Giuseppe Vaciago - Tatiana Morosetti

LE INDAGINI INFORMATICHE E LA PROVA DIGITALE

1. Aspetti processuali

1.1. Premesse

La prova digitale e le questioni ad essa sottese, in particolare i metodi e le procedure per l'acquisizione e soprattutto la valenza probatoria ed i parametri di valutazione, hanno sollevato sin dagli inizi, e ancora sollevano, dubbi applicativi e contrasti interpretativi. Certamente la prova digitale, caratterizzata dalla immaterialità, modificabilità e volatilità, presenta agli operatori del diritto problematiche nuove, sia nella fase della individuazione ed acquisizione, sia nella fase della valutazione dell'efficacia probatoria in giudizio.
Una causa delle difficoltà operative che hanno caratterizzato i primi approcci con il nuovo mezzo di prova, può essere sicuramente ricondotta ad una forte carenza normativa: il codice di procedura penale, difatti, nulla prevede in tema. Tuttavia, l'assenza di norme specifiche da sola non giustifica gli *empasse* applicativi, giurisdizionali ed interpretativi che ne sono seguiti[1]. La conoscenza della materia, cioè del mezzo informatico e delle sue principali caratteristiche, unitamente ad una interpretazione aderente ai principi fondamentali ed alle garanzie stabiliti dal codice di procedura penale, possono essere validi strumenti per affrontare un tema così discusso. Un altro elemento che può essere concausa degli attuali dubbi interpretativi è la prolungata assenza di un coordinamento istituzionale ed il mancato consolidarsi all'interno della polizia giudiziaria

[1] Luparia, L., *Diffusione di virus e accesso abusivo a sistemi telematici. Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova penale digitale – I profili processuali*, 2006, pp. 156: «... i princìpi consolidati della teoria processuale possono spesso essere sufficienti per risolvere le questioni connesse al nuovo fenomeno delle indagini informatiche e che, anzi, l'eccessivo scostamento dallo *ius commune iudiciale*, perseguito da chi sostiene la bandiera di una presunta "autonomia sistematica" delle operazioni di *computer forensics*, finisce col provocare pericolose derive tecniciste e fenomeni di aggiramento delle garanzie processuali».

e degli organi inquirenti di uniformi *best practices*[2]*:* sia in materia di disciplina legale della prova digitale, sia per quanto concerne il coordinamento e la formazione degli operatori di polizia giudiziaria, almeno inizialmente l'Italia è rimasta indietro rispetto non solo agli USA, patria della *computer forensics*, ma anche alla maggior parte dei paesi europei.

La versione aggiornata al 2003 del *CSIRT Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries* riportava una situazione poco confortante per l'Italia: la disciplina della *forensics* veniva descritta «still at an early developed stage» (trad. lett. ancora ad uno stadio di sviluppo iniziale), in un panorama complessivo nel quale gli organi giudicanti tendevano spesso a sottovalutare la rilevanza della corretta metodologia dell'acquisizione della prova digitale, focalizzando l'attenzione sul diritto penale sostanziale. Inoltre il *CSIRT Handbook* rilevava come le perquisizioni ed i sequestri fossero ancora elemento di discussione e che fosse prassi sottoporre a sequestro un intero sistema anche nel caso di ricerca di soli dati. Veniva infine segnalato il dibattito circa l'utilizzo di strumenti open source o proprietari per le operazioni di *computer forensics*[3].

L'aggiornamento al 2005 del *CSIRT Handbook* ha modificato i dati riportati per l'Italia: viene ora evidenziato come non vi sia una disciplina specifica in tema di *computer forensics*, essendo applicate le norme generali previste dal codice di procedura penale. Si rileva come, in tema di sequestro, siano stati emessi numerosi provvedimenti, tra cui la sentenza 1778/03 della Corte di cassazione, Sezione III Penale (vd. *infra*, Sequestro probatorio di supporti infor-

---

[2] Il termine è nato nel campo del management; a seconda del contesto le *best practices* possono essere definite come raccolte formalizzate di standard, principi, prassi, esempi, di cui si suggerisce l'utilizzo, sottoposte continuamente a studi, approfondimenti e revisioni. Per approfondimenti: http://en.wikipedia.org/wiki/Best_practice.

[3] Valeri L., Rathmell A., Robinson N., Servida A., *Handbook of Legislative Procedures of Computer and Network Misure in EU Countries - Study for the European Commission Directorate-General Information Society*, 2003. Vedasi anche il sito *EU CSIRT Handbook of Legal Procedure*, http://www.csirt-handbook.org.uk, su cui è disponibile un database online di informazioni riguardanti le normative in materia di *cyber-crimes* nei paesi europei.

