuto sembrare una disputa burocratica sull'interpretazione dei principi contabili.

Questo esempio consente di chiarire un aspetto di fondo: è chiaro che le tecniche retoriche di utilizzo dell'immagine hanno maggiore rilevanza in un contesto giudiziario come quello statunitense, del tutto determinato dal comportamento delle giuria, ma finiranno ben presto per influenzare il pensiero professionale anche degli operatori di diritto di altri Paesi.

CAPITOLO III – INDAGINI DIGITALI, PRIVACY E GARANZIE DELL'INDAGATO

1. Premessa

Se il primo decennio del XXI secolo è stato quello del commercio elettronico e delle conseguenti preoccupazioni legate alle possibili frodi (dalle truffe su e-bay alla clonazione delle carte di credito), il prossimo si preannuncia come quello del "cloud computing" e dei rischi legati alla diffusione dei propri dati personali in rete e specialmente all'interno dei *social network* (potenzialmente esposti al rischio di *data mining*[265]).

Non sorprende più il fatto che prima di iniziare ogni indagine la polizia giudiziaria sistematicamente ricerchi in rete "informazioni utili" al caso. Tra i molti esempi che si possono citare, è sicuramente singolare l'arresto avvenuto in Italia di un latitante membro della "n'drangheta", scoperto in quanto aveva creato un profilo Facebook con lo pseudonimo di "scarface" [266].

In questo contesto l'investigazione digitale ha, ora più che mai, un ruolo determinante, dato l'enorme valore di informazioni che la polizia giudiziaria può rinvenire all'interno di un personal computer, attraverso un'intercettazione telematica o anche solo grazie ad una semplice navigazione in Internet.

Occorre, inoltre, considerare che l'indagine digitale genera molto spesso un conflitto tra diverse giurisdizioni: come nessun criminale farebbe una rapina in banca a volto scoperto, così nessun cyber-criminale sarebbe tanto sprovveduto da soltanto immaginare di delinquere online senza prima delocalizzare in un Paese straniero il suo accesso alla rete o la conservazione dei propri dati (dalla casella di posta elettronica al contenuto dell'intero *hard disk*). Il conflitto giurisdizionale

[265] Per un approfondimento sul tema si veda C. Westphal, *Data Mining for Intelligence, Fraud & Criminal Detection: Advanced Analytics & Information Sharing Technologies*, 2008, CRC Press, p. 3.
[266] ABC News International, 17 marzo 2010, A. Wise, *Mafia Boss Betrayed By Facebook*, disponibile al seguente indirizzo: http://abcnews.go.com/International/facebook-finds-mafia-boss/story?id=10124958.

che segue non solo rileva sotto il profilo procedurale (rogatorie, convenzioni e accordi internazionali). Il presente capitolo propone un'analisi comparativa dei diversi approcci verso queste due tematiche rispettivamente in Europa e negli Stati Uniti.

2. Privacy vs Law Enforcement negli Stati Uniti

Prima di entrare nel merito delle questioni *de jure condendo* sul potenziale contrasto tra le nuove metodologie d'indagine e i diritti fondamentali dell'individuo, pare opportuna una premessa storica sul ruolo assunto dalla privacy nell'ordinamento giuridico statunitense[267] durante l'ultimo secolo.

Il diritto alla privacy è figlio della storia americana e racchiude, in sé, una delle motivazioni che animarono migliaia di persone di tutto il mondo a migrare verso un Paese che garantiva a tutti la libertà nelle fondamentali scelte umane: dalla religione, al matrimonio, alla politica, al lavoro e all'educazione[268]. Nonostante vivessero in piccole comunità compatte, i coloni furono portatori convinti dei valori della privacy, con specifico riguardo alla libertà individuale di pensiero e di comunicazione. Il Quarto Emendamento, già citato nel precedente capitolo, che attribuisce con dignità costituzionale il diritto alla privacy negli Stati Uniti, trae le proprie origini dalla legislazione varata nella colonia del Massachusetts prima dell'indipendenza, al fine di proteggere i coloni contro perquisizioni arbitrarie ad opera di ufficiali doganali della Corona britannica intenti a contrastare l'evasione fiscale tramite il sequestro di merce "vietata e non

[267] A parte il noto saggio di Warren e Brandeis (L. Warren, S. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, Vol. 4, December 15, 1890, No. 5), se ne possono annoverare molti altri che tra la fine del XIX secolo e la prima metà del secolo scorso hanno trattato il tema: tra questi spicca l'opera di Cooley, che, per primo, definì la privacy come "The right to be alone" (T. M. Cooley, *A Treatise on the Torts*, Chicago Callaghan & Co., 1888, p. 29), o anche D. O'Brien, *The Right to Privacy*, in *Columbia Law Review*, Vol. 2, 1902, p. 443; E. L. Adams, *The law of privacy*, North American, 1902; R. Pound, *Interests of Personality*, in *Harvard Law Review*, Vol. 28, 1915, No. 4, p. 343; L. Nizer, *The Right of Privacy: A Half Century's Developments*, in *Michigan Law Review*, Vol. 39, 1941, No. 4, p. 526.

[268] F.S. Lane, *American Privacy: The 400-Year History of Our Most Contested Right*, 2009, Boston, Beacon Press.

sdoganata". Durante l'acceso dibattito che precedette l'approvazione della legge di cui sopra, l'accanito sostenitore dell'indipendenza statunitense James Otis Jr, asserì famosamente che: "La casa di un uomo è il suo castello; e laddove venga lasciato in pace, quell'uomo ha la stessa protezione di un principe nel proprio castello"[269]. Pochi anni dopo, John Adams, che in seguito sarebbe succeduto a George Washington come secondo Presidente degli Stati Uniti, annotò nel suo diario: "Non sono vincolato da alcun obbligo morale o altro a rendere noto al mondo l'ammontare annuale dei miei oneri o introiti. Vi sono occasioni in cui e persone a cui non sono obbligato a rivelare i miei principi e opinioni in materia di politica o di religione", aggiungendo poi che tale genere di segretezza o di reticenza non era di natura ingannevole, ma meramente segno di "ritegno o, in altre parole, prudenza e discrezione"[270].

I principi sì vigorosamente sostenuti da James Otis Jr e dal Presidente Adams, furono spinti al centro dell'opinione pubblica all'inizio del secolo scorso a seguito di una causa che sollevava una questione, ancora oggi, di grande attualità, e cioè il delicato equilibrio da stabilirsi tra i principi dettati dal Quarto Emendamento introdotto dal *Bill of Rights* e l'esigenza di garantire la tutela dell'ordine pubblico. La causa che nacque dallo "scandalo delle intercettazioni telefoniche" avvenuto a New York nel 1915, che coinvolse trentanove degli istituti caritatevoli della città in una serie complessa di accuse e controaccuse[271].

Nel 1914, John P. Mitchel, il trentaquattrenne sindaco di New York, nominò John A. Kingsbury sovrintendente delle Opere Pie della Città. All'epoca, tutti gli istituti di beneficenza della città erano sottoposti alla supervisione dell'ufficio

---

[269] "A man's house is his castle; and whilst he is quiet, he is as well guarded as a prince in his castle". Si consiglia per un approfondimento la monumentale opera di Cuddihy (W. Cuddihy, *The Fourth Amendment*: *Origins and Original Meaning 602-1791*, Oxford University Press, January 2009).

[270] "I am under no oblig moral or other Obligation to publish to the World, how much my Expences [illegible] or my Incomes amount to yearly. There are Times when and Persons to whom, I am not obliged to tell what are my Principles and Opinions in Politicks or Religion", tratto dal Diario di John Adams del 20 agosto 1770. L'intero archivio degli scritti di John Adams è disponibile on line al seguente indirizzo: http://www.masshist.org/digitaladams/aea/.

[271] F.S. Lane, *op. cit.*, p. 82.

statale per le opere pie, che, tra le altre cose, si occupava del collocamento dei bambini abbandonati. Kingsbury era convinto che i suoi compiti di presidio delle opere pie della città, comprendessero il monitoraggio delle condizioni di vita garantite nei vari istituti di carità. In base alla dichiarazione di Kingsbury che accusava l'ufficio statale di trascurare taluni dei compiti affidatigli, il governatore Charles Whitman[272] nominò una commissione speciale sul tema, presieduta da Charles H. Strong[273].

Nella primavera del 1916 alcuni esponenti delle chiese cattoliche della Città lamentarono di aver subito intercettazioni telefoniche nel corso delle indagini condotte dalla Commissione Strong. Particolarmente accanite fuorono le accuse del Reverendo James J. Higgins, Sovraintendente delle Opere Pie Cattoliche di Brooklyn [274], secondo il quale alcuni dei temi trattati dalla Commissione Strong non sarebbero mai venuti alla luce se non grazie all'intercettazione di conversazioni telefoniche altamente confidenziali e attinenti a questioni matrimoniali o ad altre vicende strettamente personali di alcuni parrocchiani.

Su richiesta della Diocesi il procuratore di New York Edward Swann aprì un'indagine per accertare la commissione di eventuali reati[275]. Pochi giorni dopo queste accuse, il Sindaco Mitchel ammise di aver autorizzato l'intercettazione

[272] Charles Whitman (1868–1947) è ricordato nella storia per aver eseguito la prima condanna a morte di un poliziotto implicato nell'omicidio di un giocatore d'azzardo. Ironia della sorte, Whitman, durante le indagini, fu costretto a sentire i testimoni all'interno del suo Golf Club, per paura di essere intercettato. Per un approfondimento S. Cohen, *The Execution of Officer Becker: The Murder of a Gambler, the Trial of a Cop, and the Birth of Organized Crime*, 2007, Da Capo Press. p. 34.

[273] New York Times, articolo del 19 novembre 1915, dal titolo "Whitman Order Charities Inquiries" disponibile al seguente indirizzo: http://query.nytimes.com/mem/archive-free/pdf?_r=1&res=9F01E7D71239E333A2575AC1A9679D946496D6CF.

[274] New York Times, articolo del 30 aprile 1916, dal titolo "Plan Wiretapping Inquiries" disponibile al seguente indirizzo: http://query.nytimes.com/gst/abstract.html?res=9C05E6D6153AE633A25755C1A96F9C946796D6CF.

[275] *The Penal code of the state of New York, being Chapter 676 of the laws of 1881, as amended by the laws of 1882-1907*, Banks Law Pub. Co., 1907. Per una interessante panoramica sulle varie leggi statali e federali statunitensi sul tema della privacy si consiglia, inoltre, il seguente schema disponibile all'interno del sito della Community LawBrain disponibile al seguente indirizzo. http://lawbrain.com/wiki/U.S._Privacy_Law.

delle comunicazioni di tre sacerdoti cattolici investiti di responsabilità apicali in seno alla Diocesi.

Il 3 maggio del 1916, Samuel Greenbaum un Giudice della Corte Suprema dello Stato di New York, fu incaricato di condurre, in veste di magistrato inquirente, un'inchiesta contro ignoti volta ad accertare se le forze dell'ordine avessero effettivamente violato la privacy dei sacerdoti in questione. Dopo tre settimane di audizioni furono sollevate accuse formali solo contro Kingsbury e il suo consulente giuridico, mentre furono archiviati senza seguito i procedimenti contro tutti gli altri interessati ivi compresi il Sindaco Mitchel e il capo della polizia Arthur Woods[276].

