CONSIGLIO SUPERIORE DELLA MAGISTRATURA

Incontro di studi sul tema: "Scienze e processo penale"
Roma, 27-29 giugno 2011

Informatica e studio delle nuove tecnologie

Francesco CAJANI

Sostituto Procuratore della Repubblica presso il Tribunale di Milano – pool reati informatici

Membro del comitato tecnico-scientifico di IISFA – Italian Chapter

francesco.cajani@giustizia.it

Gerardo COSTABILE

Presidente di IISFA – Italian Chapter

gerardo@costabile.net

Mattia EPIFANI

Digital Forensics Specialist

Responsabile Formazione IISFA - Italian Chapter

mattia.epifani@realitynet.it

Per questa prima occasione di collaborazione tecnico/scientifica tra CSM e IISFA, verrà presentato un caso di scuola molto ricorrente (ritrovamento di un portatile e di un cellulare sulla *scena criminis* e metodologie ipotetiche di acquisizione ad opera della PG): esso riporterà tutti al più noto "caso Garlasco" e consentirà anche di affrontare, nei gruppi di lavoro, i temi più giuridici della ripetibilità/irripetibilità[1] delle operazioni di *computer forensics* nonché dell'eventuale trattamento sanzionatorio in caso di maldestra acquisizione della *digital evidence* durante le indagini[2].

INDICE DEI MATERIALI:

1. presentazione di IISFA: *International Information Systems Forensics Association – Italian Chapter*

2. IISFA Survey 2010 - Lo stato dell'arte della *computer forensics* in Italia (documento scaricabile da **http://www.iisfa.it/IISFA_SURVEY_2010.PDF**)

   Una nuova Survey è stata aperta su *http://surveyiisfa.questionpro.com*

   (tempo necessario per le risposte: tra i 5 e i 7 minuti)

3. G. COSTABILE, *Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008,* in *Ciberspazio e diritto*, 3, 2010

4. M. EPIFANI, *Analisi di telefoni cellulari in ambito giuridico*, in *Ciberspazio e diritto*, 1, 2009

5. Estratto da Tribunale di Vigevano, sentenza 17 dicembre 2009 (est. Vitelli)

[1] Cfr. Cass., Sez. I, 16 marzo 2009, n. 11503, in *CED 243495*; Cass. Sez. I, 18 marzo 2009, n. 11863, in *CED 243922*; Cass., Sez. I, 2 aprile 2009, n. 14511, in *CED 243150*. In senso critico cfr. A. E. RICCI, Digital evidence *e irripetibilità delle operazioni acquisitive*, in *Dir. pen. proc.*, 2010, 3, pp. 343 e ss.

[2] Cfr. E. VITALE, *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico*, in *Dir. Internet*, 2008, 5, p. 509; G. BRAGHO', *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in AA.VV. (a cura di L. LUPARIA), *Sistema penale e criminalità informatica*, Milano, 2009, pp. 190-191; C. CONTI, *Il volto attuale dell'inutilizzabilità: derive sostanzialistiche e bussola della legalità*, in *Dir. pen. proc.*, 2010, 7, p. 790.

International Information Systems Forensics Association

Italian Chapter

(www.iisfa.net - www.iisfa.org)

E' l'organizzazione internazionale dei tecnici e giuristi impegnati nella promozione scientifica dell'informatica forense attraverso la divulgazione, l'apprendimento e la certificazione riconosciuta in ambito internazionale. Le attività ruotano intorno a un codice etico e alla partecipazione a un network mondiale di professionisti. IISFA realizza un programma formativo di eccellenza basato su seminari periodici con specifiche sessioni di laboratorio, corsi di alta formazione in Computer Forensics, forum, newsGroup, pubblicazioni/Quaderni, laboratori scientifici.

Lo scopo primario dell'IISFA è promuovere lo studio, la formulazione di metodi e di standard inerenti le attività di Information Forensics, l'istruzione dei suoi membri e di sviluppare e rafforzare le loro capacità professionali in relazione alle attività di Information Forensics.

In modo più specifico gli obiettivi dell'associazione sono:

a) Favorire le iniziative che possano contribuire allo sviluppo ed all'aumento del livello formativo dei suoi membri nei campi correlati di Information Forensic e cybercrime investigations, costituendo un luogo di libero scambio delle esperienze e di informazioni anche mediante l istituzione di corsi, seminari, convegni, redazione, traduzione e diffusione di pubblicazioni, nonché collaborazioni con le Università;

b) Proporre raccomandazioni in materia di Information Forensics ed intraprendere iniziative nei confronti di aziende ed autorità competenti, con lo scopo di coordinare sul piano nazionale ed internazionale, l'evoluzione delle tecniche e dei metodi di Information Forensics;

c) cooperare con altre Associazioni o Fondazioni che abbiano per oggetto attività analoga o affine a quella del Associazione;

d) favorire il riconoscimento in Italia della qualificazione professionale di CIFI (Certified International Information Systems Forensics Investigator) promossa dall'IISFA e di tutte le altre certificazioni che l'associazione internazionale IISFA intenderà promuovere;

e) rappresentare l'IISFA nel rispetto delle regole di appartenenza a tale Associazione.

Information Systems Forensics Association

Italian Chapter

Comunicato stampa

IISFA SURVEY 2010

Lo stato dell'arte della computer forensics in Italia

In occasione dell'annuale IISFA FORUM, tenutosi quest'anno a Milano presso i locali della Società Umanitaria, sono stati presentati i risultati di una indagine svolta presso la "comunità" dei soggetti coinvolti nelle attività di computer forensics.

La rielaborazione e lo studio dei dati raccolti è contenuta in un agile volumetto di circa 50 pagine, denso di tabelle e grafici, opportunamente commentati.

L'indagine è disponibile, in formato elettronico, a questo indirizzo web:

http://www.iisfa.it/IISFA_SURVEY_2010.PDF

La survey è stata svolta per mezzo di un questionario strutturato, distinto per categorie e articolato per aree omogenee, con una sola area comune. Le domande prevedevano una sola risposta, salvo in alcuni casi la possibilità di fornire risposte libere o anche più di una risposta.

I dati raccolti sono stati trattati in modo automatizzato, tramite applicazione software.

Le categorie individuate ed oggetto di analisi sono state le seguenti:

- Consulente di azienda che fa consulenze
- Azienda che commissiona consulenze
- Pubblico ministero
- Avvocato
- Investigatore ordinario
- Investigatore che fa computer forensics
- Giudice

per un totale di 178 persone.

Per esigenze di elaborazione, le categorie suddette sono state "compresse" per individuare quattro categorie omogenee ovvero:

- Consulente e investigatore che fa computer forensics
- Azienda che commissiona consulenze
- Giudice, Pubblico Ministero e investigatori classici
- Avvocato

Gerardo Costabile, Presidente IISFA, presentando l'indagine a Milano, ha sottolineato in apertura l'importanza dei dati emersi dalla sezione comune a tutti gli intervistati, cioè quella relativa a commenti sulla legge 48 del 2008 che introduce in Italia la Convenzione di Budapest.

La quasi totalità degli intervistati (il 77%) ha rimarcato l'importanza delle innovazioni introdotte nel codice di procedura penale dalla legge 48/2008. Unanime consenso (95%) tra gli intervistati ha riscosso la necessità di disporre di linee guida per l'informatica forense: tuttavia il campione si è "spaccato" a metà tra chi propende per una codificazione normativa tradizionale con preferenza per la codificazione internazionale, e chi invece ha espresso preferenza per una codificazione non avente valore e forza di legge, ma carattere puramente di best practice.

Consulenti e investigatori sono per lo più dipendenti e la motivazione che spinge alla computer forensics è la passione (il 47% del campione): sono pochi (appena il 30%) quelli che la svolgono come unica attività e comunque non è fonte di incremento guadagni.

Questo dato trova riscontro in quanto rilevato presso gli avvocati per cui la maggior parte delle attività di computer forensics viene effettuata/richiesta come lavoro occasionale (35%) o per hobby (25%).

Il peso consistente della motivazione di svolgimento dell'attività "per passione", senza carattere di incremento del guadagno è rivelatore del fatto che la materia non ha maturità tale da spingere il consulente a staccarsi dall'hobbystica e a vivere come un professionista del settore.

Il dato "per passione" collegato con il dato "dipendente" a sua volta rivela che la computer forensics non è "core" dell'attività come dipendente e questo incide anche sull'esperienza che varia da 3 a 8 anni. Inoltre si registra una "forbice" per cui il 30% del campione ha un numero di casi per anno superiore a 15, mentre un altro 30% oscilla tra tra 1 e 3 casi annui: in mezzo il 20% ed il 14% che oscillano tra 3 e 15 casi all'anno di media.

Il consulente tipo (il 52%) lavora per lo più (in misura superiore al 50% dei casi) per clienti istituzionali e nel settore penale. Le consulenze di computer forensics riguardano nella maggior parte dei casi il computer come mero contenitore e la tipologia di reato più seguita è il p2P e la pedopornografia. In materia di illecito civile l'infedeltà aziendale ha costituito materia maggiore per consulenza di computer forensics.

Il dato "anzianità" in materia di computer forensics ha mostrato un notevole divario tra l'esperienza maturata da consulenti/investigatori tecnici da un lato e avvocati e pm/giudici/investigatori classici dall'altro: mentre questi ultimi hanno registrato esperienza di oltre otto anni (il 70% degli intervistati), i consulenti/investigatori tecnici appaiono più "acerbi" con esperienza variabile tra tre e otto anni (il 28%). Tuttavia la minore esperienza non appare avere connotazione negativa visto che a fronte di essa si registrano oltre quindici pratiche all'anno (nel 28% dei casi).

Il divario di esperienza professionale tra tecnici di computer forensics e operatori giuridici non dovrebbe avere connotazione negativa, in quanto il dato del numero di CF svolte/delegate in un anno mostra che mentre solo il 6% degli avvocati ed il 10% di PM/giudici/investigatori classici registra oltre 15 pratiche

all'anno a fronte del 28% dei consulenti/investigatori di CF. L'anzianità professionale e quella derivante dalla pratica di CF dunque non coincidono.

Nonostante la prevalenza della "passione" come spinta motivazionale per l'esercizio dell'attività di computer forensics e la minore anzianità professionale, la categoria "consulenti/investigatori di computer forensics" registra in proporzione lo stesso carico di pratiche delle altre due categorie a maggior anzianità professionale.

I guadagni costituiscono un punto dolente emerso dalla indagine.

L'importo medio dell'incarico di consulenza ricevuto da clienti istituzionali (magistratura e forze di polizia) varia da € 500 a € 1.500 nel 41% dei casi, mentre nel caso di clienti privati varia da € 1.000 a € 3.000 nel 27% dei casi. Sono percentuali che rappresentano picchi massimi e già da sole delineano la profonda diversità del settore istituzionale rispetto a quello privato che si riscontra anche nei tempi medi di pagamento: da parte di clienti istituzionali (magistratura e forze di polizia) sono oltre 150 gg. nel 60% dei casi mentre per quanto riguarda invece i clienti privati sono entro 30 gg. nel 41% dei casi, al più tardi entro 60 gg. Solo sporadicamente il pagamento si ha oltre 150 gg. (3% dei casi).

I privati pagano meglio e sono più esigenti e richiedono professionisti che si possono dedicare a tempo pieno.

La preferenza accordata al cliente istituzionale, nonostante l'enorme divario rispetto al cliente privato in termini di entità del corrispettivo e di tempi di pagamento, si spiega con la considerazione che il cliente istituzionale, in relazione alla quantità e qualità delle casistiche nonché alla qualificata esperienza, offre enormi possibilità di "vetrina" e quindi di arricchimento del curriculum.

Altro dato interessante emerso dall'indagine è quello relativo all'uso della tecnologia e agli investimenti: l'effettuazione di consulenze per passione comporta minori investimenti in materiale software di tipo commerciale (nel 56% dei casi si usa una combinazione software open e commerciale) e maggior ricerca di collaborazioni con colleghi esperti (nel 55% dei casi), sulla base di richieste formali e con divisione del compenso.

Altri temi affrontati dalla indagine riguardano la formazione e la certificazione, l'appartenenza ad associazioni (solo il 50-60% dei partecipanti alla survey è socio IISFA), la conservazione dei reperti, dettagli tecnici su hw e sw, camera bianca, etica.

In particolare per la formazione si evidenzia che nel 77% dei casi, la categoria dei consulenti/investigatori che fanno computer forensics ritiene utile una formazione professionale svolta in Italia secondo i percorsi indicati dalle associazioni o affiancando persone esperte, anche sul campo Solo nel 15% dei casi la formazione è utile se svolta negli USA presso le strutture operative in tal senso. Il 5% raggruppa coloro che effettuano la formazione studiando in autonomia,utilizzando riviste di settore, ricorrendo a forum, ai libri e in generale alle informazioni acquisibili in Rete.

Il 41% degli avvocati non sostiene costi per la formazione in quanto segue corsi gratuiti mentre un altro 40% sostiene spese per € 2.000 e oltre all'anno.

Volendo sintetizzare gli esiti della Survey, si possono usare i termini “incerto” e “contraddittorio”. Incertezza e contraddittorietà derivano dalla necessità di una formazione continua e certificata da un lato, e dalla certezza del diritto dall’altro, come suggeriscono gli investimenti nella formazione fatti dai consulenti e la richiesta di “cogenza normativa” delle linee guida formulata da metà del campione esaminato.

Queste esigenze possono costituire la base per una pratica matura della computer forensics, non legata a semplice ancorché encomiabile passione, ma saldamente ancorata a criteri professionali, con prevedibili ricadute su una equa periodizzazione e quantificazione dei compensi per l’attività svolta.

Ciberspazio e diritto 2010, Vol. 11, n. 3, pp. 465-508

Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008

Gerardo Costabile [1]

1. Definizioni e rischi

La *computer forensics* [2] è un processo teso alla "manipolazione controllata" e più in generale al trattamento [3] di dati e/o informazioni digitali e/o sistemi informativi per finalità investigative e di giustizia [4], adottando procedure tecnico-organizzative tese a fornire adeguate garanzie in termini di integrità, "autenticità" e disponibilità delle informazioni e dei dati in parola. Tale disciplina, secondo alcuni una scienza chiamata anche informatica forense, non può limitare il proprio raggio d'azione alle sole indagini relative ai c.d. reati informatici.

Prima di tutto, si desidera evidenziare come vi sia differenza tra "Informatica Forense" e "Sicurezza Informatica", seppure queste due aree di attività siano strettamente collegate. Si può pensare alla Sicurezza Informatica da un lato come elemento di ostacolo e dall'altro come fonte di strumenti e opportunità per l'Informatica Forense. Infatti la Sicurezza Informatica ha come proposito finale l'avvicinarsi alla realizzazione di sistemi il più possibile sicuri, ma qualora tale grado di sicurezza venisse elevato (ad esempio da parte del responsabile di un illecito [5]), allora per de-

[1] Presidente IISFA Italian Chapter (www.iisfa.it). CIFI, ACE, CGEIT

[2] Nell'accezione più ampia rispetto ai soli *personal computer*, si dovrebbe utilizzare la meno nota *information forensics* o *digital forensics*.

[3] Veggasi "trattamento" *ex* art 4 del D.lgs 196/03, solo per motivi di completezza della definizione, in quanto non sempre, nelle attività di informatica forense, si "trattano" dati personali, sensibili o giudiziari.

[4] Per una analisi delle varie definizioni, si rimanda a G. Ziccardi in L. Lupària, G. Ziccardi, *Investigazione penale e tecnologia informatica*, Giuffrè, Milano, 2007.

[5] In tal caso si può parlare anche di "antiforensics". L'antiforensics è, comunque, una tecnica tesa all'occultazione o falsificazione dei dati da parte dell'indagato (prima ovviamente della perquisizione), com lo scopo di "distrarre" o indurre in errore gli investigatori. Per un maggior dettaglio si rimanda D. Gabrini aka Rebus, http://informaticagiuri-

finizione dal sistema sarebbe più complicato estrarre il desiderato contenuto informativo. L'acquisizione dei reperti informatici richiederà, in tal caso, la "violazione" del sistema oggetto dell'analisi, ed in questo campo la stessa Sicurezza Informatica sarà d'aiuto, in quanto fonte di studi sulle tecniche di *hacking* (utili per realizzare l'accesso alle informazioni protette) e sulla loro applicazione pratica. Inoltre, le "best practice" di sicurezza definiscono molti requisiti sui sistemi che, se opportunamente applicati, potranno in un secondo momento rendere disponibili un gran numero di informazioni aggiuntive, utilizzabili per l'analisi forense (si considerino ad esempio i *log* sugli apparati connessi ai sistemi da analizzare, i controlli di accesso, ecc.).

Nel linguaggio comune, inoltre, per *computer forensics* si intende anche il processo investigativo mediante il quale si utilizzano tecniche informatiche per raccogliere (ad esempio) indizi o fonti di prova di varia natura (ad esempio identificare l'intestatario di una linea dati o di un sito *Web*), oppure quando l'informatica assume un ruolo di mero strumento facilitatore dell'investigatore stesso (nei casi più semplici si tratta di ricercare informazioni sul *Web* tipo una fotografia dell'indagato oppure identificare un latitante che usa imprudentemente *Facebook*, *Twitter* o altri *social network*; in quelli più complessi nell'uso di sistemi di *business intelligence* finalizzati alle correlazioni non dirette tra persone, telefonate, sospetti, informazioni). In un mondo sempre più digitale, il rischio di "allargamento" di questa definizione potrebbe indurre gli studiosi ad "abusare" del ruolo di tale disciplina nei vari contesti investigativi, spostando di fatto il baricentro a favore dell'informatica la quale, invece, deve rimanere il più possibile neutra ed "al servizio" di questa o altra materia. In tal caso potremmo definire una "nuova" disciplina dal nome "digital investigation" o "informatica investigativa", sorella della *computer forensics* e cugina della più nota informatica giuridica.

Questo rischio di tecno-centrismo [6], che ha appassionato molti studiosi (tecnici e giuristi), ha portato talvolta a confondere i ruoli all'in-

dica.unipv.it/convegni/2007/pdf/Gabrini.pdf, A. Ghirardini - G. Faggioli, Computer Forensics, Apogeo, pp. 349 ss., S. Zanero, *Anti-forensics, come ti sfuggo ai RIS*, disponibile *on line* su http://home.dei.polimi.it/zanero/slides/antifor-zanero.pdf.

[6] Cfr. L. Lupària, G. Ziccardi, *Investigazione penale e tecnologia informatica*, Giuffrè, p. 136, dove si rimarca il rischio di una "deriva tecnicistica": "Del resto,per

terno di alcuni processi sui reati informatici. È accaduto, ad esempio, che alcuni giuristi, con alcune competenze di *computer forensics*, abbiano tentato di proporre dissertazioni tecniche per asserite modificazioni delle fonti di prova digitale, senza però definire (preferibilmente se non necessariamente con l'ausilio di un consulente tecnico) dove e come le stesse avrebbero avuto origine e conseguenza. Questa sorta di "accanimento informatico", ad avviso di chi scrive, ha fatto perdere la lucidità e la visione d'insieme di tutti gli elementi processuali, limitando l'analisi alle mere dissertazioni informatiche, con il rischio di farsi trascinare, addirittura, ad ammettere senza volere certe delucidazioni tecniche dell'accusa[7].

quanto sia innegabile che i nuovi settori dell'investigazione pongono sempre l'interprete in uno stato di smarrimento per le difficoltà correlate al loro collocamento tra i paradigmi teorici che compongono il tradizionale bagaglio culturale del processualpenalista (a dinamiche similari si è assistito in tema di riprese visive e rilevazioni gps), è altrettanto vero che, il più delle volte,i princìpi consolidati della teoria processuale possono essere sufficienti per risolvere le questioni connesse al nuovo fenomeno delle indagini informatiche e che, anzi, l'eccessivo scostamento dallo *ius commune indiciale*, perseguito da chi sostiene la bandiera di quella presunta "autonomia sistematica" delle operazioni di *computer forensics*, finisce col provocare pericolosi scostamenti tecnicisti e fenomeni di aggiramento delle garanzie processuali". Più in generale Faigman, *Legal Alchemy: The Use and Misuse of Science in the Law*, New York, 1999; Camon, Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali", in Cass. Pen.,1999, p.1192 ss.; Caprioli, Riprese visive nel domicilio e intercettazione "per immagini", in Giur. Cost., 2002, p. 2176 ss.; F. Ruggieri, Riprese visive e inammissibilità della prova, in Cass. Pen., 2006, p.3937; Scaglione, Attività atipica di polizia giudiziaria e controllo satellitare, in *Foro it.*, 2002, II,p.635.

[7] Si riprende, a mero titolo di esempio, questo passaggio del Tribunale Penale di Bologna, Sez. I Monocratica, Sentenza 21 luglio 2005 (dep. 22 dicembre 2005) (est. di Bari): "Le attenzioni della difesa, nella memoria depositata alla udienza del 23/6/04, si sono concentrate sul fatto che il programma interagisce solo con Outlook e non con la più diffusa versione Outlook Express; su correzioni terminologiche (come il riferimento improprio ai programmi "sorgente" sequestrati all'imputato) o sulle valutazioni del teste F., in particolare in ordine alla potenziale diffusività del programma; sulle generalizzazioni ed esemplificazioni contenute nelle note di P.G. Dalle stesse considerazioni della difesa si ricava, peraltro, che "*Vierika è un codice autoreplicante in due parti…in grado di infettare…le macchine con Windows 95 o 98 con istallato il software "Outlook Professional" della piattaforma "Microsoft Office*", p. 2; si legge ancora che "*se andiamo a leggere il codice di Vierika, troviamo che esso chiama funzioni dell'interfaccia MAPI completa, in particolare per acquisire gli indirizzi dalla rubrica"*, p. 3; a p. 5 si contesta la sussumibilità delle impostazioni di protezione di Internet Explorer nel concetto normativo di misure di sicurezza, ma non che il programma apponesse tali modifiche, tanto più che – si spiega – per ripri-

Questo rischio, altresì, ha ragione d'essere evidenziato anche per quanto concerne gli investigatori. Sempre più spesso, purtroppo, si registrano "semplificazioni investigative" (principalmente per i c.d. reati informatici), che portano ad eludere le metodologie tradizionali di riscontro, pedinamento, osservazione *et similia*. Addirittura, in taluni casi, in spregio a tutte le prassi e le regole, si sono registrati casi di richieste di rinvio a giudizio senza neppure aver effettuato una perquisizione, senza aver avuto la conferma (o meno) che una determinata condotta sia stata realmente operata dall'intestatario della linea telefonica o invece, come spesso accade, da un altro familiare. Etica [8], garanzie, professionalità e più in generale qualità delle indagini a tutto tondo dovrebbero essere la spina dorsale di un settore che, invece, si lascia spesso condurre da coloro che prediligono "indagare" solo di fronte ad un PC o in un laboratorio, sottovalutando gli schemi "classici" della cultura investigativa [9].

stinare le impostazioni originarie sarebbero bastati "*quattro click del mouse*"; si contesta la ingannevolezza del messaggio *e-mail* portatore del programma, ma non il fatto che abbia una doppia estensione e contenga un codice eseguibile; si contesta che il programma abbia un funzionamento di tipo "troiano" con appropriazione e diffusione di dati riservati, ma si ammette che esplica "*funzioni di mailing del software Outlook installato sulla macchina al fine di autoreplicarsi*", p. 9; a p. 22 si riconosce che Vierika è un *worm* che si autodiffonde utilizzando gli indirizzi di posta elettronica e che si manifesta come allegato di posta elettronica." Per quanto concerne la visione d'insieme delle fonti di prova, si riporta quanto invece indicato dalla Corte d'appello di Bologna, medesimo caso e sentenza n. 369/08: "Non si vede come possa esser messa in dubbio la fidefacienza di una risultanza documentale (tale è la traccia telematica, seppur necessitante di appositi strumenti per la fruibilità), coincidente con le ammissioni dello stesso imputato".