matici). Da ultimo si rileva come il principale problema in tema di *computer forensics* sia la valutazione della prova digitale[4].
Esemplificativa dell'iniziale mancanza di punti di riferimento degli operatori e della poca conoscenza della materia, è l'operazione Fidobust del maggio 1994, nota anche all'estero come *Italian Crackdown*, prima operazione investigativa su scala nazionale in tema di violazioni del diritto d'autore e *computer crimes*, per ipotesi di duplicazione abusiva di software, frode informatica, contrabbando e associazione a delinquere. Nel corso delle attività di indagine sono stati effettuati circa un centinaio di perquisizioni e sequestri relativi a nodi appartenenti alla rete amatoriale Fidonet, tra cui hanno ricevuto un'eco mediatica internazionale il sequestro di un mouse, con relativo tappetino, e l'apposizione di sigilli alla camera da letto di un indagato in cui si trovava un computer. Con il ricorso da parte degli indagati all'autorità giudiziaria i sequestri non necessari sono stati successivamente revocati[5].
È negli anni novanta che le forze dell'ordine italiane cominciano a istituire reparti operativi specializzati in *computer crimes* e procedure informatiche. Già nel 1989 era stato istituito in seno alla Direzione Centrale della Polizia Criminale un team di specialisti con compiti di studio e analisi della criminalità legata al settore delle telecomunicazioni, con particolare riguardo alle attività svolte in seno alle grandi associazioni di stampo mafioso. Poco tempo dopo l'operazione Fidobust, nel 1996 viene istituito il *Nucleo Operativo di Polizia delle Telecomunicazioni* (N.O.P.T.), con lo specifico compito di attività di contrasto ai crimini del settore delle telecomunicazioni. Successivamente, con Decreto del ministro dell'Interno del 31 marzo 1998, è stato istituito il *Servizio polizia postale e delle comunicazioni*, al cui interno sono confluiti il N.O.P.T. e la divisione *Polizia Postale e delle Comunicazioni*, creata nel 1981 con la legge di riforma della Polizia di Stato[6]. Nel gennaio 2001 all'interno del Nu-

[4] Valeri L., Somers G., Robinson N., Graux H., Dumortier J., *CSIRT Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries*, 2006.
[5] Per approfondimenti, Coliva D., *Quando sequestrarono i tappetini dei mouse.* In *Interlex*, 2004.
[6] Per approfondimenti, vedere il sito *Servizio polizia postale e delle comunicazioni*, http://www.poliziadistato.it/pds/informatica. Per una panoramica

cleo Speciale Investigativo della Guardia di Finanza è stato istituito il G.A.T. (Gruppo Anticrimine Tecnologico, ora Nucleo Speciale Frodi Telematiche; http://www.gat.gdf.it).
In considerazione della mancanza di norme specifiche in tema di *computer forensics*, assumono particolare rilevanza le decisioni della giurisprudenza, che ha recentemente cominciato ad affrontare alcuni temi legati all'acquisizione ed alla valutazione delle prove digitali. Di seguito procederemo quindi all'esame di alcune recenti pronunce della giurisprudenza di merito.

1.2 Sequestro probatorio di supporti informatici

Il codice di procedura penale prevede tre tipologie di sequestro: probatorio, conservativo, preventivo.
Il sequestro probatorio, disciplinato dagli artt. 253 ss. c.p.p., è un mezzo di ricerca della prova, finalizzato all'accertamento dei fatti. È disposto con decreto motivato dall'autorità giudiziaria e può essere mantenuto sino a quando sussistono le esigenze probatorie e, pertanto, ha come limite massimo il provvedimento conclusivo del procedimento, cui può seguire, eventualmente, la confisca *ex* art. 240 c.p.. Può essere disposto per qualsiasi genere di reato, delitto o contravvenzione. Oggetto del sequestro probatorio possono essere il corpo del reato, cioè le cose sulle quali o mediante le quali il reato è stato commesso, oppure le cose che costituiscono il prodotto, il profitto o il prezzo del reato (*producta sceleris*). In particolare, per prodotto del reato si intendono le cose acquisite a seguito del reato o create da esso; per profitto qualsiasi vantaggio economicamente apprezzabile ricavato dal reato; per prezzo del reato gli eventuali beni o le utilità dati o promessi per la consumazione del reato. Oltre al corpo del reato, sono sequestrabili le cose pertinenti al reato necessarie per l'accertamento dei fatti. In tale nozione vengono incluse le cose che servono, anche in via indiretta, ad accertare il reato, quindi la condotta, l'evento, l'autore e le circostanze.

---

sulle modalità di indagine e sugli strumenti utilizzati dalla Polizia Postale, vedasi Ninni F., *Giudice penale e giudice minorile di fronte all'abuso sessuale*, 2001, p. 4 ss.

Il sequestro conservativo (artt. 317 ss. c.p.p.) e preventivo (artt. 321 ss. c.p.p.) si distinguono dal sequestro probatorio in quanto sono misure cautelari reali[7]: anche tali misure impongono un vincolo sulla disponibilità delle cose mobili o immobili ma con finalità diverse da quelle di indagine e, come il sequestro probatorio, sono applicabili per qualsiasi titolo di reato. Il sequestro conservativo ha lo scopo di assicurare l'adempimento delle obbligazioni relative alle pene pecuniarie, alle spese processuali ed alle obbligazioni civili derivanti dal reato. Può essere richiesto dal P.M. o dalla parte civile, solo nei confronti dell'imputato o del responsabile civile e, pertanto, non è esperibile nei confronti della persona sottoposta ad indagini preliminari. Il sequestro preventivo, invece, è disposto dal giudice su richiesta del P.M. quando vi è pericolo che la disponibilità di una cosa pertinente al reato possa aggravare o protrarre le conseguenze del reato o agevolare la commissione di altri reati; inoltre è disposto sulle cose di cui è consentita la confisca. Per quel che qui rileva, è bene tenere presente che l'art. 171-*sexies* L. 633/1941 prevede che sia «sempre ordinata la confisca degli strumenti e dei materiali serviti o destinati a commettere i reati di cui agli articoli 171-*bis*, 171-ter e 171-*quater*», anche nel caso di applicazione della pena su richiesta delle parti *ex* art. 444 c.p.p. (patteggiamento).