Nel frattempo la notizia delle intercettazioni aveva attirato l'attenzione del Comitato Thompson, un gruppo di lavoro legislativo impegnato in un'indagine sui servizi pubblici nella Città di New York[277]. Il Comitato appurò che la polizia si avvaleva di intercettazioni da più di vent'anni, e che nei soli due anni precedenti furono intercettate quasi 350 utenze telefoniche.

In quel frangente il Capo della Polizia Woods, sentito dal Comitato su propria richiesta, rese una dichiarazione infuocata che ancora oggi, quasi un secolo dopo, è spesso riproposta tra le argomentazioni a sostegno delle intercettazioni illegali. Egli concluse il suo intervento, sostenendo che: "è necessario mettere le forze dell'ordine che combattono la delinquenza in grado di utilizzare le stesse armi di quest'ultima".

Le perplessità del senatore Lawson, che insisteva sull'incostituzionalità delle intercettazioni non riuscirono a far muovere la ferma opinione del capo Woods, che – come il Comitato stesso appurò – aveva personalmente autorizzato tutte le

[276] New York Times, articolo del 17 aprile 1916, dal titolo "Gran Jury To Hear Wire Spying Charge" disponibile al seguente indirizzo: http://query.nytimes.com/mem/archive-free/pdf?res=9906E5DD113FE233A25754C1A9629C946796D6CF.

[277] *Minutes and testimony of the Joint Legislative Committee Appointed to Investigate the Public Service Commissions: transmitted to the Legislature March 30, 1916*, 1916, Volume 6, J.B. Lyon Co., printers, p. 539.

intercettazioni, senza mai preoccuparsi di richiedere un mandato all'Autorità Giudiziaria.

In un ironico editoriale il Washington Post esortava lo Stato ad aprire la posta dei cittadini chiedendosi perché fosse vietato aprire le buste se era lecito intercettare le comunicazioni telefoniche.

È interessante osservare che, mentre l'intercettazione telefonica ricadeva per l'opinione pubblica dell'epoca in una zona grigia al confine tra il lecito e l'illecito (proprio come la neutralità della rete oggigiorno), era universalmente accettato che aprire le buste costituiva attività definitivamente proscritta e intollerabile.

Nella primavera del 1917, la Corte prosciolgieva Kingsbury, avendo accertato che la sua personale condotta non aveva recato danno a nessuno. Il Sindaco John P. Mitchel non fu riconfermato e il suo successore John Francis Hylan si presentò come un paladino della privacy: poi tutto fu dimenticato con l'entrata in guerra degli Stati Uniti nel 1917.

Il caso delle intercettazioni nelle opere pie di New York aveva comunque posto in primo piano la possibilità di utilizzare le tecniche di intercettazione "nel pubblico interesse": una questione rimasta tuttora irrisolta. Il 16 dicembre 2005, il quotidiano New York Times pubblicò un articolo dal titolo "Bush autorizza lo spionaggio telefonico senza un mandato dei tribunali"[278] scritto dai giornalisti investigativi James Risen e Eric Lichtblau, che in seguito vinsero congiuntamente un premio Pulitzer per il loro reportage sulle intercettazioni illegali effettuate dal Governo.

L'articolo si riferisce all'ordine presidenziale del 2002 che autorizza la National Security Agency ad effettuare intercettazioni indiscriminate, telefoniche o telematiche, per trovare tracce del gruppo terroristico "Al Qaeda".

[278] Articolo del New York Times del 16 dicembre 2005, J. Risen, E. Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, disponibile al seguente indirizzo: http://www.nytimes.com/2005/12/16/politics/16program.html

Secondo le fonti di questi giornalisti (e cioè un gruppo di ufficiali che aveva deciso di denunciare il fatto), un massimo di 500 intercettazioni erano attive negli Stati Uniti contemporaneamente in qualunque momento. Nei giorni successivi emerse però che questa cifra era grossolanamente sottostimata[279].

Nel 2006, un tecnico recentemente in pensione dalla AT&T, una delle più importanti aziende telefoniche statunitensi, rivelò alla rivista Wired[280] che la National Security Agency aveva installato presso la sede AT&T di San Francisco un sistema di "data mining" di traffico dati, equipaggiando la postazione[281] con un sistema informatico denominato Narus STA 6400[282], in grado di intercettare simultaneamente decine di migliaia di comunicazioni telematiche. Tale sistema era in grado, effettuando analisi semantiche del traffico in rete, di isolare e ritrasmettere ogni porzione di informazione che avesse riportato alcune parole chiave[283].

Da un punto di vista strettamente legale, il Presidente Bush sostenne di essere autorizzato a compiere questa massiccia attività di sorveglianza in forza dell'"Executive Order 12333" emanato dal Presidente Reagan nel 1981 allo scopo di regolare tutte le attività di *intelligence* a livello statunitense[284].

Secondo molti la lettura di tale *executive order* non consente un'interpretazione così estensiva. Per questo motivo, Electronic Frontier Foundation nel 2006 ha

---

[279] Articolo del *Los Angeles Times* del 25 dicembre 2005, di J. Meyer, J, Menn, *U.S. Spying Is Much Wider, Some Suspect*, disponibile al seguente indirizzo: http://articles.latimes.com/2005/dec/25/nation/na-spy25.

[280] Articolo della rivista *Wired* del 4 luglio 2006 di R. Singel, *Whistle-Blower Outs NSA Spy Room*, disponibile al seguente indirizzo: http://www.wired.com/science/discoveries/news/2006/04/70619

[281] Divenuta poi nota con il nome di "Room 641".

[282] La *Narus* Inc. (http://narus.com) è una società che si occupa dal 1997 di progettare sistemi informatici integrati dedicati esclusivamente all'intercettazione e al monitoraggio del traffico dati. Dal 2010, Narus è stata incorporata all'interno della nota società Boeing.

[283] Un approfondita descrizione delle potenzialità del sistema informatico Narus STA 6400, si suggerisce una lettura dell'articolo, *All About NSA's and AT&T's Big Brother Machine, the Narus 6400*, Dailykos, disponibile al seguente indirizzo: http://www.dailykos.com/storyonly/2006/4/8/14724/28476/

[284] L'*Executive Order* NO. 13222 è disponibile al seguente indirizzo: http://www.archives.gov/federal-register/codification/executive-order/12333.html#Preamble. Da notare, tuttavia, che nel 2008 è stato modificato sensibilmente alla luce delle critiche mosse dopo le rilevazioni fatte dal New York Times del 2005 (http://www.natseclaw.com/natseclaw/2008/07/executive-order.html).

intentato un'azione legale nei confronti della National Security Agency, per conto di svariati utenti della AT&T che si ritengono sottoposti a intercettazione illegittima[285]. Il 25 gennaio 2010, il Giudice si è pronunciato a favore dell'Agenzia. La pronuncia non è ancora definitiva ed è in attesa di passare al vaglio della Corte di Appello.

Occorre ricordare, invece, che il Foreign Intelligence Surveillance Act (FISA) del 1978, descritto nel precedente capitolo, consente di ottenere i dati di registrazione di un utente e i contenuti delle sue comunicazioni anche senza un ordine del Giudice, nel caso in cui sia autorizzato dal Presidente degli Stati Uniti tramite il Procuratore Generale degli Stati Uniti; oppure in base a un ordine rilasciato della Foreign Intelligence Surveillance Court, dopo aver accertato la legittimità e l'effettiva pertinenza della relativa richiesta (ossia che il soggetto sottoposto a sorveglianza sia effettivamente una potenza straniera o un agente di uno Stato estero).

La National Agency Security[286], fin dalla sua fondazione nel 1952, sotto la presidenza Truman, non ha mai goduto di caratteristiche di trasparenza: essa fu oggetto di una indesiderata pubblicità anche agli inizi del nuovo secolo, quando una Commissione temporanea istituita dal Parlamento Europeo rivelò al mondo l'esistenza di "Echelon"[287], un programma prodotto e gestito da un gruppo di

---

[285] Tutti gli atti del processo sono disponibili al seguente indirizzo: http://www.eff.org/cases/jewel. Occorre ricordare che *Electronic Frontier Foundation* aveva già nel 2006 tentato una *class action* nei confronti della AT&T. Anche in quel caso il Giudice aveva deciso a loro sfavore sostenendo che le compagnie telefoniche godevano di un'esenzione di responsabilità in forza del *Foreign Intelligence Surveillance Act*. Per ulteriori informazioni su questo caso: http://www.eff.org/nsa/hepting.

[286] Tra le molte pubblicazioni statunitensi che hanno approfondito il tema, si consiglia, J. Bamford, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*, Anchor Books, 2009.

[287] "Echelon" è un nome in codice utilizzato dalle agenzie di spionaggio degli Stati Uniti per indicare un sistema di sorveglianza ed intercettazione satellitare. Per estensione, la Rete "Echelon" indica il sistema mondiale d'intercettazione delle comunicazioni private e pubbliche (SIGINT), elaborato da Stati Uniti, Canada, Regno Unito, Australia, e Nuova Zelanda. Il Parlamento Europeo, dopo aver costituito La Commissione Parlamentare che ha prodotto nel luglio del 2001 un'ampia relazione su tale sistema di intercettazione (disponibile al seguente indirizzo: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//IT), il 5 settembre 2001 con la Risoluzione (A5-0264/2001) esortava "gli Stati membri a rivedere e se necessario adattare le loro legislazioni nazionali in materia di attività dei servizi di informazione affinché siano compatibili con i

Paesi coordinati dagli Stati Uniti, con l'obiettivo di intercettare ogni forma di comunicazione elettronica su base planetaria.

La questione che rimane irrisolta comprende due aspetti: da un lato i criteri da adoperare per determinare i tipi di dati da sottoporre a sorveglianza, dall'altro i presidi e i meccanismi di monitoraggio e di attuazione che si devono implementare per assicurare che il sistema di intercettazione stesso operi nei confini della legge. La domanda è quella di Giovenale, che compare nel frontespizio del rapporto su "Echelon" della Commissione temporanea del Parlamento europeo: *quis custodiet ipsos custodes?* [288].

3. Le nuove metodologie d'indagine

Come accennato nel precedente paragrafo, mentre negli Stati Uniti sussiste già da tempo molta preoccupazione su possibili violazioni della privacy e dei diritti dell'indagato da parte delle forze dell'ordine, la stessa questione ha attirato l'attenzione pubblica per la prima volta in Europa solo in seguito alle rivelazioni sull'Echelon nel luglio del 2001, ed è divenuta questione di massima attualità solo dopo gli attacchi alle Torri gemelle lo stesso anno.

Per comprendere la ragione di questo diverso approccio si consideri che le leggi sulla protezione dei dati personali introdotte dal *Land* tedesco dell'*Hessen* nel 1970[289], dalla Svezia nel 1973[290], dalla Repubblica Federale Tedesca nel 1977[291]

---

diritti fondamentali come definiti dalla CEDU e con la giurisprudenza della Corte dei diritti dell'uomo" il testo della risoluzione è disponibile al seguente indirizzo: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2002:072E:0221:0229:IT:PDF.