[8] Cfr. L. Lupària, G. Ziccardi, *op. cit*, p. 25, ove si legge: "Un auspicabile momento di approfondimento,all'interno della forensics, potrebbe riguardare gli aspetti etici: la computer ethics potrebbe essere affiancata,in tal caso, da una forensics ethics, ovvero da un'analisi rigorosa dei principi etici che devono muovere ogni soggetto che analizzi dati a fini investigativi."

[9] Cfr. A. Giarda e G. Spangher (a cura di) *Codice di procedura penale* – commentato con la giurisprudenza, p. 93, evidenzia come la Corte di Cassazione abbia ritenuto legittimo l'operato degli agenti di polizia giudiziaria che, una volta ottenuto con il sequestro la disponibilità di un telefono cellulare costituente mezzo per la commissione del reato, rispondano alle telefonate che pervengono all'apparecchio al fine di utilizzare le notizie così raccolte per l'assunzione di sommarie informazioni dagli interlocutori, ai sensi dell'art. 351, sul presupposto che in tale ipotesi non vengano in rilievo né le disposizioni sulle intercettazioni telefoniche né la tutela costituzionale della segretezza delle comunicazioni di cui all'art. 15 Cost.,trattandosi di attività che rientra nelle funzioni pro-

2. La Legge n. 48 del 2008: aspetti tecnico-giuridici

Nonostante talune critiche [10], la legge di ratifica della convenzione di Budapest (la n. 48 del 2008), ha prepotentemente introdotto all'interno del codice di procedura penale alcuni importanti elementi di principio, che prima erano linguaggio di pochi addetti ai lavori nonostante, da diversi anni [11], veniva richiamata la necessità di "rinnovamento tecnologico" del dettato normativo.

Pur non innovando – di fatto – la disciplina delle ispezioni e delle perquisizioni informatiche sotto l'aspetto operativo, la norma in parola ha colmato un vuoto "formale", più volte sottolineato dalla dottrina, sulla necessità di operare sui sistemi informatici e sui dati con modalità tecniche adeguate. In pratica, precedentemente, la procedura penale italiana non indicava, neppure sommariamente, la necessità di operare secondo determinati standard di *computer forensics* anche se, come noto, in molti contesti investigativi si erano già affermate, autonomamente e sull'onda dell'influenza delle comunità di studiosi principalmente stranieri, taluni protocolli investigativi standard quali migliori pratiche nelle indagini digitali, portate a compimento con rilevanti risultati dagli uffici inquirenti delle varie Procure della Repubblica.

prie della P.G.,volta ad assicurare le fonti di prova e raccogliere ogni elemento utile per la ricostruzione del fatto e l'individuazione del colpevole (C IV 27.11.2001, El Gana, CED 220944).

[10] Cfr. L. Lupària, I profili processuali, Diritto Penale e processo n. 6/2008, pp. 717 ss, Vitale, La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico, in Dir .Internet, 2008, IPSOA, p. 506 ss. Inoltre si segnala A. Monti, Come cambia la legge sui reati informatici, in http://www.ictlex/?p-605, secondo cui questa legge potrebbe "essere interpretata nel senso che sarebbe addirittura legittimo "bucare" un sistema, se non si possiedono le *password*, pur di accedervi e prendere le prove". Tra i primissimi commenti si richiama anche S. Aterno, M. Cuniberti, G. B. Gallus, F. Micozzi, Commento alla legge di ratifica della Convenzione di Budapest del 23 novembre 2001, disponibile sul sito del Circolo dei Giuristi telematici qui http://www.giuristitelematici.it/uploads/commento-budapest.pdf .

[11] Mi si consenta il rinvio a Costabile - Rasetti, Scena criminis, *tracce informatiche e formazione della prova*, in *Ciberspazio e Diritto* vol. n. 4, 2003. Approfondito, inoltre, questo lavoro di S. Aterno, *La* Computer Forensics *tra teoria e prassi: elaborazioni dottrinali e strategie processuali*, in *Cyberspace and Law*, Bologna, 2006.

Proprio questo inserimento normativo sta portando, nuovamente, a confrontarsi [12] sulle "misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione".

3. I c.d. sequestri informatici

Per molti anni dottrina e giurisprudenza si sono misurate a distanza sul ruolo [13] del materiale informatico c.d. neutro nelle attività di perquisizione e sequestro. Più in generale il mondo giuridico e giudiziario è stato per anni diviso sulla necessità o meno di acquisire tutto il supporto informatico nella fase di sequestro penale. Molteplici sono state le posizioni, più o meno condivise dalla giurisprudenza, di coloro che indicavano come oggetto del sequestro non il contenitore in sè, ma i dati informatici ivi contenuti [14]. Negli anni la giurisprudenza non sembra aver dato ade-

[12] Cfr. S. Aterno in Corasaniti, Corrias Lucente (a cura di), Cybercrime, responsabilità degli enti, prova digitale, Cedam 2009, p. 197. Tra i primi testi completi sulla legge n. 48 del 2008 si segnala anche L. Lupària (a cura di) Sistema penale e criminalità informatica – Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cyber crime (l.18 marzo 2008, n.48).

[13] I computer e più in generale i media digitali sono i "nuovi" protagonisti nella commissione di reati, possono contenere le prove per crimini di tipo comune oppure possono essere essi stessi obiettivi di atti criminali. Ed è in tale contesto che si pone il *cyber-investigatore,* il quale ha l'esigenza e il dovere di valutare prima di tutto il ruolo e la natura delle *"impronte elettroniche",* individuare quali supporti informatici possano contenere potenziali tracce nella *scena criminis,* acquisire e preservare le stesse fino alla loro successiva analisi, laddove non fosse possibile espletare i dovuti accertamenti direttamente sul posto.

[14] Appare d'obbligo citare che, prima della recente modifica con la legge n. 48/2008, la precedente definizione del documento informatico, nel codice penale, all'art.. 491-*bis*, recitava: *"omissis… A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli".* Con la legge n. 48 del 2008, invece, viene eliminata tale definizione, riportando il documento informatico (seppur solo nella prefazione al DDL) alla definizione di "documento informatico" di cui al C.A.D. (d.lgs. 82/2005: il riferimento è erroneamente alla definizione del D.P.R. 513/97, che, malgrado sia stato già superato da numerose altre leggi – in ultimo appunto dal C.A.D. – fornisce comunque la medesime definizione di documento informatico). Sul tema, cfr. S. Aterno, M. Cuniberti, G. B. Gallus, F. Micozzi *op. cit.*, pp. 5 e 6.

guate risposte, riconoscendo alternativamente ad un computer [15] la qualità di corpo del reato, ovvero il mezzo attraverso il quale viene consumata l'azione criminosa, oppure di cosa pertinente al reato, in quanto elemento esterno dell'*iter criminis* , con l'esame del quale può essere dimostrato il fatto criminoso, comprese le modalità di preparazione ed esecuzione [16]. È palese che tale vincolo pertinenziale non sembra sussistere sempre tra il reato e l'intero supporto informatico, in luogo delle sole tracce ivi contenute, almeno nei casi in cui il computer non può essere semplicisticamente considerato come "l'arma del delitto". Per questo motivo appare fondamentale valutare il "ruolo" del computer nell'attività illecita, per motivarne l'eventuale sequestro [17]. La Cassazione, ad esempio ha ritenuto legittimo il sequestro, presso lo studio di un avvocato sottoposto ad indagini, di un intero *server* informatico completamente sigillato, al fine di verificare, con le garanzie del contraddittorio anticipato, la natura effettivamente pertinenziale al reato ipotizzato, di atti e documenti sequestrati, così escludendo indebite conseguenze sulle garanzie del difensore in violazione dell'art. 103 c.p.p. [18]. Successivamente, invece, la Corte ha evidenziato [19] come sia inutile, ai fini probatori, il sequestro di materiale informatico "neutro" rispetto alle indagini (es. stampante, *scanner*, ecc.); in particolare, nel caso di specie, non veniva indicata alcuna esigenza probatoria che avrebbe potuto rendere legittimo il permanere del vincolo sul medesimo materiale. La Corte, infatti, ha rilevato come la prova sarebbe stata tutelabile anche con il solo sequestro dell'hard disk e dei *CD/floppy*. Entrambe le sentenze, comunque, anche se apparentemente contrarie, sono condivisibili e tracciano una linea comune: ogni caso è diverso da un altro e non sempre si può affermare *ex ante* quale comportamento sia il più idoneo con il materiale informatico [20].

[15] Cfr. Cass. Pen Sez. VI, 29 gennaio 1998.

[16] Cfr. Cass. Pen. Sez. V, 22 gennaio 1997, n. 4421.

[17] Si rammenta, ad ogni buon fine, che sussistono materie specifiche dove il sequestro e l'eventuale confisca di materiale informatico apparentemente neutro è prevista *ex lege*, ad esempio nel settore del diritto d'autore e nella pedopornografia digitale.

[18] Cassazione V, 19 marzo 2002, Manganello.

[19] Corte di Cassazione, Sez. III Penale, n. 1778 del 18.10.2003/03.02.2004.

[20] Cfr. Pretura Palermo, 10 giugno 1996, Cerva, in Diritto dell'Informazione e dell'informatica, 1996, p. 962, concernente una ipotesi di frode informatica, in cui è stato considerato legittimo il sequestro dei sistemi e dei supporti informatici utilizzati per

In generale, comunque, l'*hardware* di un *computer* può essere osservato sotto due distinti profili. Il computer, e non solo quello ovviamente, può assumere la veste di mero contenitore della prova del crimine, ad esempio può immagazzinare il piano di una rapina o le e-mail intercorse tra i complici. Superando la distinzione appena riportata dalla Corte di Cassazione, quindi, in tal caso si potrebbe decidere di non operare un'azione di sequestro, ma potrà essere realizzata in contraddittorio una semplice masterizzazione delle tracce pertinenti al reato, con lo strumento di polizia giudiziaria più appropriato [21], come ad esempio un'ispezione delegata *ex* art. 246 c.p.p. [22].

In questi casi, cioè quando l'*hardware* è un mero contenitore, anche le procedure federali americane cui spesso si fa riferimento, danno maggiore rilevanza all'acquisizione del dato informatico, ritenuto centrale nell'indagine, rispetto all'*hardware* che lo contiene. Ciò non vuol dire che il sequestro *tout court* degli *hard disk* sia vietato, ma viene valutata caso per caso la fattibilità in determinate circostanze "informatiche", ov-

la duplicazione di una banca dati. Si consenta il richiamo a Costabile - Rasetti, *op cit*: "In questa prospettiva va, ad esempio, interpretato e giustificato il cauto atteggiamento di coloro che, nelle fasi di indagine preliminare di un'investigazione tesa ad accertare le responsabilità della commissione di *computer crimes*, assaliti dal dubbio di una potenziale distruzione o di un occultamento dei dati contenuti sull'hard disk nei concitati momenti dell'intervento, procedono alle operazioni di polizia giudiziaria previo isolamento dell'abitazione dalla rete elettrica ed interruzione dell'erogazione dell'energia. Tale procedura, comunque, presa singolarmente e non adeguatamente supportata da accorgimenti di contorno, non appare sempre risolutiva, atteso l'uso sempre più massiccio di strumenti sostitutivi dell'alimentazione ordinaria. Si consideri, inoltre, che la procedura di interruzione dell'erogazione elettrica a scopo di salvaguardia delle prove è non del tutto raccomandabile, atteso che la mancata alimentazione può causare la dispersione di alcuni dati contenuti nella "memoria volatile" del computer, che potrebbero costituire importanti elementi di prova o fatti a confutazione per talune tipologie di reati."

[21] Cfr. Cassazione sez. III, 26 gennaio 2000, CED 217687.

[22] Il nuovo comma 2 dell'art. 244 c.p.p. sull'ispezione recita: "Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione".

vero quando la mole di dati è di un certo spessore, oppure si ha motivo di ritenere che ci siano *file* nascosti, stenografati, crittografati, cancellati, ovvero sistemi di autodistruzione dei dati in caso di *password* errata, ecc.

Non vi è dubbio, invece, che un computer utilizzato per consumare il reato di cui all'art. 615-*ter* cp (accesso abusivo ad un sistema informatico), potrebbe quindi essere annoverato tra gli strumenti per la commissione del crimine.

In generale, la risposta più adeguata alle problematiche sopra evidenziate sembrerebbe essere il buon senso, ossia garantire una blindatura delle procedure e della relativa *chain of custody* [23], utilizzando lo strumento giuridico più adatto, motivando adeguatamente la sussistenza delle concrete esigenze probatorie con riferimento alla "pertinenza" probatoria delle cose eventualmente sequestrate o oggetto di ispezione, in relazione alle quali andranno indicati gli elementi di fatto specifici che giustificano il provvedimento [24]. Ad esempio, il semplice accenno al titolo del reato non può sostituire l'indicazione delle concrete esigenze probatorie, ma può servire solo da riferimento e presupposto per il sorgere di queste, in relazione alle finalità di accertamento dei fatti contestati [25]. Dovrà quindi essere individuato [26] compiutamente il *thema probandum*, ovvero il fatto storico e concreto riconducibile, almeno astrattamente, ad una fattispecie criminosa. In mancanza di tale individuazione non sarebbe possibile accertare né l'esistenza delle esigenze probatorie su cui si fonda il provvedimento, né la natura di corpo del reato o cosa ad esso pertinente, oggetto di ricerca ed acquisizione. In tal caso quindi la perquisizione non sarà più un mezzo di ricerca della prova, ma un criticato mezzo di acquisizione della *notitia criminis* [27].

[23] Il termine "chain of custody" è riferito alla metodologia di custodia e trasporto, sia fisico che "virtuale", delle tracce informatiche. Tale metodologia è finalizzata a consentire la tracciabilità (e ripercorribilità) della movimentazione delle *digital evidence*, dal momento in cui esse sono collazionate fino a quando queste sono presentate alla magistratura, attesa la più volte menzionata natura aleatoria delle stesse.

[24] Cfr. Cass. Penale n. 649 del 2 marzo 1995.

[25] Cfr. Cass. Penale n. 649 del 2 marzo 1995.

[26] Cfr. A. Daniele, *Il riesame della perquisizione e del sequestro penale mancanti dell'indicazione del thema probandum*, 1999, p.823, Giurisprudenza Italiana a commento di Cassazione VI Sezione, 26 marzo 1997.

[27] Cfr. Cassazione VI Sezione, 26 marzo 1997, che ritiene "insufficiente quale enunciazione, ancorché sommaria e provvisoria, d'ipotesi accusatoria, la mera indicazio-

Tale indeterminatezza, accompagnata dall'indicazione che potrà essere oggetto di sequestro "quanto ritenuto utile ai fini dell'indagine", rimetterebbe alla polizia giudiziaria la valutazione e l'individuazione dei presupposti fondamentali dell'atto cautelare, con la spiacevole conseguenza, non avendo ben precisato l'importanza di taluni dati in luogo dell'intero supporto e non avendo valutato la possibilità di un'ispezione delegata, di "agevolare" un sequestro indiscriminato di *hardware*, contenente dati anche di terze persone e quindi poco inerente [28], anche alla luce della multifunzionalità dei supporti informatici, difficilmente vincolati nella loro interezza all'attività illecita [29].

Il sequestro del bene informatico, per tali motivi, deve pertanto essere valutato caso per caso e non in maniera superficiale, attesa la molteplice destinazione e funzione dello strumento.

Tale impostazione impone un più rigoroso accertamento sulla sussistenza delle finalità probatorie e sugli strumenti tecnico-giuridici più idonei all'attività di cristallizzazione ed assicurazione della prova informatica, garantendo altresì certezza, genuinità e paternità ai dati informatici, evitando contestualmente conseguenze altamente afflittive e interdittive, ancorché lesive ed estranee alle esigenze d'indagine [30].

ne, nei provvedimenti di perquisizione e sequestro, degli articoli di legge pretesamente violati, seguiti da una collocazione spazio-temporale così ampia da non apportare alcun contributo alla descrizione del fatto".

[28] L'indeterminatezza dell'indicazione ha come conseguenza diretta la necessità, secondo parte della giurisprudenza (Cfr. Cass. Pen., V, 17 marzo 2000), di una convalida ex art. 355 c.p.p.

[29] Il Tribunale di Torino, con un noto provvedimento del 7 febbraio 2000 in materia di sequestro probatorio di *hard disk*, pur non accogliendo le eccezioni sull'asserita immaterialità delle tracce informatiche, ha ordinato il dissequestro dell'*hardware*, riconoscendo altresì che questi è cosa pertinente al reato, ma asserendo che le esigenze probatorie potevano essere garantite con l'estrazione dei soli dati oggetto dell'attività illecita, in quanto l'intero supporto conteneva anche informazioni riferibili alla corrispondenza telematica tra l'indagato e terzi, totalmente estranei ai fatti.

[30] Cfr. Cassazione penale, sez. III, 25 febbraio 1995, n. 105, e Tribunale del riesame di Torino, 7 febbraio 2000.

4. Alla "ricerca" del dato informatico: accertamenti urgenti, ispezione e perquisizione informatica

A seguito della novella introdotta dalla legge n. 48 del 2008, questi sono i commi approvati [31] e quindi introdotti negli artt. 244 c.p.p. (ispezione) e 247 c.p.p. (perquisizione): Comma 2 dell'art. 244 c.p.p.», anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione». Comma 1 *bis* dell'art 247 c.p.p.: «1-*bis*. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

È necessario precisare che la ratifica della Convenzione di Budapest, anche se con molto ritardo, è avvenuta in un momento storico molto particolare della legislatura del 2008 [32]. Nella prima versione del testo [33], infatti, non vi era nessun richiamo alla necessità di prevedere tecniche dirette ad assicurare l'integrità dei dati per gli articoli relativi alle ispezione ed alla perquisizione.

Facendo un passo indietro, quindi, nel "Disegno di legge approvato dal Consiglio dei Ministri dell'11 maggio 2007 recante autorizzazione alla ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica, sottoscritta a Budapest il 23 novembre 2001, e sua esecuzione nonché norme di adeguamento dell'ordinamento interno", all'art. 7, si leggeva: All'articolo 244, comma 2, del codice di procedura penale, dopo le parole "e ogni altra operazione tecnica" sono aggiunte le seguenti: "anche in relazione a sistemi informatici o telematici". Al secondo comma dell'art. 7, invece, si leggeva: All'art. 247 del codice di procedura penale, dopo il comma 1, è inserito il seguente: «1-*bis*. Quando vi è

[31] La norma ha modificato molti passaggi del codice penale e di procedura penale. Si riportano solo alcuni articoli, per mera motivazione espositiva. Per una versione completa delle modifiche, si rimanda a http://www.parlamento.it/parlam/leggi/08048l.htm.

[32] Il governo Prodi era stato "sfiduciato".

[33] Cfr. S. Aterno in Corasaniti, Corrias Lucente (a cura di), *Cybercrime, responsabilità degli enti, prova digitale*, Cedam 2009, pp. 198 ss.

fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione».

Alcuni studiosi, chiamati nel novembre/dicembre 2007 dalle commissioni parlamentari per una preliminare seppur estemporanea analisi dell'articolato, avevano suggerito – tra le varie ipotesi, a seguito di numerosi confronti interni su posizioni spesso diverse –, quanto meno di aggiungere in entrambi gli articoli sopra indicati la locuzione "adottando misure tecniche idonee ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione". Tali suggerimenti, poi divenuti legge, avrebbero asseritamente consentito di mettere l'accento sulle esigenze di preservazione, genuinità e non alterabilità tanto care alla Convenzione di Budapest. Del resto, tale proposta era in linea con molte delle altre norme inserite con il disegno di legge che ha portato alla legge n. 48/2008 (si pensi all'art. 254-*bis* c.p.p. e soprattutto agli artt. 260 e 354 comma 2 c.p.p. che richiedono una procedura di duplicazione che assicuri la conformità della copia all'originale e la sua non modificabilità).

Molto probabilmente, tale nuovo articolato, seppure per molti versi condivisibile, necessitava di maggiori riflessioni tecniche e giuridiche. Analogamente, la Convenzione di Budapest del 2001 non entra nel merito degli istituti giuridici, suggerendo genericamente nella versione inglese, all'art. 19, un "Search and seizure of stored computer data", che diventa "Perquisition et saisie de données informatiques stockées" nella versione francese (si rammenta che la parola ispezione si traduce, in francese, con *inspection* o *fouille*, la quale al contempo significa anche perquisizione).

Dal punto di vista tecnico, comunque, al di là degli aspetti terminologici e giuridici, le attività di ispezione e perquisizione informatiche (e finanche gli accertamenti urgenti della PG) possono essere attuate essenzialmente in modo analogo.

Ad avviso di chi scrive, anche prima della riforma del 2008 [34], l'ispezione era quell'attività tipica di Polizia Giudiziaria che più si avvicinava alla ricerca di informazioni digitali utili alle indagini [35] (informatiche

[34] Cfr. Costabile - Rasetti, *op. cit.*, 2003.

[35] Contra, Aterno, in Cybercrime, *responsabilità degli enti, prova digitale*, (a cura di Corasaniti e Corrias Lucente), CEDAM 2008, pp. 206 ss, secondo cui "l'ispezio-

e non). L'istituto volge, in generale, all'esame di persone, cose o luoghi, allo scopo di accertare le tracce e gli altri effetti materiali del reato (ad esempio impronte sul pavimento, macchie di sangue).

Questa attività, precedentemente poco utilizzata nel settore delle *digital evidence*, in quanto esigente di specifiche competenze tecniche e variegato materiale *software*, è caratterizzata dall'irripetibilità (giuridica) degli atti, con la conseguente utilizzabilità piena originaria nel dibattimento. Tale procedura, incoraggiata da tempo da alcuni studiosi della materia, appare consigliabile esclusivamente per piccoli reati (ad esempio in presenza di *dialer* , diffamazione, *virus)*, o per casi dove è necessario acquisire solo una piccola parte di dati, la cui detenzione è lecita e la cui allocazione può essere "facilmente" individuabile (ad esempio per ispezioni presso terzi non indagati, al fine di acquisire la posta elettronica di una diffamazione via *email*, oppure la contabilità elettronica di una azienda o ancora l'acquisizione delle tracce informatiche sui sistemi anti-intrusione a seguito di un accesso abusivo ad un sistema informatico aziendale). Inoltre, come già accennato, si tratta di un'attività mediamente più tecnica (anche se non necessariamente complessa, come vedremo successivamente) dove l'operatore deve, in contradditorio con la parte ed anche mediante ausiliari di Polizia Giudiziaria (nel caso di aziende complesse), "esplorare" i supporti informatici dell'indagato (o talvolta dello stesso esponente), alla ricerca di dati e tracce informatiche inerenti i fatti oggetto dell'ispezione, che saranno cristallizzati con i dovuti metodi in supporti durevoli allegati al verbale.