Nella casistica dei sequestri di materiale informatico sono sorti dubbi interpretativi soprattutto rispetto al sequestro probatorio: in particolare, riguardo la qualifica (corpo del reato oppure cosa pertinente al reato) di un computer sottoposto a sequestro, riguardo la necessità di acquisire il supporto informatico o il solo dato utile alle indagini mediante procedimento di copia sicura o *bit stream*[8] e, ancora, riguardo l'opportunità di porre sotto sequestro materiale

[7] Per approfondimenti sulle misure cautelari, Tonini P., *Lineamenti di Diritto Processuale Penale*, Cap. VI, Le misure cautelari, pp. 190-218, 2005.

[8] Attraverso tale procedimento si realizza una "copia-immagine" del supporto originale, ossia una replica esatta ed identica, bit per bit, che riproduce anche le informazioni precedentemente cancellate e non sovrascritte contenute all'interno dello spazio non allocato di un file system (dati che non verrebbero copiati tali quali nel corso di un semplice processo di duplicazione dei file). La copia *bit stream* è unanimemente ritenuta uno strumento fondamentale ed imprescindibile per le procedure di acquisizione ed analisi di dati informatici.

ulteriore rispetto al supporto dei dati (scheda grafica, mouse, stampanti, etc.).
Con riferimento al primo problema, cioè la qualifica dell'oggetto di sequestro probatorio, a seconda dei casi e delle necessità di indagine un mezzo informatico può essere qualificato come corpo del reato, cioè quale mezzo attraverso il quale viene consumata l'azione criminosa (ad esempio, nel caso di *file sharing,* di invio di e-mail diffamatorie, etc.) oppure come cosa pertinente al reato, attraverso la cui analisi possono essere ricavati elementi di prova (ad esempio, nel caso in cui tra i file del computer vi siano i piani di una rapina, la corrispondenza dell'indagato, etc.). La differente qualificazione di corpo del reato oppure di cosa pertinente al reato rileva soprattutto con riferimento ai presupposti del vincolo e alla possibilità di revoca del sequestro. Difatti, in caso di sequestro probatorio del corpo del reato, la Pubblica Accusa dovrà semplicemente qualificare correttamente il bene oggetto di sequestro quale corpo del reato, senza dover ulteriormente dimostrare la necessità del sequestro in funzione dell'accertamento dei fatti, in quanto l'esigenza probatoria che giustifica il vincolo sulla cosa corpo del reato è «*in re ipsa*, onde il decreto di sequestro è sempre legittimo quando abbia ad oggetto cose qualificabili come corpo di reato, essendo necessario e sufficiente, a tal fine, che risulti giustificata detta qualificazione»[9]. La qualificazione di corpo del reato, però, dovrà essere corretta e giustificata: sempre secondo l'interpretazione della cassazione, il provvedimento di sequestro «deve dare concretamente conto della relazione di immediatezza tra la "res" e l'illecito penale»[10]. Diversamente, il provvedimento di sequestro di cose pertinenti al reato deve essere a pena di nullità specificamente ed adeguatamente motivato in relazione alle esigenze probatorie, che costituiscono il presupposto del vincolo[11].
Con riferimento al secondo ed al terzo problema, cioè alla necessità di sottoporre a sequestro il supporto informatico o i soli dati rilevanti ai fini investigativi mediante copia *bit stream* ed ai limiti del sequestro in relazione al materiale ulteriore rispetto al supporto dei dati, in mancanza di norme specifiche in tema assumono particola-

[9] Cassazione, Sezione VI Penale, Sentenza 5 marzo 1998, n. 337, in tema di sequestro di un computer.
[10] Cassazione, Sezione VI penale, 16 marzo 1998, n. 103.
[11] Cassazione, Sezione VI Penale, 8 gennaio 2003, n. 74.

re rilevanza le decisioni della giurisprudenza, tra cui si segnala la sentenza n. 1778 della Corte di cassazione, Sezione III Penale, del 18 novembre 2003. La sentenza aveva ad oggetto il ricorso verso una ordinanza emessa dal Tribunale del riesame[12] di Siracusa in relazione al sequestro probatorio di «vario materiale informatico (tra cui un P.C., una stampante, uno scanner, n. 33 CD)» in un procedimento relativo al reato di detenzione di materiale pedopornografico (art. 600-*ter* c.p.). L'ordinanza del Tribunale del riesame aveva rigettato la richiesta dell'indagato di restituzione del materiale sequestrato, ritenendo che i beni informatici oggetto di sequestro fossero qualificabili come cose pertinenti al reato. Tra i motivi di ricorso in cassazione, l'indagato ha lamentato l'inosservanza e/o erronea applicazione di legge penale, in quanto i beni sequestrati non costituirebbero «cose pertinenti al reato utili ai fini di ulteriori accertamenti e soggetti a confisca». La Suprema Corte ha dichiarato fondato questo motivo di ricorso affermando che, poiché il sequestro probatorio aveva ad oggetto beni ritenuti cose pertinenti al reato e non semplicemente il corpo del reato, il Tribunale del riesame avrebbe dovuto controllare se il sequestro fosse giustificato ai sensi dell'art. 253 c.p.p. e, cioè, avrebbe dovuto verificare la sussistenza delle finalità probatorie. Tuttavia, secondo la cassazione, il Tribunale del riesame non ha effettuato tale verifica ma ha semplicemente ritenuto non restituibili i beni perché utili ai fini di ulteriori accertamenti senza specificare quali e senza motivare in alcun modo. Poiché era stato sequestrato anche materiale informatico definito «del tutto "neutro" rispetto alle indagini in corso (quale, ad esempio, stampante, scanner, schermo)» e che non erano state indicate le esigenze probatorie a giustificazione del vincolo, la Corte ha annullato l'ordinanza del Tribunale del riesame perché illegittima, specificando che in questo caso la prova poteva essere assicurata «limitando il sequestro alla memoria fissa del computer o ad eventuali supporti (floppy, CD) contenenti elementi utili alle indagini».