[288] La dicitura latina si traduce letteralmente "chi sorveglierà gli stessi sorveglianti?" È curioso osservare che, mentre negli Stati Uniti l'irrisolto problema delle intercettazioni nasce da decisioni governative (dal Governatore Whitman nel 1915, al Presidente Bush nel 2005), in Italia il Governo fa di tutto per limitare tale strumento investigativo mentre il potere giudiziario cerca in ogni modo di rivendicarne la sua validità (si veda ultimo il disegno di legge n. 1161 del 2010 per la riforma della disciplina delle intercettazioni, disponibile al seguente indirizzo: http://parlamento.openpolis.it/singolo_atto/38631)

[289] Datenschutzgesetz, 1970, disponibile al seguente indirizzo: http://www.datenschutz.rlp.de/downloads/hist/ldsg_hessen_1970.pdf

[290] The Data Act, 1973 disponibile in inglese al seguente indirizzo: http://archive.bild.net/dataprSw.htm.

e dalla Francia nel 1978[292], e le direttive europee 95/46/CE, 2002/19-20-21/CE, 2006/24/CE e 2009/140/CE hanno tutte una matrice comune: la Convenzione Europea sui Diritti dell'Uomo.

Sebbene l'ar7. 8 sancisca il princio cardine secondo cui: "ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza", a differenza del quarto emendamento statunitense, il secondo comma dello stesso articolo ammette con molta più "rassegnazione" una possibile ingerenza della pubblica autorità nell'esercizio di tale diritto, qualora "costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, l'ordine pubblico, il benessere economico del paese, la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui"[293].

Secondo James Q. Whitman, titolare della cattedra istituita dalla Ford Foundation in diritto comparativo ed estero presso la Yale Law School, il contrasto tra il Quarto Emendamento statunitense e l'art. 8 CEDU deriva dalle due distinte culture della privacy sviluppatesi sulle opposte sponde dell'Atlantico in conseguenza di idee-guida profondamente diverse: negli Stati Uniti quella di libertà, in Europa quella di dignità[294].

Queste diverse ideologie sono frutto della storia specifica di ciascuno dei due continenti. In Europa, dove per secoli la dignità era riservata ai nobili, la spinta per la dignità di tutti gli uomini ha accompagnato le lotte degli ultimi due secoli,

---

[291] Bundesdatenschutzgesetz (BDSG), 1977, disponibile in inglese al seguente indirizzo: http://www.iuscomp.org/gla/statutes/BDSG.htm.

[292] Loi n. 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*, disponibile al al seguente indirizzo: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20101103.

[293] Ne è una chiara dimostrazione il caso *Leander v. Sweden,* (Corte Europea dei Diritti dell'Uomo del 26 marzo 1987, 9 EHRR 433, para. 59) in cui veniva negato l'accesso di un fascicolo riservato in possesso delle Forza di Polizia ad una candidata ad un concorso per un incarico governativo. La motivazione giustificava tale diniego sostenendo che era applicabile l'art. 8, comma II, Convenzione CEDU.

[294] J. Whitman, *The two western cultures of privacy: Dignity vs Liberty*, in *The Yale Law Journal*, vol. 113, n 6, p. 1151.

così come la spinta libertaria e liberale ha accompagnato la rivoluzione e la successiva evoluzione americana.

Sempre secondo Whitman, la privacy europea tende a salvaguardare la riservatezza della persona di fronte al principale soggetto che la minaccia: il sistema dei *media* prima e, con l'avvento delle nuove tecnologie, quello derivante dalla società dell'informazione poi. La privacy statunitense si erge a tutore dell'inviolabilità delle pareti domestiche nei confronti della principale minaccia, vista come l'intrusione dello Stato.

Più statalisti degli americani, gli europei sono più inclini a cedere quote della loro autonomia personale allo Stato, mentre mal sopportano intrusioni da parte della stampa e dei nuovi *media*; gli americani, al contrario considerano a partire da Jefferson[295] la libertà di stampa come valore fondante della Costituzione, ma provano un'assoluta ripugnanza per la burocrazia europea che interviene perfino sui nomi da imporre ai neonati.

Gli europei non riescono a comprendere le indagini creditizie che caratterizzano la politica bancaria americana, così come la cordiale brutalità con cui gli amici americani chiedono loro quanto guadagnino. Per gli americani, invece, l'obbligo della carta d'identità è inaccettabile, così come è offensivo il nudismo ostentato dai vip europei (i vestiti come ultima barriera della "home").

La tecnologia (*trusted computing* e ogni altra forma di crittografia) e la rapidità con cui si evolve la Rete (motori di ricerca, *social network* e *cloud computing*), tuttavia, stanno progressivamente facendo cadere le diversità nell'approccio al tema della privacy: le recenti decisioni della Corte Costituzionale tedesca[296] dimostrano come anche l'Europa sia consapevole dell'importanza che riveste

[295] "Our liberty cannot be guarded but by the freedom of the press, nor that be limited without danger of losing it" Lettera di Thomas Jefferson a John Jay, del 1786.

[296] Corte Costituzionale tedesca, 2 marzo 2010 in tema di *data retention* (*Vorratsdatenspeicherung*), cfr. paragrafo 2.1 del capitolo II e Corte Costituzionale tedesca, 27 febbraio 2008 in tema di ricerche *on line* (*online durchsuchung*), che analizzeremo nel prossimo paragrafo.

oggi il corretto bilanciamento tra esigenze investigative e diritti fondamentali dell'individuo.

Nei prossimi paragrafi cercheremo di dimostrare come, a distanza di soli dieci anni dalla Convenzione Cybercrime, le attuali metodologie d'indagine digitale rendano necessaria la predisposizione di una nuova regolamentazione condivisa a livello internazionale.

3.1 Dati digitali pubblici e social network

La società Intelius Inc. fornisce, per un importo variabile da 1 a 10 dollari, le seguenti informazioni relative ad ogni cittadino americano: indirizzi in cui ha abitato, numero di telefono e di cellulare, indirizzo e-mail, precedenti penali, situazione economico finanziaria e patrimoniale, precedenti attività lavorative e grado di scolarizzazione. Tutte queste informazioni sono tratte, a detta della Società, da registri pubblici[297]: se questa affermazione, presente nel sito Intelius, fosse vera, dimostrerebbe che le informazioni pubbliche che ogni giorno vengono immesse in Rete, consentono di reperire un numero rilevante di dati finora ritenuti inaccessibili.

Date Check, uno dei tanti servizi di Intelius, inoltre, consente di conoscere tutte le informazioni sul proprio potenziale partner, semplicemente digitando dal proprio cellulare il suo numero di telefono: si passa dai dati personali, ai precedenti penali, alla situazione economico-finanziaria, al livello d'istruzione e finalmente all'utilissimo stato di famiglia, così che, in pochi istanti, dal proprio cellulare si può sapere se la persona davanti a sé sia di proprio gusto[298].

---

[297] Curiosamente, tuttavia, la Società Intelius preferisce non chiarire nel dettaglio le modalità con cui vengono acquisiti tali dati http://www.seattleweekly.com/2009-03-18/news/intelius-and-the-dubious-art-of-post-transaction-marketing/

[298] Esemplificativo è il video che descrive le potenzialità del servizio: http://www.youtube.com/watch?v=WLc2JLYx78k&feature=player_embedded#; diverso, ma non per questo meno interessante, è il sito www.dondatehimgirl.com dove le ragazze deluse da un appuntamento, possono mettere in guardie le atri utenti del sito, descrivendo i comportamenti negativi del ragazzo con cui sono uscite.

La giurisprudenza statunitense[299] ha sancito che "il Quarto Emendamento non proibisce di utilizzare informazioni rivelate da un soggetto ad una terza persona e da questa trasmesse all'Autorità governativa, anche se queste informazioni sono state rivelate nel presupposto di un utilizzo per uno scopo limitato". Questo principio, se applicato acriticamente alla realtà del *web 2.0*, consente a società private come alle forze di polizia di accedere senza limitazioni, sia in fase investigativa, sia con finalità di prevenzione, a tutte le informazioni contenute all'interno dei *social network*.

I rischi inerenti alla pratica sempre più diffusa in seno alle forze dell'ordine presso i *campus* universitari statunitensi di avvalersi di dati estratti da pagine Facebook per contrastare l'abuso di alcol da parte di studenti minorenni, si sono manifestati con schiacciante chiarezza in un simile caso in cui tali dati sono stati utilizzati a sostegno di un'indagine penale[300]. Sospettando due studenti di aver rubato due console di Playstation 3 nel dicembre del 2006, la polizia del *campus* dell'Università del North Carolina si apprestava a perquisire l'abitazione che i due condividevano. Informati che uno dei due sospetti aveva pubblicato su Facebook una foto di se stesso in posa con svariate armi e perciò aspettandosi una possibile resistenza violenta, i poliziotti del *campus* decisero di avvalersi dell'assistenza di una squadra SWAT (*Special Weapons And Tactics*) per fare irruzione nell'abitazione degli studenti. Il risultato dell'operazione fu tragico: uno degli agenti dello SWAT, scambiando il rumore della porta che veniva abbattuta per uno sparo, aprì il fuoco, causando la morte di uno dei ragazzi e del suo cane.

Sebbene questo caso estremo non permetta alcuna generalizzazione, evidenzia indubbiamente la necessità urgente di una seria riflessione sull'opportunità di

[299] *United States v. Miller*, 425 U.S. 435, 443 (1976).
[300] S. M. Birnbaum, *The Profile Police, Campus Officers Cruise Facebook, MySpace for Clues to School-Related Crimes, to Some Students' Chagrin*, Washington Post, Apr. 6, 2009, 1.

meramente considerare le informazioni ricavate dai *social network* come meramente pubbliche.

Immettere contenuti su una pagina web è cosa ben diversa da pubblicare fotografie di se stessi su un social network poiché nel primo caso è chiara l'intenzione dell'utente di rendere i contenuti pubblici, mentre nel secondo è fuori dubbio che le foto sono rivolte a una cerchia ristretta di amici[301].

In Italia, è facoltà della polizia giudiziaria di avvalersi liberamente, nel corso delle indagini, di tutti i dati pubblicamente accessibili sulla rete e non protetti da password, poiché secondo la giurisprudenza l'accesso a tali dati non costituisce "intercettazione delle comunicazioni private intercorse per via informatica o telematica di cui all'articolo 266 *bis* c.p.p. che, attenendo alla sfera personale, rientra nell'ambito della riservatezza costituzionalmente garantita"[302]. Di conseguenza è fatto divieto alle forze dell'ordine di accedere ai profili di utenti di social network che scelgono di mantenere riservati i dati in questione, dal momento che le informazioni non liberamente accessibili al pubblico non possono considerarsi "aperte"[303].

---

[301] R. Flor, *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del* Bundesverfassungsgericht *del 27 febbraio 2008, sulla Online Durchsuchung e la sua portata alla luce della sentenza del 2 marzo 2010 sul* data retention, in *Ciberspazio e diritto*, Vol. 11, n. 2, 2010, p. 368.