Per quanto concerne le garanzie difensive, è importante sottolineare che nei casi di urgenza l'avviso può essere dato dal pubblico ministero alla persona indagata ed al suo difensore anche senza il rispetto del termine di ventiquattro ore prima; l'avviso, invece, può essere omesso – fatto salvo il diritto del difensore di intervenire al compimento dell'atto – quando vi è fondata ragione (di cui vi deve essere traccia nella motiva-

ne è possibile limitatamente al rilevamento esteriore di tracce e di altri effetti del reato ed è quindi ipotizzabile soprattutto nel momento in cui ci si limita ad osservare il sistema informatico o telematico, descrivendo nei suoi particolari, ad esempio la presenza di periferiche collegate o scollegate, rilevando la presenza (sistema acceso) di particolari sistemi *hardware* o *software* o l'utilizzo e la presenza di sistemi particolari di connessione (reti *wireless*, adsl) o di supporti informatici di pertinenza".

zione del decreto del Pubblico Ministero) che il ritardo nell'effettuazione dell'ispezione possa provocare un'alterazione delle tracce o degli altri effetti materiali del reato (art. 364 commi 5 e 6 c.p.p.). Tale ultima ipotesi, a parere di chi scrive, è praticamente sempre attuabile nei casi di ispezione informatica.

Pare meritevole altresì segnalare un limite di natura meramente temporale: come parzialmente accennato, non è sempre possibile esplorare nel merito e sul posto una grande mole di dati, considerando anche quelli cancellati che dovranno, ove possibile, essere opportunamente recuperati [36].

Per questi motivi, dovrà quindi essere valutata preventivamente l'opportunità dell'ispezione, consigliabile preferibilmente quando un sequestro indiscriminato sarebbe sproporzionato al fatto contestato (oltre che la detenzione dei dati lecita), ovvero quando l'*hard disk* è stimabile solo come contenitore di documenti informatici inerenti alle indagini, oppure altresì per attività di Polizia Giudiziaria presso terzi (banche, *provider*, ecc.) estranei di fatto alla vicenda. In altri casi, invece, l'hardware può essere considerato come frutto dell'attività criminale, come ad esempio il contrabbando, oppure uno strumento per la commissione di reati. Altro aspetto di fondamentale importanza è valutare se è necessario, ai fini investigativi, acquisire informazioni tecniche di sistema e quindi tutto l'*hard disk* rispetto ad una sola porzione di *file*. Si pensi ad esempio all'utilizzo del PC nel corso del tempo, che può essere di notevole importanza nel caso di un c.d. "alibi informatico". In questo caso non basterebbe acquisire i soli documenti di Word ritrovati nel pc per valutare tempi e modalità di utilizzo degli stessi all'interno di un sistema.

Nell'ispezione, comunque, prevalgono le finalità di descrizione e rilevazione di dati oggettivi [37], non comportando, al contempo, alcuna apprensione, mediante sequestro, del bene oggetto della ricerca, come invece accade nell'istituto della perquisizione [38]. La giurisprudenza, su un

[36] Le attività di recupero di *file*, comunque, non sembrano poter essere ricomprese nell'istituto giuridico dell'ispezione e perquisizione, bensì trattasi di un accertamento.

[37] Cfr. Aprile, *La prova penale*, Giuffrè, pp. 290 ss.

[38] Si ritiene utile riprendere un caso specifico, richiamato da Aprile, *La prova penale*, Giuffrè, p. 297: "Con riferimento alla ispezione di cose,nella giurisprudenza di legittimità si è sostenuto che l'accertamento relativo al funzionamento dei videogiochi ef-

caso specifico, ha ritenuto [39] che non si versasse in un'ipotesi di sequestro nel caso di acquisizione, mediante riproduzione su supporto cartaceo, dei dati contenuti in un archivio informatico visionato nel corso di una ispezione legittimamente eseguita ai sensi dell'art. 244 c.p.p.. Tale assunto deriva dal fatto che non vi era stata alcuna apprensione dell'archivio informatico, il quale non era stato sottratto al possessore, bensì di una semplice estrazione di copia dei dati in esso contenuti.

Ad avvalorare che l'ispezione non si limiti alla sola e passiva osservazione, ma che si spinga ad attività di rilevamento di tracce al di fuori degli accertamenti urgenti (di cui faremo cenno successivamente), ci sono le varie norme speciali sulla criminalità organizzata ed il traffico di stupefacenti. Ad esempio, ai sensi dell'art. 27 della legge 55/90 (criminalità organizzata), gli ufficiali ed agenti di Polizia Giudiziaria possono eseguire ispezioni aventi ad oggetto mezzi di trasporto, bagagli ed effetti personali allo scopo di rinvenire denaro o valori costituenti il prezzo della liberazione della persona sequestrata oppure alla ricerca di armi, munizioni, esplosivi o denaro proveniente da alcuni reati gravi. Analogamente, ai sensi dell'art. 103 del D.P.R. n. 309/90, la Polizia Giudiziaria nel corso di operazioni specifiche può operare ispezioni nelle medesime forme, per la ricerca di sostanze stupefacenti. Pur non potendo operare prelievi di materiale biologico, la Polizia Giudiziaria potrà, nella prassi delle ispezioni personali *ex* art. 244 e ss., effettuare quelle azioni tecniche che non incidono sull'integrità fisica dell'interessato (si pensi, ad esempio, al rilevamento delle impronte, allo *stub* o ancora alle indagini radiologiche che non richiedono la somministrazione di sostanze o l'introduzione di sonde [40]).

fettuato dalla polizia giudiziaria nelle more della restituzione su beni già oggetto di dissequestro va considerato legittimo,atteso che tale ispezione può essere effettuata in ogni momento *ex* artt.354 e 358 c.p.p. come un mezzo di ricerca della prova rientrante nell'attività di indagine della Polizia Giudiziaria. Conseguentemente non trova applicazione in tal caso la disciplina della inutilizzabilità,prevista in via generale dall'art. 191 c.p.p., che si riferisce alle prove acquisite in violazione dei divieti stabiliti dalla legge (Cass., sez.III, 14 novembre 2000, P.M. in proc. Maffione, in *C.E.D. Cass., n.218352).*"

[39] Cass., Sez. III, 26 gennaio 2000, Motta, in C.E.D. Cass., n. 217687.

[40] Cfr. D'Ambrosio - Vigna, *La pratica di Polizia Giudiziaria*, Cedam 2003, p. 228.

La differenza, per certi settori investigativi ancor più sottile, tra ispezione e perquisizione ha portato ad una sorta di sovrapposizione[41] per le attività di ricerca delle tracce informatiche. La novella legislativa sulle perquisizioni informatiche aveva l'obiettivo di allineare tutte le attività di Polizia Giudiziaria alle nuove tecnologie ma, probabilmente, tale innovazione necessitava di una procedura più particolare rispetto alle medesime attività effettuate nel "mondo tradizionale". Una delle modalità che avrebbero potuto contemperare tutti gli obiettivi, compreso quello di massima garanzia difensiva, sarebbe stata la previsione di una norma *ad hoc* che consentisse la manipolazione controllata di tracce informatiche ad opera di personale qualificato (come avviene per i medici nel caso di indagini invasive o per i traduttori nel caso di indagati stranieri).

In ogni caso, la norma attuale consente una sorta di perquisizione "virtuale" in luogo di quella fisica, quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza.

Forse quest'ultimo passaggio, quello relativo alle misure di sicurezza, rende la perquisizione nel "domicilio informatico" dell'indagato quell'atto di analoga natura rispetto a quanto avviene per il "domicilio tradizionale", portando successivamente al sequestro di tutto o parte del materiale digitale ivi contenuto. Anche in questo caso, comunque, appare meritevole rammentare che non sempre è opportuno operare un sequestro parziale delle *digital evidence*, per le medesime riflessioni esposte nell'ispezione informatica. La norma, novellata dalla legge n. 48 del 2008, consente anche la possibilità di effettuare un sequestro mediante un sigillo "di carattere elettronico o informatico" (veggasi nuovo art. 260 c.p.p.). Tale ipotesi, seppure molto interessante dal punto di vista tecnico, è molto rischiosa sotto il profilo investigativo, in quanto la delicatezza del dato informatico o peggio ancora la violazione dei sigilli (che in taluni casi è meno grave del reato stesso) possono portare alla dispersione irrimediabile dei dati oggetto di sequestro.

Un articolo molto importante, per le attività di informatica forense, è il citato art. 354 c.p.p. (Accertamenti urgenti sui luoghi, sulle cose e

[41] Cfr. S. Aterno, in *Cybercrime, responsabilità degli enti, prova digitale*, (a cura di Corasaniti e Corrias Lucente), CEDAM 2008.

sulle persone. Sequestro), novellato con particolare attenzione dal legislatore del 2008. Ai sensi del citato articolo gli ufficiali e gli agenti di polizia giudiziaria "curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero" e "se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il Pubblico Ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di Polizia Giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose".

Il nuovo articolato pone la massima attenzione alle c.d. *digital evidence*: "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."

Le attività sopra descritte, in pratica, sono quelle relative ai sistemi informatici generalmente accesi. Si pensi ad un caso di *peer to peer* o ancora ad un accesso abusivo ad un sistema informatico. Molte informazioni potrebbero essere difficilmente o irrimediabilmente recuperabili nel caso, ad esempio, di attesa prolungata (si pensi alla sovrascrittura dei log di un sistema anti-intrusione) o di spegnimento del sistema informatico (in particolare per quanto concerne la memoria volatile, cd. RAM [42]). In tali casi sono necessarie alcune operazioni tecniche tese alla cristallizzazione delle tracce informatiche più fragili, oltre che le connessioni attive. Per quanto concerne le attività descrittive, si suggerisce di effettuare riprese e fotografie per documentare le attività tecniche di *computer forensics* fin dalle prime fasi [43]. L'attività forense richiede pertanto che ogni operazio-

[42] Cfr. F. Schifilliti, Memory forensics: *introduzione alle procedure di acquisizione delle memorie volatili*, in *IISFA Memberbook 2009*, Digital Forensics (a cura di G. Costabile e A. Attanasio), Experta.

[43] Cfr. C. Maioli, secondo cui "Naturalmente questo significa che quando si acquisiscono reperti informatici bisogna comportarsi scrupolosamente, acquisire non solo i singoli *file* o singoli elementi, ma immagini di interi dischi con metodi e attrezzature

ne eseguita sul dato, dall'estrazione all'analisi, sia documentata in modo da assicurare la massima trasparenza su quanto effettuato.

Il codice distingue abbastanza chiaramente tre tipi di interventi [44]: i rilievi, che hanno una funzione meramente conservativa [45] dello stato dei luoghi e delle cose in vista di un futuro accertamento tecnico; gli accertamenti tecnici ripetibili; gli accertamenti tecnici non ripetibili, con un'ulteriore sottodistinzione tra i casi in cui l'irripetibilità dipenda dalle naturali modificazioni cui sarebbero comunque soggette le fonti di prova e il caso in cui sia lo stesso accertamento a comportarne la modificazione o la distruzione.

Nel caso di accertamenti urgenti *ex* art. 354 [46] c.p.p., dovrà trattarsi di interventi di tipo conservativo, pur essendo possibile, comunque, che la Polizia Giudiziaria si faccia assistere da persone dotate di specifiche competenze tecniche (art. 348 comma 4).

In dottrina [47], sul tema, si è sostenuto che i "rilievi sono quegli atti urgenti che non implicano né una valutazione di dati, né una modificazione dello stato delle cose: l'urgenza è data dal fatto che i dati sono soggetti ad alterazione per il passaggio del tempo. Gli accertamenti tecnici

certificate ed affidabili; la letteratura consiglia di utilizzare anche il supporto di una macchina fotografica o di una videocamera per documentare con maggior dettaglio quanto eseguito.", disponibile qui http://www.dm.unibo.it/~maioli/docs/fti_informatica_3009.doc. Veggasi anche D. Caccavella, in S. Aterno - Mazzotta, La perizia e la consulenza tecnica, Cedam 2006, p. 201 secondo cui "Per quanto riguarda l'acquisizione di un disco rigido, bisogna innanzitutto tener presente che indipendentemente dalla sede in cui viene eseguita (sia esso un accertamento tecnico *ex* art. 359 c.p.c. o accertamento tecnico irripetibile ex art. 360 c.p.c. o incidente probatorio) l'acquisizione dovrà garantire l'immodificabilità del reperto, o almeno che vengano apportate il minor numero possibile di alterazioni del reperto stesso, ed inoltre altra elemento aspetto fondamentale è che sia documentate accuratamente tutte le fasi dell'operazione di acquisizione, cioè "documentare documentare, documentare".

[44] Cfr. A. Nappi, *La prova scientifica nella prospettiva delle parti*, Formazione CSM, disponibile qui http://appinter.csm.it/incontri/relaz/9976.pdf.

[45] Cfr. Cass., sez. I, 26 giugno 1998, Cappellini, m. 211278, Cass., sez. I, 5 dicembre 1994, Rizzo, m. 200239.

[46] Tale accertamento ha utilizzabilità piena fuori dal dibattimento. Può fornire al Pubblico Ministero spunti per richiedere consulenza e perizia, oltre che eventuali domande a consulenti di parte e periti.

[47] Cfr. P. Tonini, *Manuale di procedura penale, App. aggiornamento*, Giuffrè Milano, 2001, p. 53.

(invece) sono attività di acquisizione e valutazione compiute su persone, cose e luoghi il 'cui stato è soggetto a modificazione' (art.360 comma 1), ovvero attività che determinano esse stesse la modifica delle cose, luoghi o persone (art. 117 disp.att.)".

I rilievi e le operazioni tecniche eseguite nel corso delle attività di Polizia Giudiziaria, quindi, sono finalizzati alla mera rilevazione degli elementi a disposizione e per tale motivo si differenziano dagli accertamenti *ex* artt. 359 e 360 c.p.p. del consulente tecnico, in quanto questi ultimi comportano una elaborazione e valutazione dei citati elementi [48].

5. Ripetibilità e irripetibilità della computer forensics

In alcuni processi sui reati informatici, fuori e dentro le aule di giustizia, alcuni studiosi della materia si sono dibattuti sulla ripetibilità o irripetibilità delle attività di *computer forensics*.

Sotto il profilo generale, appare meritevole richiamare in questa sede alcuni principi giurisprudenziali: "… più specificamente l'acquisizione dei dati da sottoporre ad esame, non implica necessariamente l'irripetibilità dell'accertamento." (Cassazione Sez I, 3 giugno 1994, Nappi "…i semplici 'rilievi', ancorché siano prodromici all'effettuazione di accertamenti tecnici, non sono tuttavia identificabili con essi, per cui, pur essendo essi irripetibili, la loro effettuazione non deve avvenire nell'osservanza delle forme stabilite dall'art. 360 c.p.p., le quali sono riservate soltanto agli 'accertamenti' veri e propri, se ed in quanto qualificabili di per sé come irripetibili" (Cass., sez. I, 9 maggio 2002, Maisto, in C.E.D. Cass., n. 221621; Cass., sez. I, 6 giugno 1997, Pata, ivi, n. 207857).

Alcuni studiosi [49], per "complicare" lo scenario su una presunta "irripetibilità intrinseca della *computer forensics*", affermano che i programmi informatici utilizzati per la *computer forensics* "sono quasi sempre coperti da licenza, in quanto commercializzati da grandi aziende informati-

[48] Cfr. Aprile, La prova penale, Giuffrè, pp. 290 ss. e D'Ambrosio - Vigna, *La pratica di Polizia Giudiziaria*, Cedam 2003, p. 231.

[49] Cfr L. Lupària, "Sull'ipotesi di una irripetibilità intrinseca delle attività di Computer Forensics", in L. Lupària, G. Ziccardi, *Investigazione penale e tecnologia informatica*, Giuffrè 2007, pp. 152 ss.

che. Ciò impedisce di poter accedere ai c.d. "codici sorgente",vale a dire alle vere e proprie fondamenta che sorreggono l'intelaiatura del programma e ne condizionano il suo funzionamento. L'eccezione difensiva che voglia far leva sulla impossibilità,per giudice ed avvocato, di esaminare il concreto funzionamento di quel programma e quindi di poter monitorare la correttezza dell'*iter* da esso seguìto, con conseguente garanzia di fedeltà della copia effettuata, parrebbe quindi del tutto fondata".

Tale affermazione è opinabile per più ragioni. Prima di tutto molti dei programmi degli stessi indagati sono di tipo "proprietario" e non è possibile accedere ai c.d. codici sorgenti (si pensi al 80-90% della popolazione che utilizza almeno un sistema di tipo Windows). Non per questo si mette in discussione la rappresentazione di atti o fatti giuridicamente rilevanti quando si analizzano documenti informatici scritti con i più comuni programmi informatici (ad esempio Office Word, sul quale può essere apposta anche una firma digitale legalmente riconosciuta dalla norma italiana). Altro aspetto da non sottovalutare è che, comunque, le analisi condotte dal NIST [50] hanno portato a definire qualitativamente affidabili questi strumenti di analisi forense nelle varie versioni. In ogni caso, queste importanti *software house* sono disponibili a fornire il codice sorgente al Giudice, mediante una sorta di accordo di segretezza, per le eventuali attività peritali volte all'analisi del comportamento di tali strumenti informatici.

Per quanto concerne, più in generale, il tema della ripetibilità della *computer forensics*, durante in 2009, in diverse occasioni, spesso non relative ad indagini informatiche, la Corte di Cassazione ha affrontato la spinosa questione. Ad esempio, la Corte di Cassazione, con sentenza n. 14511/09, è intervenuta sull'irripetibilità degli atti con riferimento alla copia dei *file* di un computer.

La Suprema Corte ha ritenuto: "che la nozione di atto non ripetibile non ha natura ontologica, ma va ricavata dalla disciplina processuale, caratterizzata dal bilanciamento degli interessi tra la ricerca della verità nel processo e il sacrificio del principio costituzionale relativo alla formazione della prova nel contraddittorio delle parti"; di "escludere che l'attività di

[50] *National Institute of Standards and Technology* che, con un progetto specifico chiamato Computer Forensic Tool Testing (CFTT), effettua test approfonditi di *hardware* e *software* per la *computer forensics*. Veggasi www.cftt.nist.gov

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 nè 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".

Analogamente, con sentenza n. 11863 del 2009, la 1^ Sezione della Corte di Cassazione si è pronunciata, in un caso di criminalità organizzata, sul tema della ripetibilità degli accertamenti informatici, seppure con motivazione che avrebbe necessitato di qualche passaggio in più. La difesa, nel caso in parola, aveva eccepito l'inutilizzabilità dell'accertamento tecnico, in quanto asseritamente effettuato senza le garanzie della difesa previste dall'art. 360 c.p.p. (attraverso il quale era stata estratta da un supporto informatico una lista di nomi). Ad avviso della Corte, quindi, per "l'estrazione dei dati contenuti nel supporto informatico – essendo l'accertamento all'evidenza ripetibile se eseguito, come non è dubbio sia avvenuto nel caso di specie, da personale esperto perfettamente in grado di evitare la perdita dei dati medesimi – è stato applicato l'art. 359 c.p.p. e non l'art. 360 c.p.p".

Con Sentenza n. 807 del 2009 (11503/09 - udienza 25.2.2009), la Corte di Cassazione ha analizzato un caso analogo, dove la difesa ricorrente aveva ipotizzato la violazione, a mente dell'art. 606 comma 1 lettere b) ed e), degli artt. 273 c.p.p., 117 disp. att. c.p.p. e 360 c.p.p., in quanto "l'hard disk rimosso dal computer sequestrato ad …omissis… sarebbe stato letto senza la presenza dei difensori e senza la possibilità che tecnici della difesa presenziassero all'operazione, delicata, ad avviso della difesa, dappoichè cagione certa di alterazione del disco prelevato, e, pertanto, atto irripetibile". Ad avviso della Corte, l'eccezione della difesa risulta infondata, poiché "la lettura dell'hard disk non integra affatto atto irripetibile", considerato, tra l'altro, che "l'attività svolta al riguardo dalla PG rientra tra quelle svolte dalla stessa ai sensi degli articoli 348 e 354 comma 2 c.p.p. e perché, infine, possibile nel prosieguo del processo ogni attività difensiva dello *omissis*… il quale, se del caso, potrà far valere, quando sarà e se sarà eventualmente accertata l'alterazione del disco informatico, alterazione allo stato soltanto affermata dalla difesa del ricorrente, peraltro persona diversa dal proprietario del computer, e, si ribadisce, per nulla accertata".

Pur condividendo alcuni principi delle sentenze ivi richiamate, è necessario, ad avviso di chi scrive, valutare caso per caso la ripetibilità e irripetibilità delle attività di *computer forensics*. Infatti, tale assunto dipende dalla tipologia del sistema informatico (*server* o semplice computer), dal suo stato (acceso o spento, ad esempio), oltre che dal momento "storico" delle attività di Polizia Giudiziaria e più in generale investigative. La tecnica informatica, anche in questo caso, seguirà al meglio le indicazioni degli investigatori e della legge, muovendosi in attività di ricerca e cristallizzazione cautelativa delle tracce informatiche negli atti irripetibili di Polizia Giudiziaria[51], mentre suggerirà al pubblico ministero, in un secondo momento, quelle procedure ove sia possibile operare in condizioni di accertamento ripetibile ex art. 359 c.p.p. (si pensi ad un "semplice" *hard disk* di un computer portatile).

Per questo motivo, potremmo definire certamente irripetibili ma non di meno valore le attività di acquisizione delle memorie volatili durante una ispezione, perquisizione o accertamento urgente *ex* art. 354 c.p.p.. Le successive analisi, invece, saranno ripetibili, in quanto operate su un supporto durevole (ad esempio un *cd rom* non riscrivibile).

[51] Cfr. Lorenzetto, "Le attività urgenti di investigazione informatica e telematica", in "Sistema Penale e criminalità informatica" (a cura di Luca Luparia), pp. 147 ss., dove si legge che "il concetto di irripetibilità può scindersi in due proiezioni che qualificano l'atto investigativo come "indifferibile", quando verte su un oggetto destinato all'inevitabile modificazione a prescindere dal compimento dell'atto medesimo,ovvero come "non reiterabile", quando può essere effettuato una sola volta poiché la sua esecuzione determina un mutamento irreversibile dell'elemento. Posto che in occasione del primo accesso alla fonte di prova digitale è consentito individuare e acquisire il dato ma non apportarvi variazioni unilaterali,deve concludersi che l'attività urgente di investigazione informatica può dirsi legittimamente irripetibile solo in quanto "indifferibile" e mai in quanto "non replicabile". Ed invero, ogni operazione di *computer forensics*, anche quella di mera preservazione del dato, è dotata di un'intrinseca componente di indifferibilità poiché interviene su una realtà digitale per definizione precaria. Tuttavia, proprio perché l'operazione di improrogabile raccolta interviene allo scopo di conservare immutato lo *status quo*, deve riconoscersi la piena legittimazione all'iniziativa autonoma dell'investigatore,potendo anzi ravvisarsi nella rilevazione non dilazionabile il tratto tipico dell'attività investigativa urgente secondo la disciplina di cui all'art. 354, comma 2, c.p.p. Diverso è il caso in cui l'attività di rilevazione determini essa stessa un'irreversibile modifica del quadro digitale rinvenuto, ipotesi che esula ontologicamente dalla mera preservazione del dato informatico appena menzionata e che, pertanto, non è suscettibile di unilaterale compimento in occasione dell'approdo alla fonte digitale."

6. Le best practices *sulla* computer forensics

La dottrina, e recentemente anche la giurisprudenza, si sono confrontate affannosamente sulla necessità di aderire alle migliori *best practices* sulla *computer forensics*.