[12] Il Tribunale del riesame, o anche Tribunale delle libertà, è competente a decidere sulle impugnazioni (riesame o appello) nei confronti delle decisioni in materia di misure cautelari (vd. artt. 309 ss. c.p.p. per le misure cautelari personali e artt. 322, 322-bis, 324 c.p.p. per le misure cautelari reali).

L'impostazione della cassazione non è però stata ancora pienamente recepita dalla giurisprudenza di merito, come dimostra l'ordinanza del Tribunale del riesame di Venezia n. 62 del 31 marzo 2005. Il Tribunale ha rigettato il riesame proposto dall'indagato verso il decreto di sequestro probatorio emesso dal P.M. in relazione al reato di divulgazione di materiale pedopornografico di cui all'art. 600-*ter* co. 3 c.p., che punisce chiunque distribuisca, divulghi o pubblicizzi, con qualsiasi mezzo, anche in via telematica, materiale pedopornografico o notizie finalizzate all'adescamento o alla sfruttamento sessuale di minori. Con il provvedimento del P.M. era stata disposta la perquisizione locale dell'abitazione dell'indagato, cui era seguito il sequestro probatorio del personal computer, delle periferiche e dei relativi supporti, ritenuti necessari ai fini della prova. Tre le argomentazioni a sostegno del ricorso al Tribunale del riesame: innanzitutto, il computer sequestrato sarebbe stato acquistato in epoca successiva ai fatti contestati e quindi non avrebbe potuto essere considerato corpo di reato, cioè mezzo o strumento di commissione del reato. Inoltre l'indagato ha contestato la sussistenza del reato poiché l'impiego dei programmi di *file sharing* non concretizzerebbe il concetto di divulgazione richiesto dall'art. 600-*ter* co. 3 c.p. ed infine ha contestato la sussistenza della finalità probatoria del sequestro esteso a componenti ulteriori rispetto all'hard disk, con richiesta di limitare il sequestro solo rispetto a questo.
Il Tribunale del riesame ha rigettato le tesi della difesa: in primo luogo ha ritenuto che i programmi di *file sharing* siano uno strumento di divulgazione che si rivolge ad un numero indefinito di destinatari integrante la condotta di cui all'art. 600-*ter* co. 3 c.p. Inoltre, il Tribunale non ha ritenuto decisivo lo scontrino fiscale con data successiva al reato prodotto dall'indagato, poiché non poteva essere ricondotto esclusivamente e senza alcun dubbio al computer posto sotto sequestro e ritenendo che questo era stato comunque utilizzato per la realizzazione del reato dato che su di esso erano state comunque "riversate" le immagini pedopornografiche rinvenute. Infine, il Tribunale ha rigettato la richiesta di limitare il sequestro al solo hard disk, ritenendo che, se da un lato il quadro probatorio raggiunto permettesse di ritenere sussistenti gravi indizi di colpevolezza circa il reato contestato, dall'altro lato, il quadro probatorio stesso fosse incompleto e che fosse quindi necessario

«ricostruire con esattezza la dimensione, frequenza e durata dell'attività delittuosa». A tal fine, il Tribunale ha rigettato la richiesta restituzione parziale del materiale sequestrato, definita prematura, ritenendo necessario «un approfondito esame tecnico della strumentazione informatica [...] non potendosi escludere che la disponibilità di tutto il materiale sequestrato possa consentire, o comunque facilitare, operazioni tecniche più complesse quali, ad esempio, la ricerca di tracce file già scaricati e, successivamente, cancellati».
L'omessa specificazione da parte del Tribunale del riesame delle finalità riconducibili al vincolo sui singoli componenti ulteriori rispetto all'hard disk non consente di valutare a fondo le motivazioni dell'argomentazione, anche se ben difficilmente è ipotizzabile che tali oggetti possano effettivamente apportare elementi utili di indagine. Non vi può essere dubbio sul fatto che la limitazione del sequestro al solo hard disk (o l'acquisizione di una copia *bit stream* dello stesso) avrebbe sicuramente potuto soddisfare le esigenze poste a fondamento del provvedimento di rigetto e, cioè, la ricostruzione «con esattezza della dimensione, frequenza e durata dell'attività delittuosa». Il Tribunale ha indicato, ad esemplificazione delle ulteriori analisi, la ricerca di tracce di file cancellati, che, tuttavia, può essere tranquillamente assicurata con la limitazione del sequestro del solo hard disk, come richiesto dall'indagato, o anche con l'acquisizione di copia *bit stream*.