[302] Tribunale Milano, 30 ottobre 2002, in *Foro ambrosiano*, 2003, p. 55. La fattispecie riguardava la consultazione di un sito relativo ad una vendita *online* aperta ad un numero indeterminato di possibili clienti, del tutto assimilabile ad un'offerta di vendita di prodotti pubblicizzata su di una qualsiasi rivista cartacea di annunci commerciali. Si osserva, inoltre, che il D.M. del 20 agosto 2006 sul Riassetto dei comparti di specialità delle Forze di Polizia prevede che "La Polizia postale e delle comunicazioni è, altresì, impegnata in attività di investigazione per la prevenzione ed il contrasto alle violazioni sul diritto d'autore […] le quali possono svolgersi anche attraverso il monitoraggio di internet per individuare le violazioni commesse attraverso la Rete".

[303] L'accesso a tali dati per scopi investigativi è consentito solo nell'ambito di indagini mirate a combattere la pedopornografia. Ai sensi dell'art. 14 della legge n. 269 del 3 agosto 1998, come modificato dall'art. 16 legge n. 38 del 15 febbraio 2006, gli ufficiali di polizia possono addirittura agire da "agenti provocatori" sfruttando siti web "civetta" concepiti appositamente per servire da trappola a possibili utenti che immettono o scaricano contenuti pedopornografici *online*. Per un approfondimento si veda A. Manna-F. Resta, *I delitti in tema di pedopornografia, alla luce della legge 38/2006. una tutela virtuale?*, in *Dir. Internet*, 2006, p. 223; L. Pistorelli, *Colmate le lacune della pregressa disciplina*, in *Guida al diritto*, 2006, n. 9, p. 45 e ss.; V. Musacchio, *La nuova normativa penale in materia di sfruttamento sessuale dei bambini e pedopornografia a mezzo internet*, in *Riv. pen.*, 2006, p. 399.

Tuttavia, considerando che le bacheche[304] di molti profili di *Facebook* o di altri *social network* non sono "nascoste", è possibile non solo recuperare dati utili all'identificazione del soggetto, ma anche intercettare il contenuto delle sue conversazioni o scoprire la sua rete di contatti. Diventa, quindi, indispensabile classificare i dati digitali presenti sui *social network* in funzione della loro accessibilità.

Un interessante sondaggio condotto dall'Istituto "Privacy and Cybercrime" della Ryerson University a Toronto, su un campione di 2000 studenti canadesi, ha dimostrato che mentre la maggior parte dei giovani considera riservate le informazioni immesse in un social network (in base ad una sorta di "privacy del network") a differenza di quelle pubblicate su siti web, sia le istituzioni accademiche, sia le imprese non riconoscono tale concetto e ritengono, al contrario, che qualsiasi informazione emessa in rete debba ritenersi pubblica e priva di tutela[305].

È indubbio è che più l'Internet si rivela una fonte ricchissima di indizi utili per scoprire, combattere e prevenire il crimine, maggiore sarà la tendenza delle forze dell'ordine di avvalersi di tecniche forensi digitali. La giurisprudenza farà bene a non sottovalutare questo fenomeno e di stabilire i criteri per definire i tipi di dati online che possono essere legittimamente sfruttati dalle forze dell'ordine per generare elementi probatori ammissibili agli atti: considerare il "domicilio

[304] La "bacheca" di un *social network* (in inglese "*wall*", ossia muro) costituisce un luogo virtuale dove un utente scrive dei brevi messaggi che vengono visualizzati in tempo reale solo da tutte le persone che appartengono al suo gruppo di contatti. Tuttavia, se l'utente non ha impostato correttamente le impostazioni della privacy, tali messaggi possono essere visti da chiunque, in quanto i contenuti immessi in tale "bacheca" sono visibili a tutti gli utenti del *Social Network* in questione.

[305] Significativo a riguardo è il caso di una donna canadese che soffriva di depressione e che si è vista negare quanto le spettava per il congedo per malattia poiché l'assicuratore del suo datore di lavoro sarebbe venuto a conoscenza di fotografie che la donna aveva pubblicato su Facebook, ritraendola in vacanza mentre era sedicentemente in mutua dimostrando secondo l'assicuratore che non soffriva affatto di depressione. La donna si è difesa sostenendo che aveva avvisato la compagnia assicurativa che sarebbe partita in quanto il suo medico le aveva consigliato come terapia una vacanza in un posto caldo. Articolo di CBC News del 21 novembre 2009, *Depressed woman loses benefits over Facebook photos*, disponibile al seguente indirizzo: http://www.cbc.ca/canada/montreal/story/2009/11/19/quebec-facebook-sick-leave-benefits.html.

virtuale" di un utente di un *social network* come un luogo liberamente accessibile significa non comprendere il ruolo e la finalità con cui tali strumenti vengono utilizzati.

Ne è conferma il recente progetto inglese denominato "Interception Modernisation Programme"[306] che, sulla falsariga del progetto statunitense "NSA Call Database", dovrebbe comportare la creazione di una banca dati integrata in cui potrebbero venire memorizzati non solo i numeri di telefono chiamati e gli indirizzi *e-mail*, ma anche i siti *web* e i *social network* visitati da milioni di cittadini britannici. Tale progetto, fortemente osteggiato dal gruppo a utela della privacy APPG (All Party Parliamentary Privacy Group), ove dovesse diventare operativo, dimostrerebbe sicuramente la carenza di attenzione che, a livello europeo, fino ad ora è stata rivolta all'enorme potenziale delle informazioni contenute nel web 2.0.

È altrettanto vero che, come hanno spesso ricordato le Autorità Garanti della privacy in Europa, è importante che vi sia anche da parte delle nuove generazioni e non solo, una maggiore responsabilizzazione sul tipo di contenuti che all'interno di questo "domicilio virtuale", vengono immessi[307].

Negli Stati Uniti la sensibilità rispetto a tale tema sembra essere maggiore, anche perché i servizi commerciali collegati ne evidenziano ancora di più i potenziali rischi[308]. Nella causa civile Crispin v. Christian Audigier, Inc., et al., la Corte Distrettuale Centrale della California ha parzialmente annullato un provvedimento (*subpoena duces tecum*) che obbligava due noti *social network* (Facebook e MySpace) a divulgare sia i messaggi privati sia i contenuti da "bacheca" riferiti agli account dell'attore allo scopo di chiarire le ragioni dei

[306] Per un approfondimento sul progetto "Interception Modernisation Programme" si consiglia la lettura del documento redatto dalla London School of Economics, disponibile al seguente indirizzo: http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/IMP_Briefing.pdf.

[307] Working Party "Article 29": *Opinion 5/2009 on online social networking*, adottato il 12 giugno 2009, (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf)

[308] T. P. Crocker, *From Privacy To Liberty: The Fourth Amendment After Lawrence*, 57 UCLA L. Rev. 1.

convenuti in una complessa vicenda nata da pretese violazioni di copyright[309]. La Corte ha ritenuto totalmente invalido il provvedimento per quanto riguarda i messaggi privati, mentre ne ha solo sospeso l'efficacia in merito ai contenuti immessi in "bacheca" rimandando tale aspetto all'accertamento del giudice di primo grado con lo specifico compito di determinare, sulla base delle impostazioni di privacy emesse dall'utente, se i contenuti da "bacheca" debbano considerarsi accessibili al pubblico in generale o solo a una cerchia ristretta di amici e confermare o annullare il proprio provvedimento di conseguenza. Nella sentenza è stato precisato che non è illecito intercettare o divulgare comunicazioni elettroniche rivolte al pubblico in generale anche senza specifica autorizzazione giudiziaria. L'attenzione dimostrata dalla Corte statunitense sul tema della diversa accessibilità dei dati digitali contenuti all'interno dei *social network*, rappresenta un segnale indubbiamente positivo ed è auspicabile che la medesima sensibilità venga adottata anche dai Giudici europei.

3.2 La crittografia e le garanzie dell'indagato

Uno dei problemi più spinosi che si possa affrontare nell'ambito di una perquisizione sorge qualora l'indagato si rifiuti di fornire la chiave d'accesso al proprio personal computer o altro supporto informatico.

Da un punto di vista giuridico, questa scelta è più che legittima, in quanto nessuno può essere obbligato a fornire dichiarazioni auto-indizianti (art. 63 c.p.p. e il Quinto Emendamento della Costituzione statunitense). Ne discende che gli ufficiali di polizia giudiziaria sono costretti a tentare di scoprire le chiavi d'accesso necessarie sfruttando tecniche forensi digitali.

[309] *Crispin v. Christian Audigier*, 2010 U.S. Dist. LEXIS 52832 (C.D. Cal. May 26, 2010), disponibile al seguente indirizzo: http://www.huntonfiles.com/files/webupload/PrivacyLaw_Crispin_v_Christian_Audigier.pdf

Se la *password* di protezione è inserita a livello di sistema operativo, il recupero della stessa è molto semplice; lo è di meno nel caso in cui la *password* sia stata inserita prima dell'avvio del sistema operativo[310]; come comportarsi, tuttavia, nel caso in cui l'indagato abbia crittografato l'*hard disk* con una chiave a 256-bit e non sia intenzionato a rilasciare la chiave di decifratura?

Come è noto ai più la crittografia è una tecnica per rendere inintellegibili documenti a chi non dispone della relativa chiave e dell'algoritmo necessario a decifrarli. Esistono molti software per decifrare un *hard disk* crittografato e tutti garantiscono il successo, ma nessuno è in grado di garantire la durata di tale operazione[311].

É, infatti, totalmente inutile tentare di prevedere il tempo necessario per superare la cifratura, dato che tale operazione potrebbe durare da pochissimi secondi a svariate migliaia di anni in funzione sia del tipo di algoritmo usato per la protezione dei dati in questione sia degli strumenti di decifratura a disposizione. Ad esempio una chiave di cifratura a 20-*bit* consente fino a un milione di combinazioni possibili, per cui con un normalissimo computer portatile che processa circa un milione di operazioni al secondo, il tempo di cifratura massimo sarà addirittura inferiore al secondo. Tuttavia con un sistema di cifratura con una chiave a 56-*bit* lo stesso elaboratore potrebbe impiegare fino a 2285 anni per verificare tutte le combinazioni possibili. Per rendersi conto della complessità di

---

[310] Vi sono centinaia di *blog* che spiegano nel dettaglio quali sono le attività da compiere e i *software* da utilizzare. A livello scientifico si suggerisce: S. McClure, J. Scambray, G. Kurtz, *Hacker 6.0*, Milano, 2009, Apogeo, p. 165 oppure, anche se meno aggiornato, A. Ghilardini, G. Faggioli, *Computer Forensics*, *op. cit.*, p. 173.

[311] Per un approfondimento sugli strumenti per decifrare un dato criptato si veda: E. Casey G. J. Stellatos, *The impact of full disk encryption on digital forensics*, in *Operating Systems Review*, 2008, 42 (3): 93–98; C. Frichot, *An Analysis and Comparison of Clustered Password Crackers*, 2004, p. 3, disponibile al seguente indirizzo: http://scissec.scis.ecu.edu.au/publications/forensics04/Frichot-1.pdf; per un approfondimento circa la complessità di decifrare tali tali si veda: Regarding practical approaches in responding to the challenge of encryption see: J. Siegfried, C. Siedsma, B. Countryman, C. Hosmer, *Examining the Encryption Threat*, in *International Journal of Digital Evidence*, Vol. 2, Issue 3, disponibile al seguente indirizzo: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf.

tale operazione basti considerare che la più diffusa versione del software di cifratura PGP (Pretty Good Privacy) al momento attuale si basa su una chiave di 1024-bit[312].