Gli Stati Uniti [52], che hanno molta più esperienza tecnica rispetto all'Europa in ordine alle nuove tecnologie, anche investigative, pur con le dovute differenze sul piano giuridico [53], hanno modificato negli ultimi anni il loro approccio alle linee guida sulla *computer forensics*. Infatti, mentre le prime pubblicazioni degli anni '90 erano molto più dettagliate e procedurali, nell'ultimo decennio si è dato maggior rilievo alla codifica di principi di massima [54] e di un codice etico [55], lasciando allo stato

[52] Cfr. G. Ziccardi in G. Ziccardi, L. Lupària, *op cit.*, pp. 103 ss. dove si analizzano alcune tra le linee guida, specialmente statunitensi, del settore. A titolo esemplificativo si evidenziano, in questa sede, le "Best Practices for seizing electronic evidence", progetto congiunto di United States Secret Service,International Association of Chiefs of police e National Institute of Justice, oppure la Good Practice Guide for Computer based Electronic Evidence, elaborato dalla Association of Chief Police Officiers-elaborata da NHTCU in collaborazione con la National Hi-Tech Crime Unit for Scotland (NHTCUS) e il Police Service for Northen Ireland (PSNI) – che fornisce alcune interessanti considerazioni, sempre in un'ottica prettamente investigativa, in tema di *computer forensics*.

[53] Sia nei singoli Stati che in ambito federale sussistono numerose differenze, non solo dal punto di vista sostanziale, sulle modalità di acquisizione delle fonti di prova informatiche. Ad esempio, in alcuni casi, il *Federal Rule of Criminal Procedure n. 41* consente agli agenti, previo decreto, il sequestro dell'intero *hardware*, qualunque sia il materiale ivi contenuto. Successivamente sarà effettuata la *digital analysis* del contenuto delle risorse informatiche dell'indagato. Paradossalmente in Usa sarebbe possibile sequestrare un'intera rete informatica laddove fosse accertata la commissione di un reato ad opera di un amministratore di rete nell'esercizio della propria attività.

[54] Cfr. a titolo di esempio le "Linee Guida IACIS" (International Association of Computer Investigative Specialists), dove si precisa che tutte le procedure di esame di computer e di *media* digitali sono differenti e l'esaminatore deve considerare sempre la totalità delle circostanze nel momento in cui procede all'analisi. Non tutti,quindi, i suggerimenti delle linee guida potrebbero essere necessari in ogni situazione, e gli esaminatori può darsi che si debbano adattare a condizioni inaspettate o inusuali sul campo. Per una maggiore disamina, si rimanda a G. Ziccardi in L. Lupària, G. Ziccardi, *op cit*, p. 111. Dello stesso avviso Lorenzetto in Lupària (a cura di), *op. cit.*, p. 140, dove si legge: *"Apprezzabile,al riguardo,la scelta di mantenersi su standards generici idonei a ricomprendere le più diversificate evoluzioni del progresso tecnologico,capace di inventare imprevedibili dispositivi per la memorizzazione e la trasmissione dei dati informatici."*

[55] Veggasi, a mero titolo di esempio, il codice etico dell'associazione di settore IISFA Italian Chapter, disponibile su www.iisfa.it.

dell'arte della prassi ed della tecnica un maggior dettaglio per gli addetti ai lavori [56].

Questo vuol dire che assume sempre più importanza la formazione, lo studio, l'aggiornamento, la qualità e, trasversale, l'etica. Sempre più di sovente si stanno affacciando, anche in Italia, corsi di specializzazione in *computer forensics* con relative certificazioni [57]. Anche in questo caso, uno dei rischi maggiori, se non si decide di filtrare questa tendenza prevalentemente tecnica con gli aspetti giuridici italiani ed europei, è quello di credere che le indagini possano (ed in taluni casi debbano) essere guidate dagli informatici di professione, Sherlock Holmes per passione. È di fondamentale importanza, invece, che l'investigatore (accusa o difesa che sia) valuti l'approccio tecnico più adeguato alla luce delle molteplici scale di grigio, considerando di volta in volta con il supporto del tecnico le migliori azioni (*rectius*: quelle più adeguate) rispetto al contesto tecnico-operativo ma anche giuridico. Questa "nuova" visione si discosta definitivamente dalla linea difensiva di alcuni processi italiani, dove si è tentato di affrontare in modo rigido il tema degli standard investigativi, senza peraltro sostenere quali siano le buone pratiche e quanto (e come) le azioni degli investigatori si erano discostate dalle asserite linee guida. Ad avviso di chi scrive, in un modello maturo di *computer forensics*, pur essendo necessario tracciare un percorso formativo, di principi e di prassi, talvolta duro nel merito e del metodo, dovrà sancirsi una sorta di indifferenza

[56] Sul piano storico, ad esempio, sul Codice per lo Regno delle due Sicilie – Parte quarta – 1819, si leggeva, "*quando manchi il cadavere si verificherà la esistenza precedente della persona uccisa; si designerà il tempo da che non se ne sia più avuta notizia……. Omissis…. E generalmente si procurerà di raccogliere tutte quelle prove che suppliscano al difetto dell'ingenere".* Tale approccio, nel tempo, ha poi portato ad una maggiore atipicità delle fonti di prova, mentre sul più recente art. 220 del c.p.p. l'impiego di uno strumento scientifico-tecnico è individuato come necessario, ma nulla si stabilisce sul tipo di strumento da utilizzare, la cui individuazione compete all'esperto che deve attingerlo dal patrimonio della scienza e della tecnica. Per una maggiore disamina si rimanda a O. Dominioni, *La prova scientifica*, Giuffrè, pp. 36 ss e, in termini critici, Focardi, *La consulenza tecnico extraperitale delle parti private,* Padova, 2003, p. 183.

[57] In ambito internazionale, esistono numerosissime certificazioni di *computer forensics*, tra le quali si richiamano le seguenti: CIFI, CFCE, ACE, CSFA, ENCE, CCE, CHFI, CFIA, CSE (specifica sulla steganografia), PCI (Asis), SANS GCFA. Una buona certificazione dovrebbe avere una parte teorica ed un esame pratico, oltre che necessitare di un continuo aggiornamento professionale per il suo mantenimento nel tempo.

qualitativa [58] rispetto alla tecnica da utilizzare, pur condividendo la necessità di adottare procedure tecnico-organizzative tese a fornire adeguate garanzie in termini di integrità, "autenticità" e disponibilità delle informazioni e dei dati in parola, assicurando, di fatto, "la conservazione dei dati originali e ad impedirne l'alterazione" (come richiesto dalla legge n. 48 del 2008). Il giudizio sulla validità di tale metodo acquisitivo è rimesso "al prudente apprezzamento del giudicante, in ossequio ai principi del libero convincimento del giudice e del divieto di prove precostituite nel diritto processuale penale" [59]. Eventuali sbavature, approcci "analogici" e/o non propriamente ortodossi o, peggio ancora, eventuali cattive conservazioni o alterazioni dei dati originali, sarà valutato in termini di minore affidabilità e/o inidoneità e/o infondatezza della prova c.d. informatica [60]. Appare necessario rammentare, in questa sede, che il nostro sistema processuale, non avendo accolto il principio di tassatività della prova, consente al giudice, *ex* art. 189 c.p.p., di assumere prove non disciplinate dalla legge, purché ne verifichi l'ammissibilità e l'affidabilità: il giudi-

[58] Un ottimo e condivisibile approfondimento è rilevabile in G. Braghò, in L. Lupària, (a cura di) *Sistema penale e criminalità informatica – Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cyber crime (l.18 marzo 2008, n. 48),* pp. 189 ss.*: "Viene sancita a priori l'indifferenza qualitativa fra le varie misure tecniche, tutte ab origine potenzialmente idonee ad assicurare il risultato probatorio, purchè le parti processuali possano verificare in ogni momento il percorso di acquisizione di ciò che ha formato oggetto di prova informatica. Un medesimo dato informatico può dunque essere indifferentemente acquisito attingendo alle linee guida che l'investigatore digitale o il forenser ritiene più affidabili secondo la migliore scienza e tecnica".*

[59] Cfr. G. Braghò, in L. Luparia, (a cura di) *Sistema penale e criminalità informatica – Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cyber crime (l.18 marzo 2008, n. 48)*, pp. 189 ss.

[60] Cfr. G. Braghò, in L. Lupària (a cura di) *Sistema penale e criminalità informatica – Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cyber crime (l.18 marzo 2008, n. 48),* pp. 189 ss.. *Contra,* Vitale, *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico,* in *Dir. Internet,* 2008, pp. 509-510, in cui si ricostruisce la violazione delle misure tecniche idonee in termini di nullità: "l'esattezza (o l'inesattezza) delle relative procedure dev'essere verificabile *ex post*, atteso che, in àmbito digitale il *modo* col quale si raccoglie una certa informazione influisce direttamente sulla capacità dimostrativa della stessa informazione. Se, dunque, non fossero attuate le misure di conservazione e salvaguardia dei dati originali, *l'ispezione o la perquisizione sarebbero nulle; di conseguenza anche le prove raccolte (si pensi ad esempio, ad un file di Log) sarebbero anch'esse nulle".*

ce, ad esempio, potrà utilizzare come elemento di prova la copia, anziché l'originale, di un documento, quando essa sia idonea ad assicurare l'accertamento dei fatti [61]. Attraverso tale principio si afferma che il processo deve accertare comunque una verità sostanziale mediante il meccanismo procedimentale.

Una delle pochissime sentenze sulla *computer forensics* in Italia (certamente la più complessa e articolata), che ha segnato un passo importante nella maturazione del settore, è quella di primo grado e di appello sul c.d. caso Vierika [62]. Pur avendo utilizzato metodi semplici ed in contraddittorio con la parte, durante le attività di perquisizione e sequestro, molti hanno "cavalcato" la notizia ed il relativo processo, facendosi promotori di una "battaglia garantito" contro asserite violazioni delle migliori pratiche investigative, per gli "accertamenti tecnici eseguiti dalla polizia giudiziaria senza il contraddittorio con la difesa [63]" o peggio ancora "una "truffa delle etichette" idonea ad incidere negativamente sulla correttezza del percorso che conduce alla sentenza e sulla pienezza del diritto di dife-

[61] Cfr. Aprile, La prova penale, Giuffrè, Milano, pp. 64 e 65: "Tale principio è stato formulato in una fattispecie relativa a rigetto di doglianza attinente alla produzione della copia e non dell'originale del verbale di prelevamento dei campioni degli scarichi dei reflui derivanti da insediamento produttivo (Cass., sez.III, 22 gennaio 1997, Winkler, in ottobre 1993, Fumero, ivi, n. 195557)". Più in generale, "tali attività vanno inquadrate nel novero dei mezzi destinati alla acquisizione di prove non disciplinate dalla legge,consentite dall'art.189 c.p.p. senza necessità di decreto autorizzativo della autorità giudiziaria (Cass., sez. VI, 3 giugno 1998, Pacini Battaglia, in C.E.D. Cass., n. 212220)."

[62] Tribunale Penale di Bologna, Sez. I Monocratica, Sentenza 21 luglio 2005 (dep. 22 dicembre 2005) (est. di Bari) e Corte d'App. Bologna, sent. N. 369/08, disponibili tra l'altro su www.penale.it.

[63] Cfr. A. Monti, su "Ictlex-news - Aggiornamenti del 18 gennaio 2006", disponibile su https://phobos.andreamonti.net/pipermail/ictlex-news/2006-January/000000.html. Non si comprende come possa essere eccepita la mancanza di contraddittorio con la difesa rispetto a questo importante passaggio della sentenza di Appello, che pure rimarca: "Nel corso del dibattimento di primo grado (udienza 23.9.04) con l'accordo delle parti, sono state acquisite ex art. 493, c.3, CPP, e dichiarate utilizzabili per la decisione le annotazioni di polizia giudiziaria (Guardia di Finanza) del 13.3.01, 19.3.01, 28.3.01, 15.5.01. Già il rilievo dell'acquisizione con dichiarazione di utilizzabilità, avvenuta con l'espresso consenso della difesa, è esaustivo della infondatezza dei motivi di impugnazione in proposito, relativi alla natura di accertamento tecnico non ripetibile delle annotazioni."

sa all'imputato" [64]. Eppure, come peraltro recentemente rimarcato in una primissima sentenza di Cassazione della fine del 2008 [65] (successiva alla legge n. 48 del 2008, rispetto al caso vierika che è del 2001), erano state masterizzate le tracce informatiche (nella circostanza alcune cartelle con i codici sorgenti del *virus*) in alcuni cd-rom non riscrivibili. Le copie erano state effettuate, sotto stretta vigilanza degli operanti, dallo stesso indagato il quale, "ammettendo" di aver scritto Vierika, chiedeva di evitare un sequestro indiscriminato del copioso materiale informatico, in quanto lo stesso era asseritamente indispensabile per il suo lavoro nel settore dei giochi (in particolare del *bowling*). L'indagato "dimostrava" una reale collaborazione guidando gli investigatori, senza voler farsi assistere per le attività di Polizia Giudiziaria, nell'estrazione dei dati oggetto delle indagini. La masterizzazione dei *cd rom* non riscrivibili può dirsi conforme alla legge n. 48 del 2008, ovvero una misura tecnica idonea a salvaguardare i dati originali e ad impedirne l'alterazione? Ad avviso di chi scrive la risposta è affermativa (già prima [66] delle citate sentenze della Corte di Cassazione), pur ammettendo che in tal caso può esistere un ragionevole rischio di incompletezza delle informazioni estratte, direttamente proporzionale al bagaglio informativo dell'investigatore rispetto all'indagi-

[64] Cfr. L. Lupària in L. Lupària, G. Ziccardi, Investigazione penale e tecnologia informatica, Giuffrè, pp. 199-200.

[65] Cfr Cass, Sez. II, 13 marzo 2009, (ud 12 dicembre 2008), n. 11135, Bruno, che si riferisce ad un caso di sostituzione di persona, accesso abusivo a sistema informatico e tentata truffa.

[66] Durante l'IISFA Forum 2008, a Bologna, il sottoscritto ha stato mostrato che la mera apertura, il trascinamento o la masterizzazione di un *file* di office (nel caso di specie una presentazione in Powerpoint) non comportava una modifica della sua "impronta informatica", ovvero del suo *hash* (MD5, per precisione). Le uniche informazioni che vengono modificate sono quelle relative ai c.d. metadata (che contengono informazioni "di contorno", talvolta molto importanti per le indagini), ovvero ad esempio la data di creazione del *file* (il *file* di fatto riporterà la data del trascinamento o masterizzazione e non più quella di creazione "originale"). Questa informazione, comunque, può essere importante per talune indagini e quindi, pur ammettendo in casi particolari una masterizzazione dei citati *file*, appare preferibile raggruppare i *file* in una cartella compressa, in modo da evitare la modifica delle citate informazioni afferenti alle date/ore. Analogamente, andrebbe acquisita anche l'informazione sulla congruità dell'orologio di sistema e della data rispetto all'orario delle operazioni, evidenziando eventuali discrasie.

ne [67]. Incompletezza in particolare per l'accusa, atteso che i supporti informatici rimarrebbero in tal caso nella disponibilità dell'indagato. Come già rimarcato in precedenza, l'estrazione parziale di dati, quindi, pur essendo conforme al dettato normativo del 2008, è una misura da valutare caso per caso, in quanto può essere insufficiente laddove vi siano ulteriori dati la cui necessità di acquisizione fosse intervenuta in un momento storico diverso. Penso ad esempio all'ipotesi di un "alibi informatico", in questi ultimi tempi uno degli strumenti più utilizzati nei casi di delitti di sangue. Acquisire parte delle informazioni (ad esempio i *file* di una tesi di laurea alla cui lavorazione nelle medesime ore si "aggrappa" l'indagato), è sicuramente un "errore" che l'investigatore non deve commettere. Per definire l'uso continuativo di un computer ed un buon grado di veridicità rispetto a date e orari di un "orologio informatico", è necessario dover disporre di tutta la memoria del computer, oltre che preferibilmente di dati esterni che possano avvalorare alcune ipotesi (penso ad esempio al ricevente di *email* inviate dall'indagato, ai *log* di connessione dati per la navigazione, alle antenne BTS di telefonia cellulare, ecc). Come noto, infatti, è molto semplice modificare gli orari di un computer e quindi creare artatamente un alibi informatico, anche con l'ausilio di *software ad hoc* che simulano la presenza umana di fronte ad un computer.

Tornando al caso di scuola "Vierika", la difesa dell'imputato sia nel corso dell'istruttoria, che nell'arringa finale ha reiteratamente posto in discussione la correttezza del metodo utilizzato dalla Polizia Giudiziaria per "estrarre" i dati informatici dal computer dell'imputato. Ad avviso del Tribunale di Bologna (sentenza di primo grado), non è compito del Giudice "determinare un protocollo relativo alle procedure informatiche forensi, ma semmai verificare se il metodo utilizzato dalla P.G. nel caso in esame abbia concretamente alterato alcuni dei dati ricercati. In altre parole, non è permesso al Tribunale escludere a priori i risultati di una tecnica informatica utilizzata a fini forensi solo perché alcune fonti ritengono ve ne siano di più scientificamente corrette, in assenza della allegazio-

[67] Sempre nel caso Vierika, come emerge dalla documentazione disponibile e dalle stesse sentenze, i codici sorgenti di Vierika erano solo un tassello dell'impianto accusatorio, basato tra l'altro su *file* di *log* di due *provider* esterni (*upload* in amministrazione del *worm* su una pagina *Web* e *log* di connessione dati dalla linea telefonica fissa).

ne di fatti che suggeriscano che si possa essere astrattamente verificata nel caso concreto una qualsiasi forma di alterazione dei dati e senza che venga indicata la fase delle procedure durante la quale si ritiene essere avvenuta la possibile alterazione. In termini generali, quando anche il metodo utilizzato dalla P.G. non dovesse ritenersi conforme alla migliore pratica scientifica, in difetto di prova di una alterazione concreta, conduce a risultati che sono, per il principio di cui all'art. 192 c.p.p., liberamente valutabili dal giudice alla luce del contesto probatorio complessivo (fermo restando che maggiore è la scientificità del metodo scelto, minori saranno i riscontri che il giudice è chiamato a considerare per ritenere attendibili gli esiti delle operazioni tecniche)". Inoltre, continuando in ordine alla medesima sentenza, il Giudice evidenzia "come la difesa si sia limitata ad allegare che i metodi utilizzati, non essendo conformi a quelli previsti dalla (supposta) migliore pratica scientifica, conducono a risultati che non possono essere ritenuti *ab origine* attendibili, senza peraltro allegare che nel caso concreto si è prodotta una qualche forma di alterazione o che *avrebbe potuto prodursene alcuna, indicandone la possibile fonte, forma e fase di azione*[68]. Gli accertamenti compiuti dalla P.G. in ordine alle

[68] Dello stesso avviso Cassazione n. 14511/09, sul tema dell'irripetibilità delle acquisizioni di *file* da un computer durante le attività di polizia giudiziaria. Secondo Cass., sez. VI, 4 febbraio 1998, Ripa, m. 210378, l'onere della prova dei fatti processuali non incombe solo all'accusa, ma anche sull'imputato che li deduca; sul tema Catalano, 3, 2002, pp. 521 ss. Sulla necessità di fare riferimento alla teoria della verità come corrispondenza, v. Ferrua, 13, 1992, pp. 47 ss., De Caro, 3, 2003, pp. 12 ss. Sul tema della c.d. prova informatica, invece, si segnala F. Cajani, *Anatomia di una pagina web, commento a tribunale di Milano, Sez. III penale, 19 marzo 2007 - Giud. Mon. Mambriani, Diritto dell'internet*, IPSOA, n. 5/2007 pp. 487-488: "Spetterà a quel punto alla difesa dimostrare il contrario, non in termini generali ed astratti (limitandosi per esempio a rappresentare al giudice, come spesso avviene, l'esistenza di migliori pratiche di acquisizione del dato informatico) ma semmai indicando gli elementi, anche acquisiti a seguito di indagini difensive, che dimostrino come nel caso concreto il processo di individuazione/acquisizione/conservazione del dato informatico, così come rappresentato in dibattimento dall'accusa, abbia invece portato ad una alterazione dello stesso, tale da inficiarne un giudizio di attendibilità probatoria. Questo in adesione ad un principio motivazionale che, per quanto autorevolmente messo in discussione, non è solo del "caso Vierika" ma rientra nei generali canoni di valutazione probatoria dei complessivi elementi portati all'attenzione del giudice da tutte le parti e nel contraddittorio tra esse. Solo in tali termini il Processo, anche ove caratterizzato da questioni di carattere prettamente informatico, assolverà maggiormente la sua innata tensione ad accertare una verità processuale che sia il più possi-

tracce telematiche possono ritenersi pienamente attendibili alla luce del contesto probatorio complessivo (confermando, indirettamente, che il metodo utilizzato non ne ha alterato gli esiti).” Ad ulteriore conferma, il Giudice evidenzia ulteriormente che “la difesa si è limitata a porre suggestivamente la questione in ordine alla metodologia di sequestro del programma: non ha, invece, allegato la sua avvenuta alterazione in concreto, nonostante la disponibilità della versione da cui fu copiato il programma successivamente analizzato dalla P.G., rimasta nel possesso dell'imputato, le avrebbe permesso l'accertamento e l'allegazione di eventuali anomalie”…. “Non solo il disco rigido dell'indagato non fu sottoposto a sequestro, ma non risulta che vennero nemmeno rimossi i *files* trovati nel computer del C.: venne, infatti, sottoposta a sequestro una loro copia masterizzata su c.d., lasciando gli originali nella disponibilità dell'imputato.”

Addirittura, come emerge dal primo grado, “nella fattispecie in esame la difesa, nonostante abbia presentato quattro memorie *ex* art. 121 c.p.p., non ha prodotto alcun documento o parere che disconosca il funzionamento del *worm* nei suoi aspetti delineati al punto 2, gli unici valorizzati in questa sede: a fronte della descrizione del codice operata dalla P.G., *non ha invero allegato un diverso funzionamento del programma, chiedendone l'accertamento ad opera di un perito”….* “Quanto al principio del contraddittorio, la parità di armi fra accusa e difesa si garantisce non solo con il controesame del teste esperto addotto da una delle parti, ma con la facoltà di dedurre testimoni e produrre documenti e memorie, an-

bile coincidente con la realtà storica dei fatti.”. Contra, L. Lupària, I profili processuali, Diritto dell'Internet, IPSOA, 2006, pp. 153 ss “Si colloca in effetti fuori dall'architettura sistematica del nostro ordinamento processuale l'apposizione, a carico della difesa, di un onere di prova circa le esatte modificazioni del dato digitale provocate dall'avvenuto scostamento dalle *best practices*. La tutela della genuinità della *electronic evidence* costituisce infatti un valore assoluto al quale devono conformarsi gli organi inquirenti, pena l'inutilizzabilità del materiale raccolto per *unreliability*, vale a dire per inidoneità delle evidenze ad assicurare un accertamento attendibile dei fatti di reato. All'imputato spetta soltanto di mostrare che le modalità utilizzate per l'apprensione, per il mantenimento della *chain of custody* e per la successiva elaborazione non rispecchiano i canoni generalmente riconosciuti come affidabili. Ove ciò si appalesi, grava sull'accusa il peso di dimostrare che quel metodo, seppur difforme dalla miglior prassi tecnica, non ha, nel caso di specie, alterato i dati e ha salvaguardato la cosiddetta “integrità digitale”. E in caso di incertezza su quest'ultima circostanza, si dovrà accogliere la regola di giudizio dell'*in dubio pro reo*, e non certo quella secondo cui *in dubio pro republica*”.

che avvalendosi di consulenti tecnici (per la considerazione che il diritto alla controprova non può, invece, avere ad oggetto l'espletamento di una perizia, essendo questo mezzo di prova di per sé neutro, cfr. Cass. pen., sez. VI, n. 275/96, Tornabene)".