1.3 La tutela della integrità e della genuinità della prova digitale

I provvedimenti emessi dal Tribunale di Bologna, di Chieti e di Pescara sono le prime, recenti, applicazioni giurisprudenziali di merito in tema di valutazione della integrità e genuinità delle prove digitali e di utilizzabilità delle stesse ai fini dell'accertamento di fatti costituenti reato.

1.3.1 L'aderenza ai protocolli scientifici

La prima sentenza in ordine cronologico è stata emessa dal Tribunale di Bologna, Sezione I Penale, in data 21 luglio 2005 (dep. 22 dicembre 2005), nel procedimento comunemente noto con il no-

me del virus diffuso in rete nel marzo 2001, Vierika[13]. Il procedimento vedeva imputati due fratelli per i reati di cui agli artt. 110, 615-*ter*, 615-*quinquies* e 81 cpv. c.p. «poiché, in concorso tra loro, creando un "virus" (programma atto a danneggiare sistemi informatici) denominato vierika trasmesso in via informatica al provider "Tiscali" e tramite questo a circa 900 utilizzatori del provider, si introducevano nei sistemi informatici di tali utenti e acquisivano dati anche riservati contenuti nei loro personal computers - tra i quali indirizzari e-mail - a loro insaputa, inoltre per mezzo del virus danneggiavano i programmi contenuti nei personal computers raggiunti e ne pregiudicavano il corretto funzionamento». Per quanto concerne i dettagli tecnici del funzionamento del virus, ampiamente descritti nella sentenza, Vierika è un *worm* realizzato in Visual Basic, i cui effetti derivano dalla interazione di due script differenti, programmato per colpire i sistemi Windows 95 o 98 con installato il software Outlook Professional. Il primo script (Vierika.JPG.vbs) è allegato ad un e-mail con oggetto "Vierika is here" e testo del messaggio "Vierika.jpg". Si legge nella motivazione della sentenza che «una volta eseguito, il programma agisce sul registro di configurazione di Windows, abbassando al livello minimo le impostazioni di protezione del browser Internet Explorer ed inserendo come home page del predetto browser la pagina web http://web.tiscalinet.it/krivojrog/vierika/Vindex.html. Il secondo script in Visual Basic, di dimensioni maggiori, è contenuto nel documento html Vindex.html, e si attiva quando l'utente, collegandosi ad Internet, viene automaticamente indirizzato dal browser sulla nuova home page sopra indicata: il basso livello di protezione impostato dalla prima parte del codice, permette l'automatica esecuzione dello script contenuto nel documento html. L'effetto di questo secondo script è quello di creare nella prima partizione del primo disco rigido del computer il file c:\Vierika.JPG.vbs, contenente la prima parte del codice, e di produrre un effetto di mass-mailing, inviando agli indirizzi contenuti nella rubrica di Outlook una e-mail contenente l'attachment sopra descritto, in modo tale che il programma Vierika si autoreplichi».

[13] Il testo della Sentenza è reperibile in Rete sul sito *Penale.it, Diritto, procedura e pratica penale,* all'indirizzo http://www.penale.it/page.asp?mode=1&IDPag=182.

A seguito dell'istruzione dibattimentale, esclusa qualsiasi partecipazione nel reato dell'imputato C.S. (il fratello C.G. si è infatti assunto l'esclusiva responsabilità dei fatti contestati e l'unico indizio a carico del C.S. era l'intestazione delle utenze telefoniche usate per le connessioni) il Tribunale ha condannato il solo C.G., noto con il nome utilizzato in rete, Krivoj Rog, in relazione ad entrambi i reati di accesso abusivo e diffusione di programmi diretti a danneggiare un sistema informatico[14].

Queste le fonti di prova acquisite agli atti e su cui si è basata la decisione del Giudice: verbali di perquisizione e sequestro presso l'abitazione dei due imputati; verbale di acquisizione di tracce telematiche presso Infostrada S.p.A.; documento telefax di Infostrada S.p.A. relativo alla amministrazione dello spazio web digilander.iol.it/vierika/index.html; verbale di esibizione e sequestro eseguito presso Tiscali S.p.A.; comunicazione e-mail proveniente da Tiscali S.p.A. relativa all'amministrazione del sito web.tiscalinet.it/krivojrog/vierika/Vindex.html; annotazioni di polizia giudiziaria; testimonianze di operatori di polizia giudiziaria che hanno svolto le indagini nonché di dipendenti dei due provider; verbale di interrogatorio dell'imputato.

Le indagini sono state effettuate dalla Guardia di Finanza di Milano che, dopo aver ricevuto un e-mail contenente il primo script del programma, ha individuato due siti web aventi nell'url la parola Vierika, uno sul server della società Tiscali S.p.A. e contenente il secondo script, il secondo sul server della società Infostrada S.p.A., sul quale lo script non è stato rinvenuto. Successivamente, sono stati eseguiti due decreti di esibizione e sequestro delle tracce telematiche relativi ai due siti dei provider Tiscali e Infostrada. Dai dati forniti da Tiscali S.p.A. risultavano alcuni interventi di gestione del sito ad opera dell'utente con username krivoj, registrato presso il provider con i dati dell'imputato C.G. e che si connetteva mediante una linea telefonica intestata al fratello C.S. Dai dati forniti da Infostrada S.p.A. risultavano degli interventi sul sito digilander.iol.it/vierika/index.html, sempre da parte dell'utente con username krivoj, registrato anche presso questo provider con i dati di C.G. e sempre attraverso l'utenza telefonica intestata al fratello.