Vista l'impossibilità di trovare una soluzione da un punto di vista tecnico, negli ordinamenti anglosassoni si è tentato un approccio diverso: negli Stati Uniti un Giudice federale del Vermont (Jerome Niedermeier) ha annullato un ordine emesso da una *Grand Jury* con il quale l'indagato (Sebastien Boucher) era stato obbligato a rivelare la chiave d'accesso alla partizione crittografata del proprio portatile sul quale erano state rinvenute immagini sessualmente esplicite di minorenni nel corso di una perquisizione di routine effettuata alla frontiera tra Stati Uniti e Canada. Le immagini sono emerse dopo che il Boucher aveva volontariamente concesso loro l'accesso ai contenuti del proprio portatile. Dopo l'analisi preliminare effettuata dalla polizia di frontiera, tuttavia, il portatile è stato spento e acquisito agli atti. Il perito tecnico legale incaricato di esaminare l'elaboratore ha successivamente scoperto che l'*hard disk* in questione era protetto da crittografia. La Procura ha quindi ottenuto dalla Grand Jury un ordine obbligando il Boucher a rivelare la *password* ai dati memorizzati sulla partizione crittografata[313]. Il Giudice Niedermeier ha annullato tale ordine ritenendo che lo stesso fosse in contrasto con il diritto a non fare dichiarazioni autoincriminanti spettante al Boucher in base al Quinto Emendamento. La decisione del Giudice

[312] Come se non fosse sufficiente, esistono sul mercato numerose applicazioni di "Trusted Computing" che hanno l'obiettivo di rendere dispositivi come computer o telefoni cellulari più sicuri mediante l'uso di opportuni *hardware* e *software*. Il raggiungimento di tale scopo viene ottenuto inserendo in ogni dispositivo un processore (denominato Trusted Platform Module o più brevemente TPM) dotato di una coppia di chiavi crittografiche (univoca per ogni chip), impossibili da modificare anche per il proprietario, e capace di generare altre chiavi per la crittografia di dati o dispositivi. Per un apprendimento sull'ambiente di *Trusted Computing*, si consiglia S. Mason, *Trusted computing and forensic investigations*, Vol.2, N.2, p. 189, disponibile al seguente indirizzo: http://www.stephenmason.eu/articles/trusted-computing-and-forensic-investigations/; M. Burmester, J. Mulholland, *The Advent of Trusted Computing: Implications for Digital Forensics*, disponibile al seguente indirizzo: http://www.cs.fsu.edu/~burmeste/tc.pdf; Vol. 2, Issue 4; M. Carney, M. Rogers, *Casey Practical Approaches to Recovering Encrypted Digital Evidence*, in *International Journal of Digital*, Volume 1, questione 3.

[313] In Re Grand Jury Subpoena to Boucher, 2007 WL 4246473 available at: http://www.crowell.com/PDF/In-re-Boucher.pdf

Niedermeier è stata rovesciata in appello dalla Corte Distrettuale Federale che ha stabilito che il diritto previsto dal Quinto Emendamento non rilevasse nel caso in esame, in quanto, con la rivelazione della chiave d'accesso o la presentazione dei dati in forma intellegibile, l'indagato non avrebbe comunque concesso alla Procura alcun indizio testimoniale in merito alla sua incriminazione (esistenza dell'*hard disk*, ubicazione nel portatile e/o la sua autenticità), poiché tali elementi risultavano stabiliti *ipso facto* ("*as a foregone conclusion*") dalla circostanza stessa che l'indagato aveva già ammesso di essere in possesso e in controllo del portatile e che gli agenti di polizia avevano visionato le immagini incriminate[314].

In Inghilterra, invece, nel febbraio del 2007 è stata emanata un'apposita norma (*section 49*) all'interno del Regulation of Investigatory Powers Act (RIPA) del 2000 che obbliga l'utente a rivelare la chiave di cifratura nel caso di dati criptati[315].

Esistono, tuttavia, strumenti che, creando diversi livelli di crittografia su diverse partizioni dell'*hard disk*, sono in grado di ingenerare nei pubblici ufficiali la convinzione di aver ottenuto l'accesso ai dati, quando in realtà è ancora presente una partizione crittografata[316].

A livello nazionale, fortunatamente, il problema della crittografia non ha ancora assunto livelli preoccupanti e forse per questo non vi sono stati interventi né a livello giurisprudenziale, né a livello normativo

4. L'intervento della Corte Costituzionale tedesca sugli strumenti di monitoraggio online

[314] In Re Grand Jury Subpoena to Boucher, 2007 WL 4246473 available at: http://www.volokh.com/files/Boucher.pdf

[315] La norma di riferimento del RIPA è disponibile al seguente indirizzo: http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_8

[316] Per un approfondimento si veda: M. Ward, *Campaigners hit by decryption law*, BBC News, 20.11.2007, disponibile al seguente indirizzo: http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/technology/7102180.stm

Il 20 dicembre del 2006, la Germania ha introdotto, come emendamento al § 5 co. 2, n. 11 della legge sulla protezione della Costituzione nel Nord Reno-Westfalia[317], una legge in materia di raccolta e trattamento dei dati degli utenti da sistemi informatici o attraverso la Rete[318].

L'emendamento rinforzava i servizi segreti nazionali, ossia "L'Ufficio Federale per la Protezione della Costituzione" (*Bundesamt für Verfassungsschutz*) poiché autorizzava l'istituzione di un apposito organismo incaricato di effettuare due diverse tipologie di indagine: l'accesso segreto a sistemi informatici e il monitoraggio segreto della Rete[319].

L'accesso a sistemi informatici poteva avvenire sia attraverso l'installazione di strumenti hardware (sonda e intercettazioni parametriche su dorsali di comunicazione) che abbiamo già analizzato nel capitolo relativo alle modalità operative dell'intercettazione telematica, sia attraverso sistemi "da remoto", ossia software (*keylogger*, *sniffer*) installati in forma di *trojan horse* ad insaputa dell'utente, ma con la partecipazione attiva di quest'ultimo che viene indotto a

---

[317] Legge sulla protezione della Costituzione del Nord Reno-Westfalia (*Gesetz über den Verfassungsschutz in Nordrhein-Westfalen*) come modificato il 20 dicembre 2006, § 5 co. 2, n. 11, § 7 co. 1, § 5 co. 3, § 5° co. 1 e § 13 (VSG). Per un approfondito commento si veda, R. Flor, *Brevi Riflessioni a margine della sentenza del* bundesverfassungsgericht *del 27 febbraio 2008, sulla c.d.* Online Durchsuchung. *La prospettiva delle investigazioni ad alto contenuto tecnologico ed il bilanciamento con i diritti inviolabili della persona. Aspetti di diritto penale sostanziale*, in *Riv. trim. dir. pen. ec.*, 3, 2009, p. 695; W. Abel, B. Schafer, *La decisione della Corte Costituzionale tedesca sul diritto alla riservatezza ed integrità dei sistemi tecnologici d'informazione – un rapporto sul caso BVerfGE*, NJW 2008, p. 822, disponibile in italiano al seguente indirizzo: http://www.jei.it/approfondimentigiuridici/notizia.php?ID_articoli=601.

[318] Il dibattito pubblico e giuridico su questo argomento si scatenò nel 2006 a partire da un ricorso proposto da un procuratore statale al fine di ottenere dalla Corte Federale di giustizia tedesca (*Bundesgerichtshof*) l'autorizzazione di effettuare il monitoraggio a distanza di certi sistemi informatici utilizzati da svariati indagati, in base all'applicazione per analogia e quindi *de jure condendo* della disciplina in materia delle normali perquisizioni di locali fisici. Rigettando il ricorso la Corte Federale di Giustizia ha ritenuto che non era possibile trarre valide analogie tra il monitoraggio clandestino a distanza di elaboratori e la perquisizione di locali fisici, ma non ha totalmente precluso l'adozione di nuove leggi concepite appositamente per dotare le forze dell'ordine di specifici poteri per perquisire dati digitali in transito sulla rete o memorizzati su supporti informatici allo scopo di assicurare la pubblica sicurezza e contrastare la criminalità. É stata quest'ultima parte della decisione che è servita da spunto per la modifica della legge a protezione della Costituzione del Nord Reno-Westfalia.

[319] I poteri di monitoraggio clandestino del traffico web consentivano la raccolta di informazioni non solo tramite i canali abituali quali i siti web pubblicamente accessibili, le bacheche pubbliche, le chat e altri forum online, ma anche tramite l'accesso diretto a siti web privati e protetti grazie all'uso di password ottenute da altre fonti compresi pentiti e informatori.

scaricare i programmi maliziosi con ingannevoli tecniche di *social engineering*[320].

Ai sensi di tale normativa, si potevano attivare, senza alcuna autorizzazione preventiva giudiziaria, le suddette attività di monitoraggio che potevano proseguire senza alcun limite di tempo.

Per questo motivo, la Corte Costituzionale ha preso in esame l'incostituzionalità di tale normativa sotto tre distinti profili: la riservatezza delle comunicazioni[321], l'inviolabilità del domicilio[322] e il "diritto all'autodeterminazione informativa"[323], diritti costituzionalmente protetti dalla Legge Fondamentale[324].

Per quanto riguarda la riservatezza delle comunicazioni, la Corte Costituzionale ha affermato che la protezione di questo diritto fondamentale copre ogni tipo di telecomunicazione a prescindere dal mezzo di trasmissione utilizzata (via cavo o radiotrasmissione, trasmissione analogica o digitale) e dal tipo dei dati trasmessi

---

[320] Cfr. capitolo II, par. 2.5; per un approfondimento si consiglia S. McClure, J. Scambray, G. Jurtz, *op. cit.*, p. 269; sulla possibilità di creare un *keylogger* per recuperare i dati biometrici, M. Lewis, *Biologger - A Biometric Keylogger*, IRM Research, presentato alla *Black Hat Conference*, Amsterdam, 27-28 marzo 2008, disponibile al seguente indirizzo; http://www.blackhat.com/presentations/bh-europe-08/Lewis/Whitepaper/bh-eu-08-lewis-WP.pdf; per i più pazienti si consiglia l'episodio 621 della Internet TV Hak5 (www.hak5.org) *dal titolo MiTM Javascript Keylogger, Social Engineering Toolkit and more* disponibile al seguente indirizzo: http://www.hak5.org/?s=keylogger&x=0&y=0.

[321] Articolo 10 *Grundgesetz*: "1. La riservatezza della corrispondenza, della posta e delle telecomunicazioni è inviolabile. 2. Le restrizioni possono essere ordinate solo in virtù della legge. Se la restrizione serve a proteggere il libero ordine democratico fondamentale o l'esistenza o la sicurezza della Federazione o del Lander, la legge può prevedere che la persona interessata non debba essere informata della restrizione e che il ricorso ai tribunali venga sostituito da una revisione del caso da parte di agenzie e agenzie ausiliarie nominate dal legislatore".