Tali considerazioni, inoltre, sono state condivise anche dalla sentenza di appello Vierika, la quale ha ulteriormente avvallato [69] la posizione del giudicante di primo grado in ordine alla "correttezza" dell'acquisizione delle cosiddette "tracce informatiche" o delle prove documentali di natura informatica. La lezione che abbiamo compreso dall'indagine in esame, infine, è che più che giudicare quasi scolasticamente l'uno o l'altro protocollo delle procedure informatiche forensi (cosa, come già detto, neppure effettuata in Vierika, anche se asserita nei commenti dottrinali), il giudice "dovrà verificare se nella fattispecie l'acquisizione probatoria sia fidefaciente, o se abbia subito alterazioni." (Cfr. appello Vierika).

7. Computer forensics*: profili tecnici*

Esistono differenti approcci tecnici all'analisi dei sistemi informatici in seguito all'identificazione di un possibile illecito.

Una delle classificazioni più note può derivare dallo stato di funzionamento dei sistemi oggetto di analisi, quali ad esempio: Analisi *post-mortem*: ci si riferisce ad una analisi effettuata a macchina spenta, eseguita dopo la consumazione di un illecito. Questo tipo di attività è la più so-

[69] A mero titolo di esempio si riporta questo passaggio dell'Appello del caso Vierika: "I rilievi mossi alla metodologia del sequestro informatico peraltro mai sono stati attinenti all'effettivo funzionamento e scopo del programma "Vierika", come accertato nella sentenza impugnata e sopra ripercorso, in realtà mai messi in discussione, neppure nelle memorie "tecniche" depositate dalla difesa; in esse, e del pari nei motivi di appello, mai è allegato o prospettato un funzionamento del programma diverso da quello sopra descritto. Le stesse richieste di perizia attengono ad aspetti non rilevanti per l'accertamento del funzionamento di Vierika, quali le modalità di generazione e conservazione dei log (registri di collegamento), acquisiti presso il gestore Tiscali ed Infostrada (rilevanti per individuare le generalità di "Krivoj", fatto non in discussione, od il numero di accessi al sito infettante), ovvero concernono l'originale del codice sorgente del programma e pertanto (atteso che esso era nel 2001 nella memoria del computer dell'imputato) non più espletabili, oltre che non necessarie."

vente nelle azioni di Polizia Giudiziaria, quando ad esempio si sequestra un hard disk o altra memoria da analizzare, successivamente, in laboratorio (o presso un consulente tecnico). *Live Forensics Analisys*: comprende tecniche di analisi su sistemi attivi, sviluppate negli ultimi anni; nel caso ad esempio di flagranza di reato per accesso abusivo a sistemi informatici, spesso non vi sono molte tracce sugli *hard disk* ma le informazioni possono essere allocate sulla memoria RAM (quella temporanea). Tali dati si perderebbero spegnendo il dispositivo con le modalità note nel settore [70]; inoltre, spesso i dispositivi di memoria sono protetti da meccanismi di cifratura, ed anche le chiavi sono contenute nella memoria temporanea.

Un'altra tipologia di classificazione della *computer forensics* [71], dipendente dal campo di applicazione, può essere la seguente: *Disk Forensics*: è una specifica attività legata all'estrazione di informazioni dagli *hard disk* (e più in generale alle memorie di massa) dei sistemi previa generazione di immagini forensi, su cui effettuare le relative analisi; *Memory Forensics*: si riferisce al recupero dell'informazione contenuta nella memoria RAM di un computer, caratterizzata da una forte volatilità (generalmente non sopravvive allo spegnimento [72]). Tale attività si interseca con la *Disk Forensics* precedentemente citata, ove si consideri l'analisi dello SWAP *Space*; *Network Forensics*: il termine si riferisce all'analisi di sistemi

[70] La modalità più nota è quella della disconnessione "bruta" della corrente elettrica (per la maggior parte dei sistemi), preferibilmente staccando il cavo dal computer e non dalla presa del muro (per evitare che un sistema "tampone" possa consentire al sistema di restare acceso comunque). *Contra* D'Agostini, L. Violino in *Diritto penale dell'informatica. Dai computer crimes alla digital forensics*, 2007, dove secondo gli autori tale approccio tecnico potrebbe determinare la distruzione di prove informatiche o perdita dei dati per i proprietari del sistema. Per un caso pratico dove la polizia giudiziaria aveva spento un computer acceso sulla scena del crimine si segnala G. Nicosia, D. Caccavella, *Indagini della difesa e alibi informatico: utilizzo di nuove metodiche investigative, problemi applicativi ed introduzione nel giudizio*, in *Dir. Internet*, 2007, IPSOA, p. 525.

[71] In questa classificazione non si fa riferimento alla **mobile forensics** ed all'analisi di sistemi *embedded*.

[72] Durante il 2008, l'università di Princeton, in California, ha effettuato uno studio dimostrando l'insicurezza di un computer spento. Si è scoperto che le cariche dei moduli della RAM si scaricano lentamente dopo che il viene spento. Qui è disponibile la documentazione ed un video dimostrativo http://citp.princeton.edu/memory/. Lo studio, anche se di pregio per quanto concerne i risultati, non può definirsi una pratica comune o *best practice*.

di rete, al fine di determinare elementi probatori inerenti un determinato caso investigativo; *Internet Forensics*: specializza le tecniche e le metodologie proprie delle altre tipologie di forensics al caso di illeciti che coinvolgono Internet (reati commessi "su" Internet o "mediante" Internet). Può dirsi, per certi versi, una sottocategoria della *Network Forensics*.

Al di là delle classificazioni, che potrebbero differenziarsi o arricchirsi per tipologia e per tecnica, è necessario in ogni caso considerare ortogonali le due classificazioni proposte, in quanto ad ogni specifico campo di applicazione della *computer forensics* si associa una scelta preferenziale sullo stato di funzionamento del sistema (in determinati casi la scelta è obbligata, ad esempio *Live Forensics* per il recupero dei dati in RAM).

8. La cosiddetta preview

Un altro aspetto da evidenziare, inoltre, è quello relativo alla "preview" dei reperti durante le attività di Polizia Giudiziaria. Si può decidere, ad esempio, durante le perquisizioni e/o le ispezioni, di verificare preliminarmente il contenuto di un *hard disk* prima di decidere di eseguire un sequestro. Tali attività dovrebbero essere operate da esperti tecnici, al fine di utilizzare tecniche che non modifichino lo stato del computer trovato spento (ad esempio mediante un *live* CD di tipo forense, quale ad esempio il CAINE[73], DEFT[74] o HELIX). Anche laddove il tutto fosse eseguito secondo gli schemi classici della *computer forensics*, tale ipotesi è da valutare caso per caso in relazione alla tipologia di indagine. Ad esempio, tale tecnica può avere un suo profilo positivo nelle indagini sulla pedopornografia *on line*, dove l'identificazione di materiale illecito detenuto con dolo (quindi presente sull'*hard disk* e non cancellato), può portare al sequestro dei soli *hard disk* "inerenti", lasciando fuori dal sequestro materiale "neutro" rispetto alle indagini[75]. Diverso, invece, il discorso relativo

[73] Progetto italiano, maggiori informazioni su www.caine-live.net.

[74] Per maggiori dettagli si rimanda al progetto italiano chiamato DEFT, www.deftlinux.net, ospitato da IISFA Italia.

[75] Come già anticipato precedentemente, sulla pedopornografia e sul diritto d'autore, esiste la possibilità di eseguire un sequestro di tutto il materiale informatico utilizzato per commettere il reato, per la successiva confisca. Appare meritevole segnalare, in

ad indagini per stabilire un c.d. alibi informatico o dove si rende necessario analizzare anche i *file* cancellati o di sistema. In tali casi, quindi, sarà opportuno sequestrare tutto il materiale contenente dati, anche per effettuare correlazioni e/o stabilire la c.d. *timeline* (la linea del tempo).

Tuttavia, facendo nuovamente un passo indietro, è opportuno sottolineare che un elemento chiave per la scelta del metodo di raccolta delle informazioni su tali sistemi, che potenzialmente ospitano dati di interesse per l'indagine, dipende dallo stato in cui il dispositivo viene rinvenuto (tendenzialmente: operativo, in *stand-by* e spento/scollegato). L'unico stato in cui si può avere un'accettabile probabilità che i dati rimangano "immutati" nel corso del tempo (ed in particolare durante lo svolgimento delle attività preliminari all'attuazione di tutte le contromisure che permettano l'acquisizione "sicura" della fonte di prova) è lo stato in cui il dispositivo sia spento o scollegato. Ad esempio, una chiave USB tendenzialmente mantiene i propri dati intatti finché non viene collegata ad un dispositivo in grado di accedere al contenuto di questa.

Al contrario, se l'investigatore dovesse imbattersi in sistemi attivi o in *stand-by* dovrà procedere tenendo conto che ogni operazione effettuata sul sistema potrebbe portare all'alterazione dei dati, ma potrebbe anche favorire l'identificazione di importanti informazioni che altrimenti non potrebbero essere rilevate (i processi attivi in quel determinato momento, i contenuti della memoria RAM, lo stato delle schede di rete, le tabelle di *routing*, ecc).

9. Le fasi del processo di computer forensics

Il processo di cristallizzazione della fonte di prova è un'attività mirata a congelare i dati contenuti nel sistema in modo da attribuirgli le caratteristiche di protezione richieste, definite anche dalle *Best Practice* del settore. Si considerino, ad esempio, le informazioni che sono memorizzate all'interno dei *file* di *log* di un *server*: tali *log* vengono sovrascritti con

questa sede, la proposta del Dott. Francesco Cajani, presentata in seno all'IISFA, afferente alla *"Destinazione dei beni informatici e telematici sequestrati o confiscati. Spunti per una modifica normativa in tema di contrasto al Cybercrime",* disponibile qui http://www.iisfa.it/atti_siracusa_F.Cajani.pdf.

una certa periodicità, pertanto è essenziale estrarre le informazioni che possano configurarsi come fonte di prova prima che queste vengano cancellate o modificate.

Più in generale, il processo di *computer forensics* prevederà l'esecuzione delle seguenti macro-attività: Riconoscimento e identificazione della fonte di prova; Acquisizione del dato (o del sistema); Conservazione e protezione del dato (o del sistema), trasversale rispetto a tutte le successive fasi; Analisi forense;Valutazione dei risultati estratti dall'analisi (sotto il profilo tecnico, giuridico ed investigativo); Presentazione dei risultati (al titolare delle indagini, al giudice o al committente in caso di attività stragiudiziale).

Tali macro-attività rappresentano il ciclo di vita del dato nell'ambito dell'analisi forense dal momento della sua identificazione fino alla chiusura delle attività. In particolare, le azioni più delicate di cristallizzazione sono quelle relative alle lettere A, B e C. Dalla D alla F, invece, le azioni sono meno delicate in quanto si lavora su una copia forense del dato in parola. Comunque, le attività devono essere sempre affiancate dalla redazione della documentazione sulla catena di custodia e di appositi verbali nei quali vengono riportate dettagliatamente tutte le attività svolte.

10. La copia forense

La copia forense è una copia 1:1 del supporto di memoria in un dispositivo di memorizzazione equivalente. La copia deve essere, a livello logico, perfettamente identica al dispositivo originale. Dovranno essere preservati quindi non solo i dati, ma anche lo spazio libero sul disco, i metadati, il *master boot record*, ecc. Per fare questo si può ricorrere alla tecnica del "bit stream image", che consentirà di replicare su un altro supporto di memoria un'immagine equivalente all'originale in termini di contenuto informativo, fino al livello del *bit*. Verranno preservati, quindi, anche eventuali parti apparentemente vuote, ma che potrebbero contenere *file* (o frammenti di *file*) cancellati e non visibili con i normali strumenti del sistema operativo. Esistono differenti strumenti in grado di eseguire il "bit stream image", sia via *software* che via *hardware*.

L'operazione di copia non deve in alcun modo modificare l'integrità dei dati contenuti nel supporto di memoria: per tale motivo è opportuno ricorrere all'ausilio di un *Write Blocker*[76], che impedirà la modifica dei dati sul supporto di memoria contenente la fonte di prova. In altri termini, un blocco in scrittura rende il supporto accessibile in sola lettura, permettendo l'interfacciamento alla postazione forense che ne eseguirà la *bit stream image*. Affinché la duplicazione della fonte di prova abbia maggiore valore, è richiesto che a seguito della duplicazione del dato sia eseguita una verifica d'integrità atta a dimostrare che l'originale sia identico alla sua copia. Per fare questo si ricorre a una funzione matematica detta "hash". L'*hash* è una funzione non reversibile, atta a trasformare un dato di dimensione arbitraria in una stringa di lunghezza fissa. L'*hash* di un dato rappresenta una sorta di "impronta digitale" del dato. Le funzioni di *hash* svolgono un ruolo essenziale per verificare l'integrità del dato, poiché l'esecuzione dell'algoritmo su un dato anche minimamente modificato fornisce un "message digest" (o "impronta del messaggio") completamente differente rispetto a quello calcolato sul dato originale permettendo di identificare anche le più piccole differenze (anche una virgola su un intero *hard disk*). La funzione di *hash* realizzata attraverso algoritmi pubblici e noti è strumento sufficiente per garantire che la copia e l'originale presentino le medesime caratteristiche. La lunghezza dei valori di *hash* varia secondo gli algoritmi utilizzati. Il valore più comunemente adottato è di 128 *bit* (c.d. MD5), in ambito forense è consigliato l'utilizzo di algoritmi in grado di generare *hash* di lunghezza maggiore come SHA, in grado di fornire *hash* a 224, 256, 384 e 512 *bit* (più resistenti)[77].

[76] Si tratta di un dispositivo usato dagli investigatori nel campo dell'informatica forense per prevenire eventuali scritture su dispositivi di memoria oggetto di investigazioni.

[77] Dal 2005, alcuni ricercatori cinesi hanno ritrovato alcune collisioni degli algoritmi MD5 e SHA1, comunemente utilizzati da molti *computer forensics examiner* in tutto il mondo. Ciò non vuol dire che gli stessi non possano essere ulteriormente utilizzati, anche perchè per adesso la collisione è teorica e matematica, avente scarsa efficacia reale, ma la comunità scientifica internazionale (ed anche i laboratori più avanzati in Italia) consigliano di utilizzare un doppio *Hash* di MD5 e SHA1, per ogni singolo *file* del computer. Tutto questo, nel tempo, riduce il rischio di critiche dibattimentali, che già soffrono i lunghi tempi della giustizia, in quanto si "giudica" l'operato dell'esaminatore in

Il dispositivo di memoria contenente la fonte di prova (solitamente un *hard disk*, o una memoria USB) dovrà essere estratto dal sistema, interfacciato con *Write Blocker* e collegato ad una postazione forense in grado di eseguire la copia attraverso il *bit stream image*. Tale operazione può essere svolta anche attraverso l'utilizzo di sistemi *hardware* concepiti per attività forensi (ad esempio Talon, Shadow, ecc). Nel caso in cui il supporto di memoria contenente il dato sia in sola lettura, come un CD / DVD rom, sarà possibile eseguire una copia del dispositivo senza porre le specifiche attenzioni legate alla citata protezione dalla modifica accidentale del dato (e quindi senza la necessità di un *Write Blocker*).

11. Acquisizione mediante "duplicazione" del dato

Come già anticipato sotto il profilo giuridico, la duplicazione del dato viene solitamente utilizzata durante le attività di *computer forensics*, ove sia sconsigliabile procedere con tecniche differenti, anche in relazione all'urgenza delle attività ed al materiale tecnico disponibile dagli operanti [78]. Infatti, in alcuni casi, la duplicazione del dato è ragionevolmente l'unica attività possibile: si consideri, ad esempio, il caso in cui l'indagine porti all'individuazione di un sistema acceso dotato di un disco crittografato "montato" contenente la fonte di prova. In tale circostanza, si suggerisce all'investigatore una copia dei dati, laddove il disco crittografico sia accessibile ed il sistema acceso. Paradossalmente, in tal caso, le misure tecniche in parola, specialmente se in contraddittorio, sono dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. Si tenga presente, infatti, che lo spegnimento di un sistema con un disco crittografato attivo renderebbe assai più complessa l'attività di estrazione del dato, in particolare se non si ha a disposizione la chiave per decifrare la componente crittografica.

Analogamente, lo stesso vale per acquisizioni sui server di posta elettronica o data base aziendali, *et similia*). Affinché la duplicazione del dato

un tempo molto successivo rispetto alle analisi forensi, senza affermare con decisione una sorta di *"tempus regit actum"*.

[78] Pensiamo, ad esempio, ad un accertamento urgente ex art. 354 c.p.p. o nella flagranza del reato.

abbia una certa resistenza dibattimentale, questa dovrà avvenire con l'ausilio di strumenti e specifiche procedure atte a garantire che il dato duplicato sia identico all'originale.

In particolare vi sono due aspetti di primaria importanza: la duplicazione del dato deve avvenire in modo completo e senza che questo sia modificato in alcun modo durante la fase di copia; tutti i dati che vengono duplicati per attività forensi assumono validità solo se viene verificata la loro congruenza con il dato originale. Tale operazione, come già anticipato, può essere svolta utilizzando tecniche di *hashing*.

L'acquisizione di dati nelle attività di *computer forensics* può avvenire con tecniche differenti, soprattutto in funzione del tipo di sorgente su cui si va ad agire. Qualora, infatti, l'oggetto da riprodurre sia un intero disco o altro supporto di memorizzazione dei dati, è importante che vengano preservate tutte le caratteristiche logiche dello stesso, anche in termini di settori danneggiati o apparentemente non contenenti dati, o simili. Se invece fosse necessario duplicare singoli elementi (ad esempio singoli *file* Office o .PDF, l'archivio .pst contenente le *email*, un singolo messaggio di posta in formato .msg, ecc.), è possibile adottare un approccio basato sulla semplice copia del *file*, a cui seguono i necessari passi di "firma" del dato, come descritto in seguito.

Si consideri, come approccio generale la cui valutazione di applicabilità sarà poi sempre a carico del personale operante l'acquisizione, che la scelta di acquisire singoli *file* anziché un intero supporto è in genere opportuna quando si operi in contraddittorio con la parte, che quindi è disposta a fornire collaborazione anche operativa all'operazione (da compiersi comunque sotto la supervisione dell'incaricato all'acquisizione della fonte di prova ed eventualmente di personale tecnico esperto[79]). Un discorso a parte, invece, riguarda la duplicazione di fonti remote (ad es. siti *Web* utilizzati per il "phishing"), ecc.

In ogni caso, a seguito della copia, dovrà essere verificata l'integrità della sola porzione di dato replicata. Nell'esecuzione di una copia parziale delle informazioni si deve tenere conto della possibilità che alcune informazioni perse siano ignorate, ad esempio quelle nascoste, oppure collocate

[79] Ad esempio per attività di perquisizione e/o ispezione in aziende, sarà possibile nominare come ausiliario di Polizia Giudiziaria un amministratore di sistema, che fornirà tutto il supporto tecnico adeguato alle azioni di Polizia Giudiziaria.

in altre porzioni di memoria. Ove possibile, quindi, si consiglia comunque di procedere con la copia intera del supporto di memoria nelle modalità descritte, specialmente per talune attività investigative complesse.

Nella grande maggioranza di tali circostanze, tuttavia, si è nella casistica di uno strumento informatico inteso come "contenitore" di informazioni utili a ricostruire l'illecito, e pertanto è possibile ritenere che il personale coinvolto nell'estrazione del dato non abbia alcun interesse ad operare manipolazioni su di esso.

In ogni caso, si ricorda come le azioni attuate nel processo di copia di *file* ricadano in un ambito assimilabile alla "live forensics", e pertanto la loro esecuzione è sempre soggetta ad un rischio di alterazione del dato: tale rischio deve essere attentamente valutato prima dell'esecuzione (motivo per cui l'acquisizione di singoli *file* è consigliabile quando si sia in presenza di una controparte). Limitatamente al caso specifico dell'acquisizione di *file*, si riportano qui di seguito alcuni passi procedurali che l'incaricato dell'acquisizione (anche con cognizioni tecniche di minor spessore) potrà seguire per minimizzare i rischi di contestazioni relativamente al materiale acquisito.

Si consideri pertanto lo schema seguente un prospetto riassuntivo utile come riferimento operativo. Identificazione del *file* desiderato; in caso sia bloccato anche in lettura da uno specifico processo, verifica della possibilità di terminare il processo (ad es:. il programma di posta elettronica attivo); calcolo dell'*hash* del/dei *file*; si noti che il calcolo dell'*hash* è effettuato sul contenuto del *file*, quindi è indipendente dai metadati dello stesso (date, nome, estensione, ecc.); salvataggio delle informazioni di *hash* in *file* separati; creazione di un archivio (ad esempio un *file* ".zip") contenente i *file* (questo permette di spostarli mantenendo inalterati i metadati; occorrerà poi tenere a mente che all'atto dell'estrazione dei *file* su altro supporto le date di creazione e di ultimo accesso saranno modificate nel *file* estratto, e saranno impostate all'istante di esecuzione dell'operazione); masterizzazione del *file* zip contenente i *file* di interesse, unitamente agli *hash* calcolati per detti *file*; si prevede precauzionalmente la realizzazione di 3 copie del supporto (una per la controparte, una per le analisi forensi ed una che rimanga all'ufficio operante); Firma digitale con relativa marcatura temporale (ove possibile, specialmente nel caso di operazione effettuate senza la qualifica di pubblico ufficiale) dei

CD/DVD realizzati. In caso di impossibilità (ad esempio per mancanza di connessione dati che possa consentire la marcatura temporare *on line*) può essere sufficiente una firma fisica con pennarello indelebile sui supporti fisici; andranno incluse le firme dell'acquisitore, della controparte e la data/ora di realizzazione [80].

12. Acquisizione di un sito Web

L'acquisizione di un sito *Web*, allocato o meno sul territorio nazionale, costituisce sempre più spesso un tema di particolare importanza nelle fasi investigative e più in generale nelle c.d. fonti di prova digitali. Fin dal 2004, la Cassazione – Sez. Lavoro [81], aveva affrontato questo tema spinoso, indicando che "le informazioni tratte da una rete telematica sono per natura volatili e suscettibili di continua trasformazione e, a prescindere dalla ritualità della produzione, va esclusa la qualità di documento in una copia su supporto cartaceo che non risulti essere stata raccolta con garanzie di rispondenza all'originale e di riferibilità a un ben individuato momento".

Più recentemente, in ambito penale, il Tribunale di Pescara [82] ha esaminato nel merito l'aspetto dell'acquisizione di un sito *Web*. Tale sentenza ha, nel caso specifico, definito di scarsa valenza probatoria la riproduzione stampata di un sito *Web*, nel corso di una operazione di Polizia Giudiziaria. Secondo il tribunale abruzzese, infatti, la documentazione non sarebbe stata acquisita seguendo le formalità previste per il rilascio di copie certificate (facendo riferimento, di fatto, alle indicazioni del DigitPA, già CNIPA e prima ancora AIPA). La principale attività analizzata dal Tribunale in parola, come emerge dalla documentazione disponibi-

[80] Sarà poi la verbalizzazione a supporto dell'attività di materiale riproduzione a dare formalmente atto di tali accorgimenti ed a determinare, in modo certo, il riferimento temporale del dato creato, che dovrà risultare corrispondente all'orario di creazione dei *cd-rom* stessi. Pure importante sarà il dare atto della coincidenza dell'orario riportato dall'orologio dei verbalizzanti con quello del sistema operativo del pc (o del diverso rapporto esistente tra i due, laddove non coincidano gli orari), ferma restando la compatibilità con l'esistenza di uno scarto, minimo e perciò trascurabile.