[14] Per un approfondimento sui reati di accesso abusivo e detenzione di codici, vedi *infra*.

La Guardia di Finanza ha quindi eseguito una perquisizione presso l'abitazione dei due fratelli, nel corso della quale C.G. ha indicato agli operanti i file relativi al programma Vierika contenuti nell'hard disk di un proprio computer e, sotto il controllo di questi, ne ha masterizzato copia, che è stata sottoposta a sequestro.
Nel corso del processo, la difesa dell'imputato ha contestato l'utilizzabilità degli elementi probatori, mettendo in dubbio sia il metodo attraverso il quale è stato individuato l'amministratore degli spazi web su cui era ospitato il secondo script del programma Vierika, sia il metodo utilizzato dalla polizia giudiziaria per l'acquisizione dei dati dal computer dell'imputato, evidentemente difformi dai protocolli scientifici e ritenute inidonei a garantire l'effettivo contraddittorio all'imputato, anche in considerazione della ritenuta irripetibilità delle operazioni di indagine. A sostegno della propria tesi, ha prodotto le Linee Guida IACIS®, che sono state per quella che risulta essere la prima volta acquisite agli atti in un procedimento penale.
Inoltre, per quel che qui può rilevare, la difesa ha sostenuto la non offensività del programma: secondo lo stesso imputato, infatti, si trattava di un software non invasivo o distruttivo, programmato per motivi di studio.
Il Tribunale ha ritenuto che la contestazione della difesa circa il metodo di acquisizione non avesse concreta rilevanza, non avendo la difesa prodotto alcuna prova di alterazioni concrete sui dati acquisiti, affermando che «non è compito di questo Tribunale determinare un protocollo relativo alla procedure informatiche forensi, ma semmai verificare se il metodo utilizzato dalla p.g. nel caso in esame abbia concretamente alterato alcuni dei dati ricercati». Poiché la difesa dell'imputato si sarebbe limitata a contestare la correttezza dei dati acquisiti, senza allegare elementi che dimostrassero che vi fosse stata, o potesse essersi verificata, una alterazione dei dati, il Giudice ha escluso che tali dati fossero inutilizzabili: al contrario, ha stabilito che i dati erano liberamente valutabili alla luce del contesto probatorio complessivo per il principio del libero convincimento, di cui all'art. 192 c.p.p. Partendo da tale presupposto, il Giudice ha ritenuto che gli accertamenti e le acquisizioni compiuti dalla polizia giudiziaria fossero da considerare pienamente attendibili ed utilizzabili ai fini della decisione. Inoltre, ha ritenuto di non accogliere la richiesta della difesa di eseguire una perizia sul

funzionamento del programma ai sensi dell'art. 220 c.p.p., ritenuta non necessaria poiché gli operatori di polizia giudiziaria sentiti in dibattimento per esplicare il funzionamento del programma «avevano le competenze tecniche necessarie per la decifrazione del codice» ed inoltre poiché la difesa non avrebbe in sostanza contestato il funzionamento del programma.

Prescindendo in questa sede dalle valutazioni sulla decisione del Giudice in merito al dibattito sulla cogenza della perizia, è interessante sottolineare come la decisione sembra introdurre nel sistema processuale una inversione dell'onere probatorio, come si evidenza nella massima della sentenza: «dal compimento di investigazioni informatiche che si discostano dalla migliore pratica scientifica non discende un'automatica inutilizzabilità del materiale probatorio raccolto. Spetta infatti alla difesa l'onere di dimostrare in che modo la metodologia utilizzata ha concretamente alterato i dati ottenuti»[15].

La decisione, se anche può apparire corretta nel caso concreto, in cui peraltro l'imputato aveva ammesso in sede di interrogatorio la paternità del programma Vierika, non può andare esente da critiche. Difatti, l'ordinamento processuale prevede che l'onore probatorio sia a carico dell'accusa, la quale deve dimostrare i presupposti oggettivi e soggettivi del reato oggetto di contestazione e l'affermazione del Giudice sembra effettuare una inversione di tale principio[16].

Oltre al fatto che la decisione sembra invertire l'onere della prova, l'elemento che qui maggiormente rileva è la metodologia di indagine utilizzata per gli accertamenti effettuati dalla polizia giudiziaria presso l'abitazione dell'indagato. Difatti, nel corso della perquisizione, rinvenuti elementi utili ai fini delle indagini consistenti nel codice del programma, peraltro indicato dallo stesso indagato, questi sono stati acquisiti mediante copia dei file sul computer dell'indagato attraverso una procedura di masterizzazione effettuata dallo stesso indagato con i propri strumenti hardware e software. Una simile procedura, oltre a discostarsi dai principi internazionalmente riconosciuti per l'acquisizione di dati digitali, produce, in

[15] Per approfondimenti, Luparia L., *Diffusione di virus e accesso abusivo a sistemi telematici. Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova penale digitale*, cit.

[16] Luparia L., *ibidem*, p. 158.

linea di massima, un risultato non ripetibile[17]. Secondo il codice, un accertamento è irripetibile e, quindi, necessita di particolari procedure espressamente codificate, se riguarda situazioni modificabili nel tempo, come ad esempio, nel caso di rilievi da effettuare in seguito ad incidente stradale, rilievi autoptici, esami di sostanze che ne comportino la totale distruzione, etc.[18] L'acquisizione così effettuata si colloca al di fuori di qualsiasi protocollo scientifico ed è inidonea ad assicurare l'integrità e la genuinità delle prove raccolte, secondo i principi delle *best practices* in materia, ove è posta particolare attenzione soprattutto in relazione alle fasi di acquisizione e conservazione dei dati digitali[19].