[322] Articolo 13 *Grundgesetz*: " 1. La dimora è inviolabile. 2. Le ricerche possono essere autorizzate solo da un giudice o, quando il tempo è essenziale, da altri autorizzati designati dalla legge, e possono essere effettuate solo nei modi in questa prescritti".

[323] Il diritto "all'autodeterminazione informativa" deriva dall'articolo 2 co. 1 in combinato disposto con l'articolo 1 co, 1 GG, i quali garantiscono rispettivamente il diritto al "libero sviluppo della propria personalità" ed il "diritto alla dignità della persona". Tale diritto era stato riconosciuto dalla Corte Costituzionale tedesca in una storica decisione che aveva avuto un ruolo determinante per l'adozione della legge sulla protezione dei dati personali (Sentenza del *Bundesverfassungsgerichts* del 15 dicembre 1983, BVerfGE, 65, 1, <43>; 84, 192).

[324] Interessante notare che la Corte interpellò ben quattro consulenti tecnici: tre provenienti dal mondo accademico (Prof. Felix Freiling, della cattedra di Informatica dell'Università Mannheim, Prof. Dr. Andreas Pfitzmann, capo del gruppo di privacy e sicurezza dell'Università di tecnologie di Dresden e il Prof. Dr. Ulrich Sieber, direttore dell'Istituto per il diritto penale estero ed internazionale Max Plank e uno proveniente dal mondo "hacker" (Andreas Bogk, collaboratore esterno in qualità di *hacker* al Clozure Inc e CEO del Chaos Computer Club Events).

(discorsi, immagini, suoni, o altre informazioni). Tuttavia la Corte ha anche sottolineato che tale protezione non si applica nel caso in cui i dati delle telecomunicazioni siano memorizzati all'interno di un computer dopo il termine della trasmissione. Questo significa che il recupero di dati a distanza da un hard disk in ragione del diritto fondamentale alla riservatezza delle comunicazioni.

Per quanto riguarda il secondo diritto fondamentale in gioco nella fattispecie, la Corte Costituzionale ha osservato che l'inviolabilità del domicilio, garantita dall'art. 13.1 GG, forniva protezione solamente contro l'intrusione fisica in locali privati allo scopo di manomettere i sistemi informatici ivi ubicati. Tuttavia, poiché l'accesso può essere eseguito a prescindere dal luogo in cui è situato il sistema tecnologico, la tutela potrebbe rivelarsi inadeguata ogni qualvolta i dispositivi elettronici in questione si trovino al di fuori di locali privati.

La Corte Costituzionale ha, infine, esaminato la legge alla luce del "diritto all'autodeterminazione informativa" che tutela gli utenti web dalla raccolta e dalla successiva profilazione dei dati immessi in rete. Anche in questo caso, tuttavia, l'attività di monitoraggio prevista ai sensi della modifica della legge sulla protezione della Costituzione va oltre la semplice raccolta di dati personali a fini di profilazione, visto che l'accesso non autorizzato a qualsiasi sistema informatico è atto di per sé a potenzialmente fornire un tesoro di dati altamente sensibili riferiti al proprietario senza alcuna necessità di sottoporre i dati raccolti a qualunque genere di profilazione.

La Corte Costituzionale, non avendo trovato sufficiente tutela nei precedenti tre diritti garantiti dalla "legge fondamentale", ha optato per il riconoscimento di un nuovo "diritto alla riservatezza ed alla integrità dei sistemi informatici".

Alla stessa stregua del "diritto all'autodeterminazione informativa", il "diritto alla riservatezza e alla integrità dei sistemi informatici" ha come presupposto il combinato disposto dell'art. 2.1 GG (diritto allo sviluppo della personalità di ogni cittadino) con l'art. 1.1 GG (diritto alla dignità della persona) e tutela ogni

cittadino dall'accesso da parte dello Stato ai sistemi informatici nel loro complesso: sia nel caso siano utilizzati per la comunicazione che per la memorizzazione di dati.

Pur concedendo che il diritto fondamentale alla garanzia della riservatezza e l'integrità dei sistemi informatici non sia assoluto e potrebbe quindi essere sottoposto a limitazione sopratutto nell'interesse di contrastare la criminalità, la Corte Costituzionale ha insistito sul fatto che tali limitazioni potrebbero essere tollerate solo al fine di tutelare valori fondamentali prevalenti che la Corte stessa ha specificatamente elencato in:

- la vita e l'integrità degli altri cittadini;
- i fondamenti dello Stato;
- i valori essenziali di umanità.

La Corte Costituzionale, quindi, nel dichiarare l'illegittimità di tale normativa per violazione del principio di proporzionalità e di tassatività ha lasciato aperta la porta all'emanazione di una nuova normativa che, nel rispetto dei principi sopradescritti, consenta di svolgere un'attività di monitoraggio e di *remote forensics*.

È stato acutamente osservato che questa decisione ha riconosciuto i diritti del "cittadino digitale" [325]: un numero crescente di individui, infatti, non solo utilizza le tecnologie, ma vive "in linea". Internet è diventato un luogo dove le persone incontrano amici, formano società e scambiano informazioni. La Corte ha riconosciuto che la normativa esistente non è sufficiente a tutelare adeguatamente i cittadini "digitali" dalle possibili ingerenze dello Stato.

Per la stessa ragione, non si può escludere che in futuro la Corte estenderà questo concetto anche nella direzione opposta. Attualmente, il *trojan horse* è inteso come uno strumento utilizzato da ufficiali di polizia in carne ed ossa. Ma se, un

[325] W. Abel, B. Schafer, *op. cit.*, p. 826.

domani, la Corte dovesse considerare i *trojan horse* come “agenti di polizia digitali” che abitano il cyberspazio alla stesssa stregua dei “cittadini digitali”?

Conclusioni

L'analisi sulle differenze tra l'Europa e gli Stati Uniti in relazione a due temi di grande attualità, come la tutela dei diritti fondamentali dell'uomo e la lotta alla criminalità attraverso metodologie di indagine informatica, richiede sicuramente ulteriori approfondimenti ed un adeguato dibattito critico, ma è comunque possibile trarre tre considerazioni preliminari.

In primo luogo non vi sono, allo stato attuale dell'elaborazione giuridica, né vinti né vincitori sulle due sponde dell'Atlantico: se è criticabile la scelta dell'Europa di aver creato una normativa sulla *data retention* senza aver chiaramente precisato per quali tipologie di reato tali dati dovessero essere forniti, è altrettanto criticabile lo scandalo scoppiato durante l'amministrazione Bush a seguito dell'accordo segreto della *National Security Agency* con i principali gestori di telefonia statunitensi. Tale accordo era finalizzato a creare un *database* di tutte le telefonate e le attività *on line* compiute dai cittadini americani e, con tutte le ovvie attenuanti che si riassumono nella data dell'11 settembre, legittimava un atto dello Stato contrario a tutti i principi etici e costituzionali degli Stati Uniti.

In secondo luogo le affermazioni contenute nel documento programmatico redatto a Washington il 28 ottobre 2009[326] tra Europa e Stati Uniti, come quelle contenute nel programma di Stoccolma del 2 dicembre 2009[327] o quelle presenti nelle Linee Guida per la cooperazione tra le Forze dell'Ordine e gli Internet

[326] Documento congiunto Europa-Stati Uniti dal titolo "Migliorare la cooperazione transoceanica nell'area della giustizia, libertà e sicurezza" adottato a Washington il 28 ottobre 2009 dal quale si legge "Abbiamo significativi punti di contatti e un profondo e radicato impegno nella protezione dei dati personali, sebbene vi siano delle differenze nei nostri approcci" e poco dopo si legge "è nostra intenzione promuovere la modifica e l'implementazione della Convenzione sul Cybercrime del 2001". Per una versione integrale del documento si veda: http://www.se2009.eu/polopoly_fs/1.21271!menu/standard/file/EU-US%20Joint%20Statement%2028%20October%202009.pdf.

[327] Consiglio d'Europa, "Programma di Stoccolma. Un'aperta e sicura Europa in grado di proteggere i suoi cittadini" del 2 dicembre 2009. Una versione integrale del documento è disponibile al seguente URL: http://register.consilium.europa.eu/pdf/en/09/st14/st14449.en09.pdf.

Service Provider, redatte dal Consiglio di Europa il 2 aprile 2008[328], devono rappresentare un importante stimolo per l'effettiva implementazione della convenzione Cybercrime. Questo strumento, alla luce dell'esperienza acquisita dal 2001 ad oggi, dovrà essere utilizzato per trovare un punto di incontro tra la regolamentazione europea e quella statunitense.

Al riguardo un'attenzione tutta particolare merita la sentenza della Corte Costituzionale tedesca, cui si è dedicato il paragrafo conclusivo di questa trattazione. La sentenza, infatti, traccia, con un tentativo non infruttuoso, delle ipotesi di lavoro su entrambi i fronti (rispetto del diritto di difesa e dei diritti fondamentali da un lato e tutela della sicurezza dei cittadini dall'altro) anche nel medio e lungo termine.

Tuttavia il salto di qualità è racchiuso, a mio avviso, nel commento di Schafer alla pronuncia della Consulta tedesca, dove si ipotizza un futuro possibile in cui gli stessi protagonisti informatici, i programmi, potranno essere guardati come portatori di diritti e di doveri, garantiti in alcune libertà e controllati nel rispetto della norma. È come se il diritto cominciasse, con questo tipo di riflessioni, ad andare, come Alice, "oltre lo specchio" – o "oltre il monitor", assumendo un punto di vista "globalmente informatico", facendo muovere i principi giuridici ed etici in Rete, con la stessa complessità e la stessa visione aggregata d'insieme con cui gli internauti percepiscono se stessi e le regole che li riguardano.

Certo, per seguire questa linea di pensiero è indispensabile un salto di qualità della cultura giuridica. Occorre sviluppare il diritto della Rete con la *forma mentis* di chi trova in essa il suo principale meccanismo di lavoro, di svago, di documentazione, di comunicazione e di pensiero. Non basterà più che la Polizia

[328] Council of Europe, *Guidelines for the cooperation between law enforcement and internet service provider*, disponibile al seguente URL: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf. Si consideri, inoltre, l'interessante Risoluzione del Parlamento Europeo dell'11 novembre 2010 dal titolo: "Un approccio globale al transferimento dei dati dei passeggeri (PNR) a Paesi terzi e sulla Raccomandazione del Commissione Europea al Consiglio Europeo per l'apertura di una negoziazione tra l'Europa, il Canada, l'Australia e gli Stati Uniti", disponibile al seguente URL: http://www.statewatch.org/news/2011/feb/ep-resolution-eu-usa-nov-10.pdf.

Giudiziaria sia in grado di intendere il linguaggio informatico: serviranno Forze dell'Ordine delocalizzati, internazionali e veloci come i loro utenti. In questa ottica, anche gli informatici debbono, umilmente, familiarizzare con il diritto e i codici (specialmente quello di procedura penale), attuando, nei fatti, un sistema interculturale.