[81] Cfr. Cass. Sez. Lavoro n. 2912/04 del 18.2.2004.

[82] Cfr. Tribunale di Pescara, semt. 1369/06 - 3 novembre 2006 (ud. 6 ottobre 2006). Est. Bortone.

le, è quella esperita dal funzionario di polizia a seguito della acquisizione della c.d. *notitia criminis*. L'operatore di Polizia Giudiziaria, infatti, aveva verificato che su un determinato sito on line, vi era presente materiale pedopornografico liberamente accessibile, oltre che riconducibile all'indagato. La decisione del tribunale appare, per molti versi, discutibile, pur ammettendo che tali acquisizioni avrebbero come misura idonea la necessità di essere esperite con migliori modalità tecniche, ove possibile nell'immediatezza dei fatti. Infatti, atteso che i contenuti di un sito *Web* sono verosimilmente soggetti a rapido mutamento (si pensi ad esempio ad un'asta *on line*) e quindi non facilmente rinnovabili in dibattimento, tali attività di Polizia Giudiziaria non possono qualificarsi come di mera osservazione, bensì atti irripetibili ai sensi dell'art. 431 comma 1 lett. b) c.p.p. (quindi, di fatto, inseriti nel fascicolo dibattimentale) [83]. Infine, per quanto concerne gli aspetti relativi alla necessità, secondo il Tribunale di Pescara, di aderire alle regole tecniche dell'AIPA (successivamente CNIPA ed ora DigitPA), per l'acquisizione dei documenti informatici, la posizione indicata nella sentenza non appare condivisibile [84]. Infatti, se da un lato tali regole affrontano una materia diversa, ovvero di tipo amministrativo, l'applicabilità delle stesse necessita una forma di pubblicità che poco si sposa con le esigenze di riservatezza e segretezza che caratterizzano le attività di Polizia Giudiziaria.

Dal punto di vista tecnico-operativo, comunque, in questa sede si ritiene opportuno delineare una delle metodologie più complete per quanto concerne l'acquisizione di informazioni e dati sulla rete internet. In tali casi, inoltre, potrebbe accadere che la fonte di prova sia allocata fisicamente all'estero, ad esempio nelle indagini sul *phishing* ove il sito po-

[83] Cfr. E. Aprile, *Diritto dell'internet*, IPSOA, 2007 – Vol. 3, da p. 271 – "Sulla utilizzabilità processuale della riproduzione a stampa di documenti informatici effettuata nel corso di una operazione di polizia giudiziaria" (commento a Tribunale di Pescara, 6 ottobre 2006). Veggasi sul punto anche Cassazione, Sez. Unite, 28 ottobre 1998, Barbagallo, in CED Cass. n. 212758 per gli aspetti afferenti all'irripetibilità di accertamenti di tali fattezze.

[84] Cfr. E. Aprile, *op. cit*., secondo cui tali regole "hanno una rilevanza esclusivamente amministrativa, afferendo esse ai criteri per il riconoscimento del documento informatico che i certificatori amministrativi accreditati devono rispettare per il rilascio delle specifiche certificazioni".

trebbe essere ospitato presso *server* in nazioni dove tali attività non costituiscano reato o non siano perseguite adeguatamente.

In tutti i casi, può essere tuttavia necessario procedere con l'acquisizione "remota" del dato, ad esempio adottando il seguente approccio tecnico (o alcuni passi di esso): analisi preliminare del sito, che avviene attraverso la navigazione del sito *Web* con l'obiettivo di identificare collegamenti a siti esterni, script, ecc; mirroring dell'intero sito *Web* che può avvenire attraverso appostiti strumenti (*plugin* di *browser*, come "Spiderzilla", oppure tramite appositi come "wget" o "HTTrack") oppure accedendo direttamente al *file system* del *server* remoto; analisi del codice, con l'obiettivo di comprendere la struttura del sito, la presenza di *link*, *tag* o commenti (ponendo particolare attenzione alla presenza di *javascript* o codice che viene eseguito lato *browser*), la presenza di metadati (utilizzati da alcuni strumenti di sviluppo per mantenere alcune informazioni come: date, versione del programma utilizzato, nome dell'autore, ecc); identificazione di elementi nascosti come *hidden directory*, *hidden file* o porzioni di codice nascoste, ponendo attenzione a non utilizzare strumenti aggressivi che potrebbero modificare la fonte di prova.

Si desidera, tuttavia, sottolineare come l'adozione di tali tecniche possa talvolta essere contestata, ad esempio per queste ragioni: impossibilità di garantire l'identicità della replica del sito, infatti in caso di siti *Web* dinamici o dotati di sezioni protette da schermate di *login* potrebbe non essere possibile ottenere la copia; il fatto che l'esecuzione delle attività di accesso menzionate potrebbe comportare, implicazioni di natura legale (ad esempio nel caso di contenuti coperti da diritto d'autore, quando non vi sia adeguata "copertura legale").

Dal punto di vista giuridico, oltre già quanto indicato precedentemente, è bene in questa sede tracciare alcune considerazioni sull'onere probatorio in capo all'organo dell'accusa. È stato autorevolmente sostenuto [85] che lo stesso potrà ragionevolmente considerarsi correttamente assolto nel momento in cui venga indicato – oltre quanto già detto –

[85] Cfr. F. Cajani, *Anatomia di una pagina web*, commento a Tribunale di Milano, Sez. III penale, 19 marzo 2007 - Giud. Mon. Mambriani, in *Diritto dell'internet*, IPSOA, n. 5/2007 pp. 487-488.

per l'istruttoria dibattimentale, quanto segue: da chi sia stata individuata la pagina *Web* ed in quale contesto; indicazione di dettaglio di come tale dato si presentava al momento della sua individuazione ad opera della parte (ufficiale di Polizia Giudiziaria, persona offesa, terzi non aventi alcun minimo interesse ai fatti di cui al processo [86]); con quale modalità e dopo quanto tempo tale persona lo abbia acquisito (*ut supra*); in che modo siano state successivamente conservate le "sue caratteristiche oggettive di qualità, sicurezza, integrità" [87], così come presenti al momento della individuazione/acquisizione (*chain of custody*).

Come già indicato precedentemente, spetterà a questo punto alla difesa dimostrare il contrario, non in termini generali ed astratti [88] bensì indicando gli elementi, anche acquisiti a seguito di indagini difensive, che dimostrino come nel caso concreto il processo di individuazione / acquisizione / conservazione del dato informatico, così come rappresentato in dibattimento dall'accusa, abbia invece portato ad una alterazione dello stesso, tale da inficiarne un giudizio di attendibilità probatoria.

13. Le nuove sfide per l'informatica investigativa

Nuove sfide tecniche ed investigative si affacciano sugli schermi degli esperti di settore. Mentre in molti si approcciano, più o meno con confidenza, alla *computer forensics* oppure ai terminali mobili di nuova generazione (iPhone primo in classifica nella c.d. *mobile forensics*), sono sempre più soventi i grattacapi tecnico-investigativi (ed anche giuridici) che si propongono nei fascicoli dei PM e che vedremo, più o meno velocemente, nei rispettivi processi.

In molte indagini, spesso non strettamente informatiche, l'uso della posta elettronica, della *chat* e di altri sistemi di comunicazione da par-

[86] La cui testimonianza nel processo potrà essere valutata dal giudice con un maggiore grado di attendibilità, in astratto, rispetto a quanto potrebbe invece rappresentare la persona offesa.

[87] Cfr art. 21 comma 1 d.lgs. 82/2005.

[88] Cfr. F. Cajani, *Anatomia di una pagina web,* commento a Tribunale di Milano, Sez. III penale, 19 marzo 2007 - Giud. Mon. Mambriani, in *Diritto dell'internet*, IPSOA, n. 5/2007 pp. 487-488.

te della criminalità organizzata, appare sempre più massivo. Per questo motivo, magistrati ed investigatori che non si occupano quotidianamente di reati informatici si stanno interessando con maggior vigore al settore, spingendo di fatto ad una maggiore maturità investigativa oltre che legislativa. Al di là delle note difficoltà tecniche per esperire intercettazioni telematiche (più o meno parametriche o geografiche), si è a conoscenza di sistemi "atipici" di comunicazione. Ad esempio, trafficanti di droga che usano un medesimo indirizzo di posta elettronica (ad esempio prova@hotmail.com), scambiando al telefono (intercettato) la *password* di accesso. L'investigatore, assunta la *password*, potrà accedere alla citata *email*, delegato dalla magistratura? E, se sì, con quale "copertura giuridica" e con quale tecnica, attesa l'impossibilità nella maggior parte dei casi di richiedere assistenza al *provider* statunitense? Spesso, inoltre, lo scambio della *password* è finalizzato a poter accedere a comunicazioni presenti tra le "bozze" delle *email*. In pratica, il soggetto A accede alla casella, scrive un messaggio sulla quantità ed il prezzo della droga e salva il messaggio tra le bozze, senza inviarlo a nessuno. Il soggetto B, successivamente, con cadenza giornaliera, farà accesso alla medesima casella (con la *password* scambiata via telefono o sms) e leggerà il messaggio, lasciando con il medesimo metodo una risposta al suo interlocutore. *E-mail* come una bacheca elettronica tra due soggetti, con *server* in USA o in altri Stati, talvolta *off shore*. Apprendere il contenuto di quel messaggio può dirsi intercettazione telematica *ex* art. 266-*bis* c.p.p.? Oppure si potrebbe far ricorso, con delega del PM, alla cosiddetta ispezione o perquisizione informatica (artt. 244 e 247 c.p.p.)? La nuova norma ha aperto qualche spiraglio per vere e proprie perquisizioni da remoto? Le domande sono sempre molteplici, la dottrina e la giurisprudenza, forse nuovamente in contrasto, ci forniranno qualche *byte* in più nei prossimi anni, mentre i criminali avranno forse già abbandonato questo sistema per usarne altri più "sfidanti".

Analisi di telefoni cellulari in ambito giuridico

Mattia Epifani

ABSTRACT: In questo articolo l'autore esamina lo stato dell'arte e gli strumenti tecnici disponibili per l'analisi di telefoni cellulari a fini probatori.

INDICE: 1. Introduzione. – 2. Reperimento delle prove in un telefono cellulare. – 3. B*est Practises* per le procedure di analisi e repertamento. – 4. Strumenti per l'analisi di telefoni cellulari. – 5. Conclusioni e problematiche aperte.

1. Introduzione

In questo articolo sono trattati il repertamento e l'analisi di telefoni cellulari a fini probatori. La crescente diffusione di dispositivi radiomobili *GSM* ed *UMTS* li rende infatti protagonisti fondamentali della *scena criminis*. Gli investigatori possono utilizzare il telefono cellulare come fonte di prova per il reperimento dello storico delle chiamate, dei contatti, dei messaggi di testo (*SMS*) e multimediali (*MMS*) nonché di foto, video e audio.
I telefoni cellulari sono stati classificati dal NIST [1] in tre categorie, basate sulle rispettive caratteristiche funzionali:

- *Basic Phone*, ovvero un terminale radiomobile con velocità di calcolo e memoria limitata, dotato di uno schermo in scala di grigi, privo di fotocamera e scheda di memoria aggiuntiva, utilizzato per chiamate e invio di messaggi di testo, collegabile ad un computer tramite cavo o infrarosso, con una batteria ricaricabile al litio e senza la possibilità di connettersi ad Internet per la navigazione Web e l'invio di posta elettronica
- *Advanced Phone*, ovvero un terminale radiomobile con velocità di calcolo e memoria superiore, dotato di uno schermo in scala di colore, equipaggiato con una fotocamera a bassa risoluzione e dotato di un alloggiamento per schede di memoria aggiuntive, utilizzato per chiamate, invio di messaggi di testo e agenda degli appuntamenti, collegabile ad un computer tramite cavo, infrarosso o *Bluetooth*, con una batteria ricaricabile al litio e in grado di collegarsi ad Internet a velocità limitata per la navigazione *Wap* e l'invio e la ricezione di posta elettronica
- *Smart Phone*, ovvero un terminale radiomobile ad elevata capacità di calcolo e di memoria, dotato di uno schermo a colori reali, equipaggiato con una fotocamera ad alta risoluzione in grado di riprendere anche filmati, con la possibilità di contenere memorie di massa o rimovibili aggiuntive ad alta capacità, utilizzato per chiamate, invio di messaggi di testo e multimediali e agenda degli appuntamenti, collegabile ad un computer tramite cavo,

[1] "Guidelines on Cell Phone Forensics" (National Institute of Standards and Technology, Maggio 2007) e "Cell Phone Forensic Tools: an Overview and Analysis Update" (National Institute of Standards and Technology, Marzo 2007)

infrarosso, *Bluetooth* e *WiFi*, con una batteria ricaricabile al litio e in grado di collegarsi ad Internet ad alta velocità per la navigazione Web, l'invio e la ricezione di posta elettronica e l'*instant messaging*.

Dal punto di vista dell'elettronica, invece, i telefoni cellulari possono essere classificati da prima generazione (1G) a quarta generazione (4G). I telefoni della prima e seconda generazione (basati su tecnologie analogiche) sono stati ritirati dal mercato per consentire la diffusione di dispositivi e network di nuova generazione. A livello mondiale la tecnologia dominante è il *GSM (Global System for Mobile Communication)*. Negli Stati Uniti opera a 850 Mhz e 1.9 Mhz, mentre in Europa utilizza 900 Mhz e 1.8 Mhz. Questa tecnologia si è sviluppata in Europa all'inizio degli anni '90 ed ha visto la sua evoluzione nelle estensioni di terza generazione che consentono *data rate* maggiori. Gli standard 2G e 3G più noti sono *GPRS (General Packet Radio Service)*, *EDGE (Enhanced Data Rates for GSM Evolution)*, *3GSM*, *HSPA (High Speed Packet Access)* e *UMTS (Universal Mobile Telecommunications System)*.

I terminali radiomobili *GSM* sono caratterizzati da un codice di quindici cifre detto *International Mobile Equipment Identifier (IMEI),* che viene utilizzato per identificare il dispositivo all'interno della rete cellulare. Tale codice rappresenta in maniera univoca la casa costruttrice, il modello e la nazione in cui il terminale è stato prodotto. La maggior parte dei cellulari *GSM* visualizza l'*IMEI* sul display impostando la stringa **#06#*, la quale, è bene sottolineare, non assicura sempre una risposta valida e corretta del dispositivo e nemmeno il prosieguo del suo funzionamento.

Per poter accedere alla rete di servizi cellulari *GSM* o *UMTS*, è necessario inserire all'interno del dispositivo radiomobile una particolare *Smart Card*, detta *Subscriber Identity Module (SIM)*. Tale scheda consente al telefono di autenticarsi nella rete del *provider* che l'ha rilasciata.

Una *SIM* è caratterizzata da due codici:

- *Integrated Circuit Card Identification (ICCID)*, ovvero un codice di venti cifre che la identifica univocamente quale *hardware*.
- *International Mobile Subscriber Identity (IMSI)*, ovvero un codice di quindici cifre memorizzato all'interno della *SIM* e composto da tre parti:
    - *Mobile Country Code (MCC)*, che rappresenta il codice della nazione
    - *Mobile Network Code (MNC),* che rappresenta il codice di rete
    - *Mobile Station Identification Number (MSIN),* che rappresenta il numero univoco dell'utente all'interno della rete del suo operatore.

Alcuni terminali radiomobili di ultima generazione possono integrare al loro interno due schede *SIM*. Questo consente di associare ad un unico dispositivo più numeri di telefono, attivi contemporaneamente.

2. *Reperimento delle prove in un telefono cellulare*

L'analisi di un telefono cellulare ai fini probatori riguarda quattro aree di ricerca, ovvero:

- La memoria interna del terminale radiomobile
- La scheda *SIM*
- La memoria di massa o rimovibile aggiuntiva
- Il *Network Service Provider*[2]

Uno dei settori in maggior sviluppo in ambito di *digital forensics* è il recupero dei dati dalle memorie interne dei telefoni cellulari, poiché esse contengono tutte le informazioni che riguardano le attività recenti del telefono. In particolare si possono estrarre le informazioni generali (marca, modello, nazione di produzione), l'identificativo *IMEI*, la data e l'ora, la lingua utilizzata, la rubrica e le immagini associate ai contatti, le chiamate effettuate, ricevute e perse, i gruppi chiamanti, l'agenda degli appuntamenti, le note, gli *SMS*, gli *MMS* e i relativi allegati, le *email* e i relativi allegati, le foto e i video ripresi con la fotocamera, le registrazioni audio, le tracce di navigazione sul Web, le conversazioni di *instant messaging*, i documenti elettronici (file di testo, fogli di calcolo, PDF, ecc.), i *log* delle connessioni *GPRS/UMTS* e *WiFi*, i *log* dei messaggi *SMS* e *MMS* inviati e ricevuti, il *database* delle stazioni radio, le informazioni relative all'utilizzo del navigatore *GPS* (presente in alcuni *Smart Phone* moderni), le configurazioni di rete e il dizionario.

Il recupero dati dalla memoria interna è fortemente influenzato da:

- Organizzazione dei dati secondo *file system* [3] proprietari
- Utilizzo di sistemi operativi *embedded* [4] a seconda del produttore
- *Software* di analisi disponibili in commercio
- Competenze tecniche dell'investigatore

La memoria interna cui si indirizza l'analisi è una frazione di quella presente nel terminale radiomobile e precisamente una memoria *flash* integrata all'interno del dispositivo. L'estrazione delle informazioni in essa contenute può avvenire in modalità logica, ovvero collegando il telefono ad un computer e utilizzando un *software ad hoc*, oppure in modalità fisica, ovvero estraendo fisicamente la memoria dal dispositivo e leggendone il contenuto con dispositivi dedicati.

---

[2] Il *Network Service Provider* è l'operatore di telefonia mobile che fornisce l'accesso alla rete *GSM*. In Italia esistono quattro operatori principali (TIM, Vodafone, Wind e 3 Italia) e più di venti operatori virtuali, che offrono soluzioni commerciali appoggiandosi alla struttura tecnica di uno degli operatori principali.

[3] Un *file system* è l'insieme dei tipi di dati astratti necessari per la memorizzazione, l'organizzazione gerarchica, la manipolazione, la navigazione, l'accesso e la lettura dei dati

[4] Con il termine *embedded* si intende un sistema operativo sviluppato appositamente per una determinata architettura *hardware*

La scheda *SIM* è un particolare tipo di *Smart Card* che contiene una *EEPROM* [5], programmata dal *Network Service Provider,* prodotta da varie ditte secondo precisi standard internazionali e necessaria per il funzionamento del telefono quale sistema di ricetrasmissione.

Una scheda *SIM* può essere quindi utilizzata su differenti telefoni, salvo che questi non prevedano restrizioni particolari (per esempio la *SIM+TERMINALE* customizzati da un *Network Service Provider*). Dalla *SIM* si possono ricavare l'identificativo *ICCID* (che si trova anche stampato sulla *SIM* stessa), l'identificativo *IMSI*, le coordinate dell'ultima cella in cui il telefono ha ricevuto il segnale (*LOCI*), le ultime chiamate effettuate, la rubrica, gli *SMS* (inclusi quelli cancellati), le configurazioni per l'invio degli *SMS*, il *Network Service Provider* e le reti su cui la *SIM* è autorizzata ad operare.

La sicurezza di una *SIM* è garantita dalla possibilità di attivare meccanismi di cifratura dei dati in essa contenuti. Se tali meccanismi sono attivati è necessario inserire, ad ogni accensione del telefono, un *PIN (Personal Identification Number)*, ovvero un codice composto da quattro a otto cifre. Il *PIN* può essere personalizzato dall'utente, utilizzando le funzioni previste dal telefono cellulare. L'inserimento di un codice errato per tre volte manda usualmente la scheda in blocco temporaneo. In questo caso per sbloccare la scheda è necessario richiedere al *Network Service Provider* il *PUK (Personal Unlocking Key)*, ovvero un codice di dieci cifre da digitare sul telefono bloccato. Dopo dieci tentativi errati nell'inserimento del *PUK*, si può avere, anche in questo caso, il blocco definitivo della scheda e non è più possibile recuperare le informazioni in essa contenute.

Attualmente non esistono strumenti *hardware* o *software* in grado di estrarre o superare i codici *PIN* e *PUK* di una scheda *SIM*. Non è quindi possibile recuperare le informazioni senza conoscere almeno uno di questi codici di sblocco.

La maggior parte dei terminali radiomobili moderni è dotata di un alloggiamento per una memoria (di massa o rimovibile) aggiuntiva, per integrare la ridotta capacità di memorizzazione della memoria *flash* integrata. All'interno di queste memorie si trovano solitamente dati multimediali (fotografie, video, registrazioni audio) e documenti. Tali memorie possono tuttavia contenere qualsiasi dato in forma digitale e costituiscono pertanto un semplice strumento per l'occultamento di dati, anche grazie alle loro dimensioni geometriche ridotte. Durante la fase di analisi l'investigatore dovrà prestare la massima attenzione nell'identificare il posizionamento di queste memorie all'interno del telefono.

Con le opportune autorizzazioni è possibile richiedere informazioni utili all'indagine direttamente al *Network Service Provider*. Il D.Lvo 109/2008 ha introdotto le specifiche delle informazioni che il fornitore deve conservare. In particolare, in ambito di comunicazioni telefoniche cellulari, i dati che si possono ottenere dal *provider* sono:

---

[5] Una *EEPROM* è una memoria *read-only* programmabile da parte dell'utente in cui le operazioni di scrittura, cancellazione e riscrittura hanno luogo elettricamente.

- Numero telefonico chiamante
- Nome e indirizzo dell'utente registrato
- Numero composto, ovvero il numero o i numeri chiamati e, nei casi che comportino servizi supplementari (come l'inoltro o il trasferimento di chiamata), il numero o i numeri verso i quali è diretta la chiamata
- Nome e indirizzo dell'abbonato o dell'utente registrato
- Data e ora dell'inizio e della fine della comunicazione
- *IMSI* del chiamante e del chiamato
- *IMEI* del chiamante e del chiamato
- Etichetta di ubicazione (*Cell ID*) all'inizio della comunicazione.