In casi simili, quando cioè sia necessaria una limitata analisi di dati (come anche, ad esempio, in caso di virus, *dialer*, diffamazione o ingiuria), è ipotizzabile, a seconda dei presupposti di fatto, il ricorso ai seguenti istituti previsti dal codice di procedura penale:

- ispezione del P.M. *ex* artt. 244 ss. e 364 c.p.p. o ispezione delegata *ex* artt. 244 ss. c.p.p., con acquisizione di copia *bit stream* e operazione di *hashing*. L'operazione di hashing serve a generare una sorta di marchio digitale o impronta che contraddistingue univocamente il dato informatico e ne garantisce l'integrità; consiste nell'applicazione di un formula matematica (algoritmo del tipo "funzione di hash") al supporto originale e alla copia: i valori dei due calcoli coincidono solo se vi è assoluta rispondenza tra l'originale e la copia[20]. L'ispezione *ex* art. 246 c.p.p. è un particolare mezzo di ricerca della prova, disposto con decreto motivato dell'autorità giudiziaria, finalizzato all'esame di luoghi o cose allo scopo di accertare le tracce e gli altri effetti materiali del reato. L'interessato ha la facoltà di far-

[17] La sola procedura di accensione di un sistema Microsoft Windows produce numerose modifiche.

[18] Per approfondimenti sul concetto di irripetibilità, vedasi Corte di cassazione, Sezioni Unite Penali, Sentenza 17 ottobre – 18 dicembre 2006 n. 41281, in *Guida al Diritto*, n. 2 (2007), pp. 78 ss.

[19] Costabile G., *Scena criminis, documento informatico e formazione della prova penale,* 2004.

[20] Per una definizione di *hashing*, vedere http://it.wikipedia.org/wiki/Hash. Per approfondimenti sulla crittografia, della nascita della firma digitale e della funzione di *hash*, Levy S., *CRYPTO I ribelli del codice in difesa della privacy*, 2002.

si assistere da persona di fiducia che sia prontamente reperibile. Per l'applicazione di questo mezzo di ricerca della prova in tema di tracce digitali, sono ovviamente richieste specifiche competenze tecniche e la disponibilità di idonei strumenti informatici, perché l'acquisizione richiede l'utilizzo delle particolari metodologie della copia *bit stream* e dell'operazione di *hashing*. L'ispezione è caratterizzata dalla irripetibilità e quindi gli eventuali elementi probatori acquisiti sono pienamente utilizzabili in dibattimento, sempre che siano stati utilizzati metodi di acquisizione idonei a garantire l'integrità e la genuinità dei dati. I requisiti tecnici, unitamente al limitato ambito di applicazione (l'ispezione, ad esempio, non è uno strumento opportuno per svolgere analisi di un certo rilievo, anche solo dal punto di vista quantitativo dei dati), determinano lo scarso utilizzo dell'ispezione come mezzo di ricerca della prova in ambito digitale.

- Accertamenti urgenti *ex* art. 354 c.p.p.: gli ufficiali e gli agenti di polizia giudiziaria hanno il compito e il potere di curare 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: in caso di pericolo di alterazione o dispersione o modificazione delle tracce, cose o luoghi, possono compiere necessari accertamenti e rilievi, procedendo se del caso al sequestro del corpo del reato e delle cose a questo pertinenti. Anche in questo caso si presentano problemi relativi alle competenze tecniche ed alla strumentazione richieste.
- Sequestro del supporto e successiva analisi in laboratorio mediante accertamento tecnico, che può essere, a seconda dei casi, caratterizzato o meno dalla ripetibilità. Ad esempio, può essere assicurata la ripetibilità di un accertamento su un hard disk procedendo alla creazione di copie *bit stream* e lavorando su di esse. Nel caso in cui l'accertamento tecnico sia caratterizzato dalla non ripetibilità è previsto necessariamente il contraddittorio con l'indagato e l'eventuale persona offesa dal reato, che hanno la facoltà di nominare propri consulenti tecnici (art. 360 c.p.p.). L'accertamento tecnico non ripetibile è caratterizzato dalla piena utilizzabilità in dibattimento delle risultanze.

1.3.2 Acquisizione dei file di log

La seconda sentenza in ordine di tempo in tema di valenza probatoria della *digital evidence* è stata emessa dal Tribunale di Chieti in data 2 marzo 2006 e depositata in data 30 maggio 2006. Il procedimento, relativo ad una imputazione per il reato di detenzione e diffusione abusiva di codici di accesso a sistemi informatici di cui all'art. 615-*quater* c.p., si è concluso con l'assoluzione dell'imputato ai sensi del secondo comma dell'art. 530 c.p.p., per mancanza, insufficienza o contraddittorietà della prova.
Il reato di detenzione e diffusione abusiva di codici di accesso è stato introdotto dalla Legge 23 dicembre 1993 n. 547, *Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*, che, oltre ad avere fornito la prima definizione nel nostro ordinamento di documento informatico, ha modificato il codice penale prevedendo nuovi reati, suddivisibili in tre tipologie[21]:

1. reati che prevedono una condotta di danneggiamento di hardware o software (artt. 392, 420, 635-*bis*);
2. reati che prevedono una condotta di intrusione illegittima nell'ambito del "domicilio" e dei segreti informatici altrui (artt. 615-*ter*, 615-*quater*, 615-*quinquies*, 617-*bis*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 621, 623-*bis*);
3. reati che prevedono una condotta di alterazione del funzionamento di hardware e software finalizzata ad acquisire un ingiusto profitto con altrui danno (art. 640-*ter*).