La terza e ultima considerazione è un auspicio, coerente con l'elaborazione svolta sin qui: le enormi potenzialità di Internet non possono soltanto essere utilizzate per incontrare i vecchi amici del liceo o per videotelefonare gratuitamente ai propri cari. Proprio la capacità della Rete di interconnettere le persone di ogni estrazione culturale, geografica e sociale, deve essere il punto di partenza per la creazione di un sistema di regole globali, che garantiscano il diritto di ogni cittadino di difendersi e di essere difeso, senza che i particolarismi nazionali possano essere di ostacolo a tale percorso.

Negli ultimi anni, la Rete ci ha offerto l'opportunità di leggere, sentire e vedere la voce di popoli soggetti a regimi autoritari e quella dei movimenti di piazza, dei sindacati e dei gruppi di pressione. Oggi, è necessario che emerga anche la voce dei giuristi e quella degli informatici i quali, avvalendosi dell'enorme concentrazione di pensiero molteplice che la Rete è in grado di attivare, possano promuovere regole non necessariamente "nuove", ma che "vadano bene a tutti", ossia in grado di superare i confini nazionali e compatibili con lo sviluppo tecnologico.

Senza Internet siamo riusciti a stilare la Dichiarazione universale dei diritti umani. Cosa potremmo fare con Internet ?

Bibliografia

Dottrina Italiana

E. Aprile e F. Spiezia, *Le intercettazioni telefoniche ed ambientali. Innovazioni tecnologiche e nuove questioni giuridiche*, 2004, Milano, Giuffrè.

S. Aterno, *La* computer forensics *tra teoria e prassi*, in *Ciberspazio e diritto*, 2006, fasc. 4, p. 427.

S. Aterno, P. Mazzotta, *La perizia e la consulenza tecnica*, 2008, Padova, Cedam.

S. Battiato, G. Messina, S. Rizzo, *Image Forensics. Contraffazione Digitale e Identificazione della Camera di Acquisizione: Status e Prospettive*, 2009, in IISFA Memberbook, Forlì, Experta.

Fabio Bravo, *Indagini informatiche e acquisizione della prova nel processo penale*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, Vol III, N. 3 e Vol. IV – N. 1, Settembre 2009–Aprile 2010, disponibile al seguente URL http://www.vittimologia.it/rivista/articolo_bravo_2009-03_2010-01.pdf .

C. Brusco, *La valutazione della prova scientifica*, in *La prova scientifica nel processo penale*, a cura di L. De Cataldo Neuburger, 2007, Padova, Cedam.

O. Busi, *I Rilievi e gli Accertamenti tecnici nell'attività della polizia Giudiziaria e nell'esercizio delle investigazioni difensive*, in Atti del Convegno di Polizia Locale del 14 settembre 2005, in *Lex Ambiente*, http://www.lexambiente.it/acrobat/Busi.pdf.

V. Calabrò, G. Costabile, S. Fratepietro, M. Ianulardo, G. Nicosia, *L'alibi informatico. Aspetti tecnici e giuridici*, in *IISFA Memberbook 2010*, Forlì, Experta.

M. Cammarata, *Sequestri: se la polizia viola il domicilio informatico*, 22 aprile 2005, in *Interlex*, http://www.interlex.it/regole/tribvebz.htm.

A. Camon, *Le intercettazioni nel processo penale*, 1996, Milano, Giuffrè.

G. Canzio, *Prova scientifica, ragionamento probatorio e libero convincimento del giudice penale*, in *Dir. Pen. Proc.*, 2003, p. 1193.

L. Cuomo, F. Scioli, *L'incidente probatorio*, 2007, Torino, Giappichelli.

V. S. Destito, G. Dezzani, C. Santoriello, *Il diritto penale delle nuove tecnologie*, 2007, Cedam, Padova.

F. Cajani, *La Convenzione di Budapest nell'insostenibile salto all'indietro del Legislatore italiano, ovvero: quello che le norme non dicono…*, in *Ciberspazio e Diritto*, 2010, p. 185.

F. Cajani, *Alla ricerca del log (perduto)*, in *Rivista di Diritto dell'Internet*, 2006, p. 572.

F. Catullo, *Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova finale digitale – Profili sostanziali*, in *Diritto dell'Internet*, 2006, p. 160.

L. Chirizzi, *Computer Forensic. Il reperimento della fonte di prova informatica*, 2006, Roma, Laurus Robuffo.

E. Colombo, *La sentenza del caso di Garlasco e la* computer forensics, in *Ciberspazio e Diritto*, 2010, p. 454.

G. Costabile, Scena criminis*, documento informatico e formazione della prova penale*, in *Penale.it*, disponibile al seguente URL: http://www.penale.it/page.asp?mode=1&IDPag=72.

G. Costabile, Computer Forensics *e informatica investigativa alla luce della Legge n. 48 del 2008*, in *Ciberspazio e Diritto*, 2010, p. 497.

D. D'Agostini, *Le indagini sulle reti informatiche*, in *Diritto penale dell'informatica*, 2007, Experta Edizioni, Forlì.

A. Dondi, *Paradigmi processuali e* "expert witness testimony" *nell'ordinamento statunitense*, in *Riv. trim. dir. e proc. civ.*, 1996, p. 261.

L. Filippi, *L'intercettazione di comunicazioni*, 1997, Milano, Giuffrè.

R. Flor, *Brevi Riflessioni a margine della sentenza del* bundesverfassungsgericht *del 27 febbraio 2008, sulla c.d.* Online Durchsuchung. *La prospettiva delle investigazioni ad alto contenuto tecnologico ed il bilanciamento con i diritti inviolabili della persona. Aspetti di diritto penale sostanziale*, in *Riv. trim. dir. pen. ec.*, 3, 2009, p. 695.

R. Flor, *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del* Bundesverfassungsgericht *del 27 febbraio 2008, sulla Online Durchsuchung e la sua portata alla luce della sentenza del 2 marzo 2010 sul* data retention, in *Ciberspazio e diritto*, Vol. 11, n. 2, 2010, p. 368.

A. Ghilardini, G. Faggioli, *Computer Forensics*, 2008, Milano, Apogeo.

A. Ghilardini, *Intercettazioni Telematiche: Case Study su Skype*, intervento al Convegno IISFA Forum 2008, tenutosi a Bologna il 18 Aprile 2008, disponibile al seguente URL: http://www.iisfa.it/forum2008/IISFA_Forum_2008_Andrea_Ghirardini. pdf.

F. Giunchedi, *Gli accertamenti tecnici irripetibili*, 2009, Torino, Utet.

C. Giustozzi, Hash *sempre più vulnerabili*, 7 marzo 2005, in *Nightgaunt*, disponibile al seguente URL: http://www.nightgaunt.org/testi/interlex/sha1.htm.

J. F. Korose e K. W. Ross, *La sicurezza nelle reti,* in *Reti di calcolatori e Internet,* 2005, Pearson Addison Wesley, Milano.

F. Licata, *La Convenzione del Consiglio d'Europa sul cybercrime e le forme della cooperazione giudiziaria: una risposta globale alle nuove sfide della criminalità transnazionali*, in *Atti dell'incontro di Studio del Consiglio Superiore della Magistratura tenutosi a Roma il 19 settembre 2005*, p. 17, disponibile al seguente URL: http://appinter.csm.it/incontri/relaz/12009.pdf.

L. Lupária, *Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova finale digitale – Profili processuali*, in *Diritto dell'Internet*, 2006, p. 153.

L. Lupária - G. Ziccardi, *Investigazione penale e tecnologia informatica,* 2007, Giuffrè, Milano.

C. Maioli, *Introduzione all'informatica forense*, in *La sicurezza preventiva dell'informazione e della comunicazione*, a cura di P. Pozzi, 2004, Torino, Franco Angeli.

C. Maioli e R.Cugnasco, *Profili normativi e tecnici delle intercettazioni. Dai sistemi analogici al* voice over IP, 2008, Milano, Gedit.

A. Manchìa Chelo, *Acquisizione di corrispondenza o "intercettazione epistolare"?*, in *Dir. Pen. Proc.*, 2007, 8, p. 1049.

A. Manna, F. Resta, *I delitti in tema di pedopornografia, alla luce della legge 38/2006. Una tutela virtuale?*, in *Diritto dell'Internet*, 2006, p. 223.

M. Mattiucci, G. Delfini, Forensic Computing, in *Rassegna dell'Arma dei Carabinieri*, 2, 2006, p. 52.

S. McClure, J. Scambray, G. Kurtz, *Hacker 6.0*, 2009, Milano, Apogeo.

A. Monti, *Sequestri di computer. Dal Tribunale di Torino un provvedimento controtendenza*, 15 aprile 2000, disponibile al seguente URL: http://www.ictlex.net/?p=626 .

V. Musacchio, *La nuova normativa penale in materia di sfruttamento sessuale dei bambini e pedopornografia a mezzo internet*, in *Riv. pen.*, 2006, p. 399.

C. Parodi, *La disciplina delle intercettazioni telematiche*, in *Dir. pen. e proc.*, 2003, p. 889.

L. Pistorelli, *Colmate le lacune della pregressa disciplina*, in *Guida al diritto*, 2006, n. 9, p. 45.

S. McClure, J. Scambray, G. Kurtz, *Hacker 6.0*, Apogeo, 2009, p. 165.

D. Siracusano, A. Galati, G. Tranchina, E. Zappalà, *Diritto processuale penale*, Milano, Giuffrè, 1996.

F. Tagliaro, E. D'aloja, F.P. Smith, *L'ammissibilità della prova scientifica in giudizio e il superamento del Frye standard: note sugli orientamenti negli USA*

successivi al caso Daubert v. Merrel Dow Farmaceuticals, Inc., in *Riv. it. med. leg.*, 2000, 719.

M. Taruffo, *Le prove scientifiche nella recente esperienza statunitense*, in *Riv. trim. dir. proc. civ.*, 1996, p. 219.

F. Testa, *Cybercrime, intercettazioni telematiche e cooperazione giudiziaria in materia di attacchi ai sistemi informatici*, Incontro di Studio sul tema "Criminalità organizzata transnazionale: strumenti di contrasto e forme di cooperazione giudiziaria", 6-8 giugno 2005, Roma, disponibile al seguente URL: http://appinter.csm.it/incontri/relaz/11794.pdf.

P. Tonini, *Manuale di procedura penale*, 2004, Milano, Giuffrè.

Dottrina straniera

L. Adams, *The law of privacy*, North American, 1902.

J. Bamford, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*, Anchor Books, 2009.

J. Blau, *Debate rages over German government spyware plan*, 5 maggio 2007, in *Computerworld Security*, disponibile al seguente URL: http://www.computerworld.com/s/article/print/9034459/Debate_rages_over_German_government_spyware_plan?taxonomyName=Security&taxonomyId=17.

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

P. Breyer, *Telecommunications Data Retention and Human Rihgt: The compatibility of Blanket Traffic Data Retention with the ECHR*, in *European Law Journal*, 2005, p. 365.

M. Burmester, J. Mulholland, *The Advent of Trusted Computing: Implications for Digital Forensics*, disponibile al seguente indirizzo: http://www.cs.fsu.edu/~burmeste/tc.pdf.