3. Best Practises per le procedure di analisi e repertamento

La problematica principale nell'analisi di un telefono cellulare consiste nell'impossibilità di applicare metodologie tradizionali di *forensics*. A causa della specificità di sviluppo *hardware* e *software* e della mancanza di standard è impossibile, nella maggior parte dei casi, realizzare una copia forense (*bit-per-bit*) del contenuto della memoria interna di un terminale radiomobile, a meno di estrarre fisicamente la memoria *flash* integrata al suo interno. Questo approccio ha notevoli limitazioni, sia perché rende il telefono non più utilizzabile sia a causa della difficoltà di interpretazione dei dati estratti, che sono organizzati secondo *file system* proprietari.
A causa di queste limitazioni, la maggiore parte delle soluzioni disponibili per l'analisi utilizzano un approccio logico, ovvero lavorano a livello di *file* o *record* e non di *bit*. Questa scelta consente di recuperare molte informazioni utili dal telefono, ma tralascia completamente l'estrazione dello spazio non allocato e dello *Slack Space*, limitando di fatto l'analisi. Inoltre i programmi estraggono le informazioni utilizzando ognuno un approccio differente, causando spesso risultati non omogenei.
Ultimamente si stanno sviluppando soluzioni integrate *hardware* e *software* che estraggono i dati dal cellulare collegato alla macchina di acquisizione con un approccio fisico, ovvero realizzando una copia che sia il più possibile simile ad una tradizionale copia *bit-per-bit*.
Oltre a queste limitazioni tecnologiche, l'analisi di un telefono cellulare richiede opportune precauzioni che l'investigatore deve adottare per preservare al meglio l'integrità del dispositivo.
Durante la fase di sequestro è opportuno segnalare la posizione in cui il telefono è stato rinvenuto, annotare eventuali problemi fisici evidenti riscontrati (per esempio *display* rotto), fotografare tutti gli aspetti esterni del telefono, documentare le informazioni presenti sullo schermo (se il telefono viene rinvenuto acceso) ed effettuare videoriprese dell'ambiente in cui il dispositivo è stato sequestrato.
Insieme al telefono è opportuno sequestrare i cavi di connessione, il caricabatteria, gli imballaggi, le memorie di massa o rimovibili, i manuali d'uso, i supporti

contenenti il software del telefono, le bollette telefoniche associate all'utenza e la confezione della *SIM* (che riporta il *PIN* e il *PUK* di fabbricazione).
Il problema principale che un investigatore deve affrontare durante il sequestro è quello di isolare il telefono dalla rete cellulare cui è connesso e da altri dispositivi, per prevenire la cancellazione o la sovrascrittura di informazioni da parte del *Network Service Provider* o dell'utente. L'isolamento del telefono dalla rete può essere effettuato spegnendo il dispositivo, utilizzando un *jammer device*[6], riponendo il dispositivo in un contenitore schermato o richiedendo il blocco al *Network Service Provider*. Ciascuna di queste possibilità ha vantaggi e svantaggi che è opportuno valutare a seconda dei casi.
Lo spegnimento del telefono è la soluzione meno corretta, poiché può portare all'attivazione di codici di autenticazione (per esempio *PIN* della *SIM*) necessari per accedere nuovamente al dispositivo e ai dati, rallentando di fatto la procedura di analisi (per esempio richiesta del *PUK* al *Network Service Provider*). Nel caso di operatori stranieri può anche essere impossibile recuperare il *PUK* con cui sbloccare la *SIM*.
Un *jammer device* è sicuramente più efficace per garantire la conservazione delle informazioni sul telefono e l'integrità della prova, tuttavia gli utilizzi impropri di questi dispositivi violano la legge 98/1974, gli Artt.615 bis, 617, 617 bis c.p. e l'Art. 226 bis c.p.p sulla riservatezza della vita privata e le intercettazioni delle comunicazioni.
La richiesta del blocco dell'utenza al *Network Service Provider* richiede molto tempo e non è praticabile quando la *SIM* è di proprietà di un operatore estero.
La scelta di utilizzare un contenitore schermato (gabbia di Faraday) è la soluzione più praticata dalla forze di polizia. Effettivamente è la metodologia più affidabile durante la fase di sequestro e trasporto nel laboratorio di analisi. Tuttavia è opportuno considerare che comporta un aumento del consumo della batteria, a causa degli sforzi compiuti dal telefono cellulare per ricercare il segnale. Se il telefono è acceso è quindi necessario collegarlo ad un caricatore di batteria portatile, alimentato a pile, prima di inserirlo nel contenitore schermato.

Anche in fase di analisi è necessario isolare il cellulare dalla rete *GSM*. In questo caso l'isolamento radio può essere garantito con un *jammer device*, effettuando l'analisi in una stanza schermata, utilizzando una *SIM* clone, richiedendo il blocco al *Network Service Provider* o riponendo il telefono in un contenitore schermato.

I problemi nell'utilizzo di un *jammer device* e del blocco dell'utenza sono analoghi a quelli illustrati per la fase di sequestro, quindi queste soluzioni non sono consigliabili. Il costo di isolamento di una stanza per schermarla dalle onde radio è molto elevato e vincola l'analisi ad un luogo fisico fissato, quindi anche questa soluzione non è la più idonea.

L'analisi del telefono all'interno di un contenitore schermato è una soluzione percorribile, avendo cura di utilizzare cavi idonei (cioè cavi che non svolgano la funzione di antenna). Questa metodologia è la più appropriata quando il telefono viene sequestrato e mantenuto acceso.

---

[6] Un *jammer device* è un disturbatore di segnale per telefoni cellulari

La metodologia più appropriata nel caso in cui il telefono sia stato rinvenuto spento è l'utilizzo di una *SIM* clone, ovvero una scheda su cui siano stati impostati forzatamente l'*ICCID* e l'*IMSI* della *SIM* originale. In alcuni modelli, la rimozione della *SIM* originale può comportare la perdita di alcune informazioni, come la lista delle ultime chiamate effettuate, ricevute e perse. Queste informazioni possono essere tuttavia spesso ricavate analizzando separatamente la *SIM* con *software* dedicati.

Nel caso in cui non sia possibile clonare la *SIM* e sulla stessa sia attivata la richiesta del *PIN* è opportuno verificare il numero di tentativi rimasti, utilizzando appositi *software*. Il primo tentativo può essere effettuato provando il *PIN* fornito dal *Network Service Provider*, reperibile sulla confezione della *SIM* o dal *provider* stesso. È opportuno lasciare sempre un tentativo di inserimento del *PIN* (sui tre disponibili), qualora questo venisse fornito dal proprietario del telefono cellulare. In ogni caso non si deve mai superare il numero massimo di tentativi di inserimento del *PUK*, poiché ciò renderebbe completamente irrecuperabile il contenuto della *SIM*.

Prima di avviare l'analisi è necessario collegare il telefono ad una fonte di alimentazione (portatile o fissa), indipendentemente dal fatto che sia acceso o spento. La batteria completamente scarica potrebbe portare infatti alla perdita delle informazioni sulla data e l'ora, spesso di fondamentale importanza in un'indagine.

Una volta garantito l'isolamento del telefono dalla rete si può avviare la fase di analisi. L'analisi dei dati sarà effettuata utilizzando un personal computer su cui sia installato un *software* forense oppure con un dispositivo *hardware* dedicato all'estrazione dei dati. In entrambi i casi è necessario garantire una connessione tra il telefono cellulare e lo strumento di acquisizione. È opportuno utilizzare un'interfaccia di connessione affidabile e sicura, che minimizzi le modifiche ai dati presenti sul telefono.

A seconda del modello la connessione si può realizzare via cavo, tramite infrarossi oppure via onde radio *Bluetooth*. La connessione più sicura, affidabile e con minor impatto sui dati è quella via cavo. Qualora non sia disponibile il cavo di connessione per il modello sequestrato è consigliabile utilizzare una connessione ad infrarosso. La connessione *Bluetooth* deve essere utilizzata come *extrema ratio*, poiché genera modifiche al dispositivo durante la fase di attivazione e autenticazione della connessione.

Sulla base di queste considerazioni si possono definire due distinte procedure di analisi per **dispositivi spenti** e per **dispositivi accesi**.

- **Telefono cellulare spento:**
    - Effettuare un'analisi esterna e documentale del telefono (utilizzando anche fotografie e video)
    - Se il telefono contiene una *SIM*, rimuoverla
    - Se il telefono contiene una memoria rimovibile, rimuoverla
    - Effettuare l'analisi della *SIM* e recuperare le informazioni utili (*ICCID*, *IMSI*, *LOCI*, ecc.) e gli *SMS* cancellati

- Effettuare l'analisi della memoria rimovibile, garantendone la protezione in scrittura ed utilizzando metodologie e *software* forensi tradizionali (*Helix*, *Encase*, *FTK*, *X-Ways Forensics*, ecc.)
- Per preservare lo stato della *SIM* è opportuno clonarla ed utilizzare la carta clonata per la successiva analisi del telefono.
- Qualora non sia possibile effettuare un clone della *SIM*, utilizzare una metodologia alternativa di isolamento del telefono dalla rete
- Collegare il telefono ad una fonte di alimentazione (fissa o portatile)
- Attivare la procedura di riconoscimento del telefono da parte del *software* forense prescelto
- Accendere il telefono
- Stabilire la connessione tra il telefono e il *software*
- Estrarre le informazioni dal telefono, utilizzando le funzioni messe a disposizione dal *software* in uso.

- **Telefono cellulare acceso**:
  - Collegare il telefono ad una fonte di alimentazione (fissa o portatile)
  - Estrarre le informazioni dal telefono con le precauzioni illustrate sopra in ambiente schermato
  - Analizzare la *SIM* e la memoria rimovibile con le accortezze illustrate sopra.

In alcuni casi l'unica opzione disponibile per l'acquisizione dei dati è l'analisi manuale, ovvero la navigazione attraverso il menu del telefono e la cattura del contenuto del *display*. In questi casi è opportuno che l'investigatore conosca il funzionamento del dispositivo prima di procedere con l'analisi (per esempio consultando il manuale d'uso o facendo pratica con un dispositivo della stessa marca e modello), al fine di individuare le azioni che comportano una modifica dei dati utente e minimizzarne l'utilizzo. In questi casi è consigliabile effettuare una videoripresa della fase di analisi.

In casi estremi (telefono rotto, bruciato, rinvenuto all'interno di liquidi, ecc.), l'unica modalità per l'analisi della memoria del dispositivo radiomobile è l'estrazione del chip della memoria *flash* (*desoldering*). In questo caso sono necessarie attrezzature e competenze tecniche specializzate, offerte agli investigatori direttamente dalle case costruttrici o più spesso da enti di ricerca.

È importante, infine, tenere in considerazione opportune azioni per preservare altre fonti di prova che potrebbero essere più rilevanti ai fini dell'indagine (per esempio DNA, impronte, armi da fuoco, ecc.).

4. *Strumenti per l'analisi di telefoni cellulari*

In commercio esistono diversi strumenti *hardware* e *software* per l'analisi di telefoni cellulari. La maggior parte utilizza un approccio logico nell'estrazione dei dati, anche se ultimamente si stanno integrando tecniche di recupero a basso livello.

Al contrario della *computer forensics* tradizionale, inoltre, sono diffuse poche soluzioni *Open Source* (per esempio *MIAT* e *TULP2G*) e le soluzioni commerciali hanno costi di acquisto e manutenzione molto elevati, a causa del costante sforzo degli sviluppatori nell'aggiungere modelli supportati dalla specifica piattaforma.

I principali prodotti disponibili attualmente sul mercato sono:

- *Device Seizure* (*software*)
- *Oxygen Forensic Suite 2* (*software*)
- *MobilEdit! Forensic* (*software*)
- *Mobile Phone Examiner* (*software*)
- *Tulp2G* (*software*)
- *MIAT (software)*
- *Neutrino* (*hardware* e *software*)
- *UFED (Universal Forensic Extraction Device)* (*hardware* e *software*)
- *.XRY/.XACT (hardware* e *software)*
- *Celledk* (*hardware* e *software*)
- *Project a Phone* (analisi manuale)

Device Seizure[7] è un *software* di analisi forense prodotto da *Paraben Corporation*, che può estrarre dati da cellulari *GSM* e da *SIM*. *Device Seizure* può effettuare sia un'acquisizione logica, sia un'acquisizione fisica, che consentono l'esame della struttura della memoria interna e dei file in essa contenuti. L'acquisizione del telefono può essere portata a termine tramite cavo, infrarosso o interfaccia *Bluetooth*. Il *software* viene fornito con un *kit* di cavi per il collegamento dei telefoni supportati. Per garantire l'integrità del dato acquisito vengono inoltre calcolati un *hash* MD5 e SHA1 di ogni file estratto e del file in formato proprietario contenente tutte le informazioni ("*case file*"). I dati estratti possono essere esportati sia in formato *ASCII*, sia in formato *HTML*. *Paraben Corporation*, al fine di agevolare il lavoro di tutte le parti in causa, ha recentemente deciso di rilasciare gratuitamente il *software* di analisi *Paraben Device Seizure Lite*, privo del motore di acquisizione. In tal modo, si dà la possibilità alla controparte di effettuare le proprie valutazioni ed analisi sui file acquisiti dallo *Smart Phone*.

[7] Paraben Corporation - http://www.paraben.com/

Oxygen Forensic Suite 2 [8] è un *software* di analisi forense sviluppato da *Oxygen Software*, che può estrarre dati da oltre 1350 differenti modelli di cellulare. Supporta connessioni tramite cavo, infrarosso e *Bluetooth*. A seconda dei modelli può estrarre un numero di informazioni molto elevato, eseguendo in ogni caso un'analisi di tipo logico. Le informazioni acquisite possono essere esportate in un *report* dettagliato. Il *software* non offre funzionalità di verifica tramite *hashing* delle informazioni e dei file.

MOBILedit! Forensic [9] è un *software* di analisi forense prodotto da *Compelson Labs*, che può acquisire dati logicamente da cellulari *GSM* e da *SIM*. I dati possono essere acquisiti tramite cavo, infrarosso o *Bluetooth*. I dati acquisiti sono salvati in un file dal formato proprietario e possono essere esportati in formato *XML*. *Mobiledit!* non fornisce funzionalità di *hashing* dei dati acquisiti.

Mobile Phone Examiner [10] è un *software* di analisi forense prodotto da *Access Data* per l'acquisizione e l'analisi di telefoni cellulari *GSM* e di *SIM*. Supporta l'analisi di circa 800 differenti modelli attraverso connessioni via cavo, infrarosso o *Bluetooth*. Può generare *report* automatici dei dati estratti.

Tul2G [11] è stato il primo progetto O*pen Source* in ambito di *mobile forensics*. Il progetto è stato chiuso nel 2007. È in grado di effettuare analisi di un numero limitato di cellulari, attraverso un'interfaccia disponibile per sistemi Windows e Linux. Per l'analisi di *SIM* rimane tuttora un ottimo programma.

MIAT [12] è un progetto *Open Source* per l'analisi di telefoni cellulari sviluppato all'Università di Roma Tor Vergata. Non è ancora disponibile la versione pubblica, che sarà rilasciata nei prossimi mesi.

Neutrino [13] è un prodotto per l'analisi forense che può estrarre dati da telefoni cellulari *GSM* e da *SIM*, realizzato da *Guidance Software*. È composto da un dispositivo di acquisizione forense *hardware* e da un *software* per l'analisi dei dati estratti. Nel *kit* sono forniti anche i cavi per il collegamento del telefono al dispositivo o al computer di acquisizione.

Universal Forensic Extraction Device [14] è un dispositivo *hardware* per l'analisi di telefoni cellulari *GSM* e *SIM*, realizzato da *Cellbrite*. Per il suo utilizzo non è necessaria la contemporanea presenza di un personal computer, poiché il dispositivo di estrazione dei dati è autonomo e il telefono può esservi direttamente collegato con un cavo, via infrarosso oppure via *Bluetooth*. In dotazione viene fornito un *kit* con i cavi di connessione. Supporta attualmente più di 1700 modelli. Ha uno strumento per la clonazione della *SIM*, il cui utilizzo consente di neutralizzare i tentativi di accesso alla rete da parte del telefono. Permette il recupero delle informazioni dal dispositivo radiomobile (rubrica, *SMS*, storico delle chiamate, immagini, video, *IMEI*) e dalla *SIM* (storico chiamate e *SMS*, inclusi quelli cancellati ma ancora

---

[8] Oxygen Corporation - http://www.oxygen-forensic.com/
[9] Compelson Labs - http://www.mobiledit.com/forensic/
[10] Access Data - http://www.accessdata.com/
[11] Tulp2G Project - http://tulp2g.sourceforge.net/
[12] MIAT - http://www.dfrws.org/2008/proceedings/p121-distefano.pdf
[13] Guidance Software - http://www.guidancesoftware.com/
[14] Cellbrite – http://www.cellbrite.com/

presenti sulla *SIM*). Per mantenere in carica il dispositivo è inoltre fornito un caricatore portatile, con circa 50 differenti connessioni. I dati estratti dal dispositivo possono essere riversati direttamente su una memoria *USB*, che può essere successivamente collegata ad un personal computer per un'analisi approfondita.

.XRY/.XACT [15] è un dispositivo *hardware* e *software* sviluppato da *Micro Systemation* per l'analisi logica e fisica di telefoni cellulari. È un *kit* composto da un *set* di cavi, un'interfaccia fisica per la connessione al computer, un lettore di *SIM* e due *software*: *.XRY,* che si occupa dell'estrazione logica dei dati (con un supporto attualmente di oltre 800 modelli), e *.XACT,* che si occupa dell'estrazione fisica (con un supporto attualmente di 160 modelli). Entrambi i programmi possono esportare i risultati dell'analisi in un *report* in formato proprietario. La casa produttrice ha messo a disposizione un applicativo di lettura dei dati gratuito, per consentire la condivisione dei risultati acquisiti tra più investigatori.

Celldek [16] è un dispositivo *hardware* per l'estrazione e l'analisi di informazioni da cellulari *GSM*, prodotto da *Logicube*. Il dispositivo è dotato di una memoria interna che consente l'analisi anche senza l'utilizzo di un personal computer. I dati estratti possono essere successivamente esportati collegando una memoria *USB* esterna. Nel dispositivo è integrato un lettore per l'analisi di *SIM*. Il *kit* comprende inoltre un *set* di cavi per la connessione del telefono, un modulo *Bluetooth* e una batteria ricaricabile con diversi adattatori.

Project a phone è un dispositivo per l'analisi manuale di telefoni cellulari prodotto dall'omonima casa costruttrice. È composto da un alloggiamento all'interno del quale è possibile inserire il telefono e da una fotocamera digitale che riprende e memorizza le informazioni presenti sullo schermo. Utilizzando il *software* fornito in dotazione è possibile generare un *report* basato sugli *screenshot* acquisiti.

Molte delle soluzioni sopra illustrate richiedono l'utilizzo di un *software agent* [17] da eseguire sul telefono cellulare per consentire il trasferimento delle informazioni. In questo caso è opportuno installare l'*agent* su un supporto rimovibile, da inserire all'interno del telefono cellulare al posto di quello originale.

In alcuni casi, successivamente all'acquisizione con uno strumento dedicato, è opportuno procedere ugualmente ad un'analisi manuale, per verificare i risultati ottenuti e garantire in questo modo il buon funzionamento della soluzione scelta.

Come nel caso dell'analisi di personal computer, è opportuno documentare accuratamente i dettagli relativi agli strumenti utilizzati (per esempio il numero di versione del *software*).

---

[15] Micro Systemation - http://www.msab.com/

[16] Logicube - http://www.logicubeforensics.com/

[17] Con il termine *software agent* si intende un programma necessario per stabilire il collegamento tra il software e il dispositivo radiomobile

5. Conclusioni e problematiche aperte

Le problematiche illustrate in questo articolo rendono l'idea di quanto il campo dell'analisi dei telefoni cellulari sia in costante sviluppo, all'interno di un sistema commerciale privo di *standard* e metodologie di analisi definite e definitive.

L'analisi della *SIM* è il settore più sviluppato, poiché è noto e studiato[18] il sistema di memorizzazione dei dati al suo interno. Il software *Open Source Tulp 2G* fornisce funzionalità di estrazione dei dati della *SIM* che consentono di ottenere in maniera rapida e dettagliata un documento completo di tutte le informazioni utili. Richiede attenzione nella configurazione dei vari passaggi, ma il risultato finale è eccellente.

I telefoni cellulari moderni tuttavia utilizzano la scheda *SIM* unicamente come punto di accesso alla rete, salvando le informazioni utili all'analisi sulla memoria interna e sulle memorie rimovibili. L'analisi delle memorie di massa e rimovibili può essere ricondotta all'analisi di un *hard disk*, e quindi a modalità di *computer forensics* tradizionale.

L'impossibilità di effettuare una copia *bit-per-bit* della memoria del terminale radiomobile resta il problema più difficile da risolvere. Oltre a limitare l'analisi ai soli dati estraibili dal *tool* utilizzato, essa comporta un'intrinseca irripetibilità dell'accertamento tecnico. Non sono infatti note le modalità con cui ogni specifica soluzione interpreta i dati e modifica la memoria del dispositivo. Il percorso è in effetti ripercorribile in altra sede dal punto di vista informatico, ma non ripetibile poiché ogni accesso comporta modifiche.

Le procedure indicate e le considerazioni di carattere generale possono costituire un punto di inizio e linee guida generali da seguire. È tuttavia opportuno che l'esaminatore valuti attentamente la modalità di analisi ed estrazione dei dati, anche in funzione dell'utilizzo probatorio del telefono cellulare.

Ringraziamenti

I compagni del "Corso di perfezionamento in Computer Forensics e Investigazioni Digitali" dell'Università Statale di Milano:

Ennio Costa

Paola Garruto

Paolo Mecca

Leonardo Musumeci

Marco Scarito

per il contributo fondamentale alla stesura di questo articolo e il

Maggiore Marco Mattiucci, Comandante dell'RTI – Reparto Tecnologie Informatiche del RACIS (Arma dei Carabinieri), per la lettura critica e gli importanti spunti di riflessione forniti.

---

[18] F.CASADEI, A.SAVOLDI, P.GUBIAN "Forensics and SIM cards: an Overview" – International Journal of Digital Evidence (Fall 2006, Volume 5, Issue 1)

l'utenza fissa relativa all'abitazione di Stasi Alberto e per l'utenza fissa relativa ad un'agenzia di viaggi la cui sede milanese è risultata tuttavia (da accertamenti richiesti dal collegio peritale) non operativa il giorno 13 agosto 2007 causa chiusura estiva.

Dunque, sulla base di queste valutazioni ed esperiti questi accertamenti il collegio peritale concludeva per l'alta probabilità che l'utenza anonima dalla quale provenivano le chiamate senza risposta ricevute dal cellulare di Chiara Poggi la mattina del 13 agosto 2007 fosse proprio l'utenza fissa relativa all'abitazione di Stasi Alberto.

Tale grado di alta probabilità diventa ragionevole certezza se questi dati vengono combinati con i risultati a cui è giunto il collegio peritale in merito all'attività compiuta da Alberto Stasi quella mattina sul proprio personal computer.

E qui affrontiamo uno dei capitoli più critici dell'intero procedimento.

In data 14 agosto 2007 Stasi Alberto consegnava spontaneamente alla polizia giudiziaria il proprio computer portatile (marca "Compaq").

Da quel momento fino al 29 agosto 2007, quando il reperto informatico veniva consegnato ai consulenti tecnici del pubblico ministero che procedevano all'effettuazione delle copie forensi dello stesso, i carabinieri accedevano ripetutamente e scorrettamente (senza l'utilizzo, cioè delle necessarie tecniche forensi di indagine) alla quasi totalità del contenuto del computer.

Peraltro, già nel verbale di polizia giudiziaria datato 29 agosto 2007 i militari indicavano alcune delle operazioni condotte sul personal computer di Stasi.

In realtà le metodologicamente scorrette attività espletate su tale fonte di prova sono risultate, all'esito dei successivi accertamenti tecnici, ancora più consistenti: sette (e non cinque come riferito) accessi al personal computer di Alberto Stasi; non corretta indicazione dell'avvenuta installazione ed utilizzo di diverse periferiche USB (oltre a quella correttamente indicata); non corretta indicazione dell'avvenuto accesso al disco esterno in uso ad Alberto Stasi; non corretta indicazione di accessi multipli al file della tesi di laurea in vari percorsi di memorizzazione dello stesso: si vedano sul punto i rilievi del collegio peritale tecnico/informatico (ing. Porta e dott. Occhetti).