M. Carney, M. Rogers, *The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction*, in *International Journal of Digital Investigation,* 2004, p. 39.

B.D. Carrier, E.H. Spafford, *Categories of digital investigation analysis techniques based on the computer history model*, in *Digital Investigation*, 3, 2006, p. 121.

E. Casey, *Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence*, in *International Journal of Digital Investigation*, Vol. 1, p. 3.

E. Casey, *Digital Evidence and Computer Crime*, 2004, Second Edition, Elsevier.

E. Casey G. J. Stellatos, *The impact of full disk encryption on digital forensics*, in *Operating Systems Review*, 2008, 42 (3), p. 93.

P.A. Collier, B.J. Spaul, *A Forensic Methodology for Countering Computer Crime*, in 32 *J. For. Sc.*, 1992, p. 27.

Thomas M. Cooley, *A Treatise on the Torts*, Chicago Callaghan & Co., 1888, p. 29.

Thomas P. Crocker, *From Privacy To Liberty: The Fourth Amendment After Lawrence*, 57 UCLA L. Rev. 1.

G. Danezis, R. Dingledine, N. Mathewson, *Mixminion: Design of a Type III Anonymous Remailer Protocol*, in *IEEE Security & Privacy*, 2003, disponibile al seguente URL: http://www.mixminion.net/minion-design.pdf.

L. Dixon, B. Gill, *Changes in the Standards for Admitting Expert Evidence in Federal Civil Cases since the Daubert Decision*, , 2001, RAND Institute for Civil Justice.

R. C. Losey, *Introduction to e-Discovery*, 2009, ABA Publishing.

D.J. Faigman, D.H. Kaye, M.J. Saks, J. Sanders, *Modern Scientific Evidence. The Law and Science of Export Testimony*, 2002, St. Paul.

N. Feigenson, C. Spiesel, *Law on Display. The Digital Transformation of Legal Persuasion and Judgement*, 2009, New York University Press.

K.R. Foster, P.W. Huber, *Judging Science. Scientific Knowledge and the Federal Courts*, 1999, Cambridge, M.I.T. Press.

C. Frichot, *An Analysis and Comparison of Clustered Password Crackers*, 2004, disponibile al seguente http://scissec.scis.ecu.edu.au/proceedings/2004/forensics/Frichot-1.pdf.

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

M. Gercke, *Secret Online Search*, in *Computer und Recht*, 2007, p. 246.

E. Huebner, D. Bema, F. Henskensb, M. Wallisb, *Persistent System Techniques in forensic acquisition of memory,* in *Digital Investigation*, 2007, p. 129.

E. Huebner, S. Zanero, *Open Source Software for Digital Forensics*, Springer New York, 2010.

Saul M. Kassin and Meghan A. Dunn, *Computer-Animated Displays and the Jury: Facilitative and Prejudicial Effects*, in *Law and Human Behaviour*, 1997, Vol 21, no. 3, p. 269.

E. Katz, *The Beginning of the End of Data Retention Commentary*, in *EFF,* 10 marzo 2010, disponibile al seguente URL: http://www.eff.org/deeplinks/2010/03/beginning-end-data-retention.

A. Kelmann e R. Sizer, *The Computer in Court. A Guide to Computer Evidence for Lawyers and Computing Professionals*, 1982, Hampshire, Gower.

K. Kent, S. Chevalier, T. Grance, H. Dang, *Guide to integrating Forensic Techniques into Indente Response*, 2006, NIST publication, http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

O. Kerr, *Searches and Seizures in a digital world*, in *Harward Law Review*, 2005, Vol. 119, p. 531.

V. Klima, *Tunnels in Hash Functions: MD5 Collisions Within a Minute*, ricerca del marzo 2006, disponibile al seguente URL: http://eprint.iacr.org/2006/105.pdf.

F. Insa, *The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime—Results of a European Study*, in *Journal of Digital Forensic Practice*, 2006, p. 285.

F.S. Lane, *American Privacy: The 400-Year History of Our Most Contested Right*, 2009, Boston, Beacon Press.

R. Pound, *Interests of Personality*, in *Harvard Law Review*, 1915, Vol. 28, No. 4, p. 343.

Denis O'Brien, *The Right to Privacy*, in *Columbia Law Review*, 1902, Vol. 2, p. 443.

A. Reyes, K. O'Shea, R. Brittson, J. Steel, *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors*, Elsevier Science, 2007, p. 255.

Ralph C. Losey, *Introduction to e-Discovery*, 2009, ABA Publishing.

S. Mason, *Trusted computing and forensic investigations*, in *Digital Investigation*, Vol. 2, N. 2, p. 189, disponibile al seguente URL: http://www.stephenmason.eu/articles/trusted-computing-and-forensic-investigations/.

S. Mason, *Electronic Evidence. Discovery & Admissibility*, 2007, London, LexisNexis Butterwoorths.

G.B. Moore, *Federal Rule of Civil Procedure 26(b)(2)(B) and "Reasonable Accessibility": The Federal Courts' Experience in the Rule's First Year*, in *Privacy & Data Security Law Journal*, disponibile al seguente URL: http://www.bmpllp.com/*file*/1202334716.pdf.

W. Abel, B. Schafer, *La decisione della Corte Costituzionale tedesca sul diritto alla riservatezza ed integrità dei sistemi tecnologici d'informazione – un rapporto sul caso BVerfGE*, in *Jei – Jus e Internet. Approfondimenti giuridici*, 2009, disponibile al seguente URL: http://www.jei.it/approfondimentigiuridici/notizia.php?ID_articoli=601.

M. Scheetz, *Computer Forensics: an essential guide for accountants, lawyers, and managers*, 2007, John Wiley & Sons.

J. Siegfried, C. Siedsma, B. Countryman, C. Hosmer, *Examining the Encryption Threat*, in *International Journal of Digital Evidence*, Vol. 2, 3, disponibile al seguente URL: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf.

R. Stern, *Mousetrapping and Pagejacking: Introduction*, in *Computer Law*, disponibile al seguente URL: http://docs.law.gwu.edu/facweb/claw/mousetrap1.htm.

A. Swaminathan, K. J. Ray Liu, *Digital Image Forensics via Intrinsic Fingerprints*, in *IEEE Transactions on Information Forensics and Security*, 2008, disponibile al seguente URL: http://www.cspl.umd.edu/sig/publications/Swaminathan_TIFS_200803.pdf.

L. Warren, S. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 1890, Vol. 4, N. 5.

S.D. Williger, R.M. Wilson, *Negotiating the Minefields of Electronic Discovery*, in *Richmond Journal of Law and Technology*, 2004, Vol. X, Issue 5, disponibile al seguente URL: http://jolt.richmond.edu/v10i5/article52.pdf.

C. Westphal, *Data Mining for Intelligence, Fraud & Criminal Detection: Advanced Analytics & Information Sharing Technologies*, CRC, 2008, Press, p. 3.

J. Whitman, *The two western cultures of privacy: Dignity vs Liberty*, in *The Yale Law Journal*, 2004, vol. 113, n 6, p. 1151.

C. Woo, M. So, *The Case For Magic Lantern: September 11 Highlights The Need For Increased Surveillance*, in *Harvard Journal of Law & Technology*, 2002, disponibile al seguente URL: http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf.

M. Zander, *The Police and Criminal Evidence Act 1984*, Sweet & Maxwell Ltd, 2010, p. 4.

K. Zatiko, *Commentary: Defining digital forensics*, in *Forensics Magazine*, 2007, disponibile al seguente URL: http://www.forensicmag.com/node/128.182.

Jonathan Zittrain, *Beware the Cyber Cops*, in *Forbes,* 7 luglio 2002, disponibile al seguente URL: http://www.forbes.com/forbes/2002/0708/062.html.

Giurisprudenza Italiana

Cassazione Penale, 23 ottobre 1992, in *Cassazione Penale*, 1994, p. 676.
Cassazione Penale, 29 ottobre 1993, in *Cassazione Penale*, 1995, p. 134.
Cassazione Penale, Sezione III, 12 maggio 1994, n. 5630.
Cassazione Penale, Sez. III, 26 gennaio 2000, n. 384.
Cassazione Penale, Sez. II, 23 maggio 2006, n. 20228.
Cassazione Penale, Sez. VI, 31 maggio 2007, n. 40380.
Cassazione Penale, Sez. V, del 6 luglio 2007, n. 31135.
Cassazione Penale, Sez. III, 18 novembre 2008, n. 12107.
Cassazione Penale, Sez. V, 14 ottobre 2009, n. 16556.
Cassazione penale, Sez. I, 5 marzo 2009, n. 14511.
Cassazione penale, Sez. I, 26 febbraio 2009, n. 11863.
Cassazione Penale, Sez. III, 9 giugno 2009, n. 28524.
Tribunale di Brescia, 22 aprile 2004
Tribunale di Brescia, 4 ottobre 2006.
Tribunale Milano, 30 ottobre 2002, in *Foro ambrosiano*, 2003, p. 55.
Tribunale di Torino, 7 febbraio 2000.
Tribunale di Venezia, 31 marzo 2005.

Giurisprudenza straniera

Ameriwood Industries, Inc. v. Lieberman et al., 2007 U.S. Dist. LEXIS 93380 (E.D. Mo. Dec. 27, 2006).
Arizona v. Gant, 129 S. Cr. 1710 (2009).

Bundesverfassungsgerichts del 15 dicembre 1983, BVerfGE, 65, 1, <43>; 84, 192

Brigha City v. Stuart, 547 U.S. 103, 117, 2006.

Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579.

Crispin v. Christian Audigier, 2010 U.S. Dist. LEXIS 52832 (C.D. Cal. May 26, 2010)

Frye v. United States, 293 F. 1013 (D.C. Cir. 1923)

Kevin Keithley v. The Home Store.com, August 12 2008, U.S. Dist. LEXIS 61741

Hedenburg v. Aramark American Food Services, 2007 US Dist. LEXIS 3443 (WD Wash. Jan. 17, 2007).

Horton v. California, 496 U.S. 128, 136 (1990.)

In re Grand Jury Investigation Concerning Solid State Devices, Inc., 130 F.3d 853, 957 (9th Cir. 1997).

Leander v. Sweden, (Corte Europea dei Diritti dell'Uomo del 26 marzo 1987, 9 EHRR 433, para. 59)

Trulock v. Freeh, 275 E.3d, 391, 398, 403-404 (4th Cir. 2001)

United States v. Miller, 425 U.S. 435, 443 (1976).

United States v. Harvey, 540 F.2d 1345, 1350-52 (8th Cir. 1976)

United States v. Matlock, 415 U.S. 164 Œ1974).

United States v. Mancini, 8 F.3d 104, 109 (1st Cir. 1997).

United States v. Knights, 534 U.S. 112, 122 (2001).

United States v. Brooks, 427 F.3d 1246, 1252 (10th Cir. 2005)

United States v. Fleet Management Ltd., 521 F. Supp. 2d 436, 443-444 (E.D. Pa. 2007)

United States v. Andrus, 483, F.3d 711, 720-21 (10th Cir. 2007).

United States v. Grubbs, 547 U.S. 90, 98-99 (2006).

United States v. Boucher, 2007 WL 4246473.