Il complesso di queste alterazioni veniva rilevato anche dai consulenti tecnici del pubblico ministero (i Ris di Parma) nella loro successiva analisi. Pur tenendo conto di quanto sopra, i Ris, nella loro relazione tecnica e successive integrazioni e chiarimenti, concludevano sostanzialmente nel senso che il giorno 13 agosto 2007 il computer portatile di Alberto Stasi veniva acceso alle ore 9.36; quindi venivano aperte delle fotografie digitali fino alle ore 9.57 e dopo le ore 10.17 non sarebbero presenti tracce informatiche che comportino la presenza attiva di un utente che interagisce con il PC.

Il consulente tecnico della difesa, nel merito, evidenziava che in realtà il file della tesi era stato aperto alle ore 10.17 e che quella mattina erano state ivi scritte e memorizzate due pagine della tesi di laurea. In presenza tuttavia delle alterazioni al contenuto informativo della fonte di prova a causa degli accessi scorretti dei carabinieri e della ritenuta conseguente impossibilità di provare con certezza quanto sopra rilevato, la difesa dell'imputato eccepiva l'inutilizzabilità come fonte di prova del contenuto del computer portatile in parola.

Questo Tribunale respingeva tale eccezione mediante l'ordinanza datata 17 marzo 2009.

Alcune delle questioni colà trattate devono essere qui riassuntivamente richiamate.

Il documento informatico è connotato da un'intrinseca caratteristica di fragilità: nel senso che le tracce elettroniche sono facilmente alterabili, danneggiabili e cancellabili.

Per questa ragione, può essere arduo (e ciò anche a prescindere da ipotetiche manipolazioni dolose ma perfino da eventuali comportamenti colposi posti in essere da chi interviene su di esso) conservare un documento informatico inalterato, in modo da assicurare che la prova sia autentica e genuina.

Di qui la necessità di adottare particolari cautele, quali l'adozione di copie di *hard disk* conformi all'originale, che vengono rese non modificabili mediante appositi procedimenti tecnici.

Al fine di ampliare la possibile valenza dimostrativa della prova informatica (c.d. *digital evidence*) superando alcune incertezze interpretative connesse ad istituti processuali disciplinati dal legislatore prima del consolidarsi sotto il profilo socio/culturale e scientifico dell'era informatica e nel contempo positivizzare questa imprescindibile esigenza (già ben conosciuta nella prassi) legata alla genuina acquisizione del documento informativo e alla successiva attendibile valutazione della prova informatica, la recente legge 18 marzo 2008 n. 48 (in esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica) ha, fra l'altro, modificato la disciplina di alcuni mezzi di ricerca della prova nel senso di estendere espressamente l'oggetto di questi anche ai sistemi informatici e telematici e ha prescritto, nel contempo, la necessità che il soggetto operante adotti idonee cautele tecniche che assicurino la conservazione del documento informatico e ne impediscano l'alterazione. Si veda l'art. 244 cpv c.p.p. in materia di ispezioni; gli artt. 247 e 248 c.p.p. in materia di perquisizioni; gli artt. 254, 254 bis, 256, 259, 260 c.p.p. in materia di sequestri; l'art. 352 c.p.p. in tema di perquisizione nei casi particolari ivi previsti; l'art. 354 c.p.p. in tema di accertamenti urgenti.

A quest'ultimo riguardo, ovvero nel caso di pericolo che le tracce e le cose pertinenti al reato si alterino o si disperdano o comunque si modifichino e il pubblico ministero non possa intervenire tempestivamente ovvero non abbia ancora assunto le indagini, il legislatore ha introdotto la significativa eloquente disposizione: ovvero "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; se del caso, sequestrano il corpo del reato e le cose a questo pertinenti". L'art. 259 comma II c.p.p. prescrive, inoltre, che « quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria".

Ora, nel caso di specie l'attività di polizia giudiziaria presenta caratteristiche di sommarietà e di mera ricognizione di dati potenzialmente utili ai fini della immediata prosecuzione delle indagini tale da non poter essere correttamente inquadrata nell'ambito né della perquisizione, funzionale ad un sequestro che peraltro formalmente non c'è stato in quanto il computer è stato spontaneamente consegnato alla polizia giudiziaria, né dell'ispezione di cui all'art. 244 c.p.p. (in difetto sia dell'elemento formale del decreto autorizzativo sia dell'elemento sostanziale di un'"operazione tecnica" che richiama un concetto di controllo più penetrante e tecnicamente qualificato di quello effettivamente posto in essere).

Correlato a quanto appena evidenziato, bisogna porsi, inoltre, la questione se le operazioni in parola possano, comunque, rientrare nella nozione processual/penalistica di accertamento tecnico ai sensi degli artt. 359/360 c.p.p.. La risposta è negativa.

Infatti, per configurare tale attività come accertamento tecnico ai sensi degli artt. 359 e 360 c.p.p., sarebbe stato necessario che la stessa fosse consistita in un'analisi completa ed approfondita del documento informatico in sequestro sulla base di un quesito posto dal pubblico ministero, che i soggetti procedenti possedessero le competenze tecniche al fine di svolgere gli accertamenti suddetti e che gli stessi alla fine avessero dato conto, mediante argomentata relazione scritta, dei risultati raggiunti.

In realtà, si è trattato di un'attività compiuta da ufficiali di polizia giudiziaria non esperti in materia, che hanno proceduto senza un previo quesito e che al termine hanno redatto solo un verbale in cui hanno riportato la data del compimento dei suddetti indicati atti. Dunque, siamo dinnanzi ad atti di polizia giudiziaria che rientrano, invero, nell'ambito del combinato disposto degli artt. 55 e 348 c.p.p. (attività finalizzata a raccogliere ogni elemento utile alla ricostruzione del fatto e all'individuazione del colpevole) e non integrano la fattispecie dei veri e propri accertamenti tecnici di cui agli artt. 359 e 360 c.p.p..

Ciò posto, non vi è alcun dubbio, tuttavia, che le condotte poste in essere sul computer da parte della polizia giudiziaria, sebbene superficiali, dovessero, proprio per la intrinseca fragilità del contenuto del documento informatico di cui sopra, essere eventualmente svolte (se proprio necessario) con l'assistenza di ausiliari tecnici che avrebbero messo in atto le necessarie preventive cautele tecniche atte ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso provvedendo, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicurasse la conformità della copia all'originale e la sua immodificabilità.

Si deve, dunque, ritenere che questa preliminare e sommaria attività investigativa è stata posta in essere secondo una metodologia sicuramente scorretta, disattendendo i protocolli già invalsi in materia (anche prima dell'entrata in vigore della legge citata) venendo, quindi, a costituire una causa di potenziale alterazione e dispersione del contenuto del documento informatico.

Non emergendo ragioni (e nemmeno la difesa dell'imputato, peraltro, prospettava tale evenienza) per affermare che in tali accessi ed operazioni sommarie da parte della polizia giudiziaria vi fosse stato un dolo di inquinamento probatorio di qualsiasi genere, siamo ragionevolmente di fronte ad errori di metodo compiuti, salva prova contraria, in totale buona fede.

Ciò comporta due conseguenze di fondo.

La prima: la questione se i risultati conseguiti correttamente (secondo il profilo metodologico) dai consulenti del pubblico ministero e della parte civile siano comunque ragionevolmente attendibili (ed in che misura) e/o se alcuni dati ed informazioni siano stati, invece, irrimediabilmente persi a causa, appunto, di tale iniziale errore metodologico da parte della polizia giudiziaria ha una valenza oggettiva. Nel senso che vi è il pericolo (e qui l'eccezione processuale della difesa dell'imputato assume una valenza di merito degna della massima attenzione) che Alberto Stasi non riesca più a provare il proprio alibi che invece, se fossero state salvaguardate al massimo l'integrità e genuinità del documento informatico, sarebbe riuscito per ipotesi a conseguire.

Ma vi è ugualmente il pericolo, all'opposto, che il contestato (dalla difesa dell'imputato) grado di attendibilità del risultato (emerso dalla consulenza tecnico/informatica dei Ris di Parma) sulla falsità dell'alibi offerto dall'imputato (come indizio a carico dello stesso che andrebbe valutato alla luce dell'art. 192 c.p.p.) possa essere (in tutto o in parte) inficiato, appunto, dagli accessi ed operazioni sommarie di cui sopra.

Dunque, una valenza oggettiva, appunto, in quanto emerge, in ultima istanza, il pericolo di un pregiudizio al fondamentale valore neutro dell'accertamento della verità.

Sulla base di queste considerazioni, una volta che l'imputato chiedeva di essere giudicato con le forme del rito abbreviato, affidare ad autorevoli professionisti del settore un accertamento peritale in materia diventava assolutamente necessario ai fini della decisione.

Ebbene, il collegio peritale (ing. Porta e dott. Occhetti) evidenziava che le condotte scorrette di accesso da parte dei carabinieri hanno determinato la sottrazione di contenuto informativo con riferimento al personal computer di Alberto Stasi pari al 73,8% dei files visibili (oltre 56.000) con riscontrati accessi su oltre 39.000 files, interventi di accesso su oltre 1500 files e creazione di oltre 500 files.

Insomma interventi che hanno prodotto effetti devastanti in rapporto all'integrità complessiva dei supporti informatici (in questi termini si esprime il collegio peritale).

Queste alterazioni indotte da una situazione di radicale confusione nella gestione e conservazione di una così rilevante quanto fragile fonte di prova da parte degli inquirenti nella prima fase delle indagini ha comportato, in primo luogo, il più che grave rischio che ulteriori stati di alterazione rimuovessero definitivamente le risultanze conservate ancora nella memoria complessiva del computer. In secondo luogo, gli accessi in questione hanno comunque prodotto degli effetti metastatici rispetto all'esigenza di corretta e complessiva ricostruzione degli eventi temporali e delle attività concernenti l'utilizzo del personal computer portatile nelle giornate del 12 e 13 agosto 2007. Rispetto dunque ad altre questioni probatoriamente rilevanti (come, ad esempio, il movente/occasione dell'omicidio su cui torneremo nel prosieguo) non è più possibile esprimere delle valutazioni certe né in un senso né nell'altro: in questo ambito, il danno irreparabile prodotto dagli inquirenti attiene proprio all'accertamento della verità processuale.

Con riferimento all'alibi informatico, il collegio peritale (ing. Porta e dott. Occhetti) riusciva comunque a ricostruire le attività compiute da Stasi Alberto quella mattina sul proprio computer portatile.

Ciò sulla base dei seguenti passaggi.

I periti avevano a disposizione in primo luogo la versione della tesi di laurea del 12 agosto 2007 alle ore 19.00 quando si verificava un crash del sistema che consentiva di rinvenire i files temporanei che attestano il lavoro pomeridiano alla tesi di laurea. Quindi una versione del 12 agosto alle ore 19.19 acquisita durante le operazioni peritali mediante la produzione di una chiavetta da parte dei consulenti tecnici dell'imputato. Questa versione della tesi riprodotta su tale supporto non presenta, come argomentato dal collegio peritale in udienza, delle anomalie e quindi può essere considerata come una versione della tesi che si colloca attendibilmente fra quella del crash e quella del 14 agosto 2007. Del resto, è ragionevole la condotta di Stasi che, avvenuto il crash, decide di cautelarsi salvando il proprio lavoro su una chiavetta esterna temendo un eventuale successivo disguido (anomalia bloccante che poteva generare ulteriori crash) del sistema operativo.

Infine, la versione della tesi al momento del 14 agosto 2007 quando Stasi Alberto, avendo consegnato agli inquirenti il proprio computer, si presentava presso la caserma chiedendo loro di poter copiare la propria tesi di laurea su una *pen drive*.

Dunque, schematicamente possiamo ricostruire il lavoro alla tesi nelle seguenti fasi: alle ore 19.00 avviene il crash di sistema (sul sistema si cristallizzavano tutti i files temporanei attivi in quel momento non essendo avvenuta una chiusura normale dell'applicativo word), quindi vi è il salvataggio della tesi sulla chiavetta esterna. Da quel momento il sistema rimane praticamente inattivo fino alle ore 21.28 circa quando viene riaperto il file della tesi fino alle ore 21.59; alle ore 22.14 viene ripreso il lavoro alla tesi fino alle 00.10 quando viene chiuso il file di Word e messo in standby il computer.

La circostanza che l'attività sulla tesi di laurea sia stata eseguita anche successivamente al crash era, del resto, stata dimostrata dalla consulenza della parte civile (ing. Reale) che aveva evidenziato per la sera del giorno 12 l'inserimento nel dizionario personalizzato dell'utente informatico di due parole nuove "inerentemente" e "Garbarino".

Dunque, se Stasi aveva lavorato alla tesi anche la sera del giorno 12 era necessario aspettarsi che vi fossero dei files temporanei che attestassero il lavoro della tesi in quel lasso temporale: la circostanza che, invece, gli stessi mancassero era indice inequivocabile di come l'equazione sostenuta dai consulenti tecnici del pubblico ministero -mancanza di files temporanei uguale provata assenza di attività sul computer per la mattina del 13 agosto- fosse logicamente e tecnicamente scorretta.

Partendo da questo dubbio di fondo e tenuto conto della grave anomalia rappresentata dalle alterazioni del contenuto informativo dovute agli accessi dei carabinieri che ben potevano avere determinato la cancellazione delle normali evidenze presenti all'interno del sistema operativo, il collegio peritale (con la collaborazione dei consulenti tecnici delle parti) ricercava delle particolari informazioni che si trovano fuori del sistema operativo (i c.d. metadati).

Questa ricerca dava esito positivo: questi metadati ed il loro contenuto attestano con certezza (e questo è un'evidenza probatoria non contestata dalle parti) l'interazione diretta e sostanzialmente continuativa dell'utente con il computer dalle ore 10.17 fino alle ore 12.20 del giorno 13 agosto.

Dunque, possiamo dire con certezza che Stasi attivava il proprio personal computer alle ore 9.35 ed eseguiva le seguenti operazioni: accedeva al sistema con la digitazione della propria password; quindi alle ore 9.38 (circa) visualizzava una prima immagine di natura erotico/pornografica; alle ore 9.39 (circa) una successiva immagine pornografica; alle ore 9.41 (circa) visualizzava due immagini dello stesso tenore di cui sopra; alle 9.47 (circa) visualizzava un'altra immagine di natura erotico/pornografica. Bisogna precisare che dalle evidenze riscontrate sul registro di windos alle ore

9.50 vengono aperte delle cartelle; quindi alle ore 9.50 visualizzava una nuova immagine di natura erotica/pornografica; alle ore 9.57 visualizzava una nuova immagine di natura erotica/pornografica; alle 10.05 apriva la copertina di un filmato hard e poi utilizzava un programma di modifica delle immagini alle ore 10.07; poi alle 10.17 apriva la tesi.

Da quel momento sono state appunto recuperate le evidenze di un'attività sostanzialmente continua di videoscrittura sulla tesi di laurea dalle ore 10.17 fino alle ore 12.20 (quando il computer veniva messo in *standby* lasciando il file di *word* aperto).

Il collegio peritale ha quindi evidenziato che le informazioni rinvenute consentono di affermare che l'attività svolta sulla tesi è stata progressiva e quindi i salvataggi sono stati eseguiti in presenza di un testo che si è accresciuto progressivamente (la condizione di modifica del file è condizione essenziale per l'esecuzione del salvataggio che altrimenti non avviene): infatti, sia il numero di caratteri che risultano all'interno del documento sia l'andamento delle parole che tende ad aumentare progressivamente ad ogni revisione convergono verso questo risultato (si vedano sul punto i grafici a pag. 54 e 55 della relazione peritale).

Più specificamente possiamo dire che la sera del 12 e la mattina del 13 agosto Alberto Stasi procedeva ad un lavoro sulla sezione della tesi intitolata "credito d'imposta per i redditi prodotti all'estero": lo stesso è consistito in una complessiva scrittura di nuovo testo e in una revisione di parti di testo relative alle parti di testo già scritto, ad esempio con correzione di alcuni termini, introduzione di riferimenti normativi specifici, elaborazioni su dei calcoli effettuati, eliminazione di alcune parti ed aggiunta, appunto, di nuove parti di testo.

Il collegio peritale, facendo uso dei c.d. strumenti informatici di analisi del testo e considerando che il lavoro svolto la sera del giorno 12 e la mattina del giorno 13 è risultato complessivamente omogeneo non evidenziando anomalie di comportamento informatico, concludeva nel senso che "l'introduzione di revisioni specifiche relative in parte a riferimenti temporali e documentali e in parte a riflessioni in materia distribuite in tutto il corpo del testo sono compatibili con un'attività di concreta concentrazione mentale".

Con riferimento, quindi, al rapporto di tali evidenze informatiche con la questione della presenza effettiva di Alberto Stasi nella propria abitazione, bisogna risolvere due questioni.

La prima è relativa alla natura "portatile" del computer in parola e quindi all'ipotesi che tutta o parte dell'attività informatica rilevata il giorno 13 agosto possa essere stata svolta da Stasi in luoghi differenti dalla propria abitazione.

Questa ipotesi è da escludere con ragionevole certezza nel caso concreto.

In primo luogo, la riscontrata difettosità del cavo di alimentazione e le modeste prestazioni della batteria (che consentiva un'autonomia d'uso del personal computer per circa 2 ore) inducono

convergentemente a considerare che il notebook non potesse essere collocato e utilizzato in luoghi non idonei per svolgere attività di significativa durata.

In secondo luogo, alle ore 9.55 Stasi riceveva sul telefono fisso dell'abitazione la chiamata della madre Ligabò Elisabetta della durata di 21 secondi: in concomitanza a tale evento il personal computer è risultato attivo ed in stato d'uso da parte di Stasi (attività di visualizzazione di immagini). Dal quel momento in poi non emergono circostanze che possano far ipotizzare spostamenti significativi del personal computer dalla posizione nella quale era stato collocato: spegnimenti, sospensioni, standby etc… (si veda sul punto la relazione peritale a pag. 100).

In terzo luogo, la sopra rilevata attività continuativa riscontrata sul personal computer fino alle ore 12.20 non permette ragionevolmente di configurare eventi di spostamento dell'elaboratore elettronico rispetto alla posizione nella quale era stato collocato all'atto della sua riattivazione e al momento della ricezione della chiamata telefonica di cui sopra.

La seconda questione attiene all'ipotesi che i tempi associati alle attività informatiche rilevate sul PC portatile in uso all'attuale imputato possano non essere corrispondenti all'ora reale a seguito di un'attività volontaria di alterazione dei riferimenti temporali di sistema (modifica di data ed ora).

A seguito degli accertamenti peritali sul punto, l'unica astratta possibilità fa riferimento all'avvio di un sistema operativo esterno.

Tale ipotesi, tuttavia, è da escludere in concreto con ragionevole certezza.

Come convincentemente argomentato dal collegio peritale, bisogna infatti considerare che l'operazione descritta avrebbe innanzi tutto richiesto capacità e conoscenze informatiche superiori a quelle accertate in capo ad Alberto Stasi.

In secondo luogo, se un'operazione del genere fosse stata realmente condotta, ciò avrebbe implicato due scenari distinti: il primo relativo al fatto che l'operazione sia avvenuta in epoca precedente all'avvio del personal computer in data 13 agosto 2007 (ad esempio nel corso della notte del 13 agosto); il secondo relativo al fatto che l'operazione sia avvenuta la mattina del 13 agosto dopo le ore 9.36.

Questa operazione avrebbe presupposto una necessaria meticolosa sincronizzazione temporale delle diverse attività, viceversa si sarebbero riscontrati sfasamenti di orario all'atto del riavvio del PC. Infatti, per entrambe le ipotesi tutta l'attività di lavoro sarebbe dovuta essere programmata in modo da rispettare le pause di attività informatica indotte dagli eventi esterni all'attività informatica stessa quali le telefonate effettuate e ricevute da Stasi nella mattina del 13 agosto 2007: telefonate che si inseriscano, appunto, perfettamente nella loro tempistica con l'attività di lavoro sulla tesi e con i relativi riscontri di data ed ora rinvenuti sul personal computer.

Infine, come rilevato ancora dal collegio peritale, una attività di questo tipo appare del tutto inverosimile nella sua attuazione anche in considerazione che non vi era modo per Alberto Stasi di verificare il risultato effettivo di una simile alterazione in termini di credibilità e di assenza di tracce informatiche in grado di palesare le alterazioni di orario in quanto nell'ipotesi dell'alterazione "notturna" il PC non poteva più essere avviato per non inficiare e compromettere l'esito dell'alterazione; nell'ipotesi dell'alterazione "mattutina" i tempi con i quali sarebbe stata condotta l'alterazione non consentivano alcuna verifica.

Dunque, non si può che concludere con elevato grado di credibilità razionale che le attività informatiche rinvenute sul PC portatile in uso a Stasi Alberto in data 13 agosto 2007 sono effettivamente corrispondenti all'ora reale e pertanto si sono verificate in corrispondenza degli orari rilevati.

Se combiniamo queste evidenze informatiche con i riscontri telefonici e quindi con la circostanza per cui le telefonate "anonime" si incastrano perfettamente nell'ambito temporale delle rilevate pause nell'attività di scrittura alla tesi di laurea, è ragionevolmente certo -e non più solo altamente probabile alla luce del ragionamento induttivo del collegio peritale sopra esposto- che l'utenza anonima dalla quale provengono le chiamate senza risposta ricevute dal cellulare di Poggi Chiara la mattina del 13 agosto è l'utenza fissa relativa all'abitazione della famiglia Stasi.

Dunque, vi sono evidenze oggettive della permanenza di Alberto Stasi nella propria abitazione dalle ore 9.35 fino alle ore 12.20 con sostanziale continuità; quindi alle ore 12.46; alle ore 13.26 e alle ore 13.30. Dopo tale ora Alberto Stasi dichiarava di essere uscito dalla propria abitazione per verificare le ragioni per le quali la propria fidanzata non aveva risposto alle sue numerose telefonate per tutta il corso della mattina: sul punto, come visto, vi è il riscontro del vicino di casa Riboldi Antonio.

Con riferimento alle dichiarazioni di Alberto Stasi in merito alle attività compiute prima delle ore 9.35 (l'attuale imputato dichiarava di avere messo la prima sveglia alle ore 9.00 e la seconda sveglia alle ore 9.30; di essersi svegliato alle ore 9.00, di avere aperto leggermente la persiana ed acceso la televisione e di essere rimasto a letto sino alle ore 9.30) il collegio peritale, su indicazione di questo Tribunale, provvedeva ad accertare lo stato di impostazione delle funzioni di allarme o "sveglia" eventualmente presenti sul telefono cellulare che era in uso a Stasi Alberto al momento dei fatti e che è stato acquisito, con il consenso di tutte le parti, in data 18 giugno 2009 nell'ambito delle operazioni peritali. Dall'esame è risultato che nell'apposita sezione "sveglia" all'interno delle funzioni di "agenda" o "calendario" è presente l'impostazione di tre allarmi programmati per le ore 9.00, 9.30 e 14.30 per tutti i giorni della settimana; tutti gli allarmi risultavano disabilitati; inoltre era attiva l'opzione accensione automatica che consente l'attivazione degli allarmi a telefono spento qualora quest'ultimi si presentino abilitati.