L'art. 4 della L. 547/1993, in particolare, ha introdotto i reati di cui agli artt. 615-*ter*, 615-*quater* e 615-*quinquies* nel Titolo XII, *Dei delitti contro la persona* – Sezione IV, *Dei delitti contro la inviolabilità del domicilio*, del codice penale. Il primo dei tre reati, l'accesso abusivo ad un sistema informatico o telematico, punisce non solo chi si introduce abusivamente in un sistema informatico o telematico, ma anche chi vi si mantiene contro la volontà esplicita o tacita di chi ha il diritto di escluderlo. È stato rilevato sia dalla dottrina sia dalla giurisprudenza come in tal modo sia stato configurato per i

[21] Scuto S., De Riso A., *I reati su sistemi informatici: accesso abusivo a sistema informatico e frode informatica*, 2005, p. 73.

sistemi informatici un sistema di protezione analoga a quella del domicilio, tanto da ravvisare una tutela del *domicilio informatico*. In particolare, la Corte di cassazione ha affermato che «l'oggetto della tutela del reato di cui all'art. 615-*ter* c.p. è costituito dal cd. domicilio informatico, da intendersi come spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona, il quale deve essere salvaguardato al fine di impedire non solo la violazione della riservatezza della vita privata, ma qualsiasi tipo di intrusione anche se relativa a profili economico-patrimoniali dei dati»[22]; e che il reato di violazione di domicilio «è stato notoriamente il modello di questa nuova fattispecie penale, tanto da indurre molti a individuarvi, talora anche criticamente, la tutela di un "domicilio informatico"»[23]. I reati di cui agli artt. 615-*quater*, detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, e 615-*quinquies*, diffusione di programmi diretti a danneggiare o interrompere un sistema informatico, sono strettamente correlati al reato di accesso abusivo. Ad esempio, il reato di detenzione e diffusione abusiva di codici di accesso prevede una condotta spesso precedente quella di accesso abusivo. Si tratta di una fattispecie di reato a dolo specifico, in quanto è richiesto che l'agente abbia lo scopo di procurare un profitto per sé od altri o di arrecare un danno a terzi.

Nel caso della sentenza emessa dal Tribunale di Chieti, secondo la prospettazione dell'accusa, l'imputato, per procurarsi un profitto, sarebbe entrato in possesso e avrebbe detenuto abusivamente due codici di accesso al sistema informatico dell'Internet Service provider Technorail S.r.l., meglio nota come Aruba[24].

L'istruzione dibattimentale si è potuta fondare unicamente su quanto riferito dagli operanti di polizia giudiziaria riguardo le operazioni e gli accertamenti compiuti presso la società parte offesa, poiché nel corso del procedimento è stata dichiarata la nullità di un atto di perquisizione e del conseguente sequestro compiuti in fase di indagini. In particolare, i testi dell'accusa hanno riferito in giudizio circa le operazioni di acquisizione, mediante semplice consegna

[22] Cassazione, Sezione VI Penale, 4.10.1999 n. 3065

[23] Cassazione, Sezione V Penale, Sentenza 6.12.2000, n. 12732

[24] Il testo della sentenza è reperibile sul sito *Ictlex,* all'indirizzo http://www.ictlex.net/index.php/2006/05/30/trib-chieti-sent-n-17505.

da parte della parte offesa, dei file di log relativi ai codici che l'imputato avrebbe detenuto illegittimamente. A seguito di accertamenti, uno dei codici era risultato acquistato regolarmente dall'imputato, mentre l'altro sarebbe risultato di proprietà della società. Tuttavia il Giudice ha ritenuto le prove non sufficienti ad accertare pienamente la responsabilità penale dell'imputato: l'assoluzione è stata disposta, su richiesta dallo stesso Pubblico Ministero, per insufficienza del quadro probatorio, definito «alquanto equivoco» dallo stesso giudice, che ha rilevato come «il dato acquisito sia minimo e del tutto insufficiente a fondare qualsivoglia affermazione di responsabilità al di là del ragionevole dubbio». In particolare, secondo il Tribunale, le indagini non sarebbero state sufficientemente approfondite, «poiché ci si limitò ad interpellare la ditta senza alcuna formale acquisizione di dati e senza alcuna verifica circa le modalità della conservazione degli stessi allo scopo di assicurarne la genuinità e l'attendibilità nel tempo». Pertanto, il Tribunale ha ritenuto che mancassero le garanzie di genuinità ed integrità dei file di log acquisiti, definiti nella sentenza «dati tecnici di particolare delicatezza e manipolabilità», provenienti inoltre dalla stessa persona offesa e quindi da vagliare in modo ancor più rigoroso[25].

1.3.3 Acquisizione di pagine web

L'impostazione del Tribunale di Chieti è stata recentemente confermata dal Tribunale di Pescara, con sentenza n. 1369/2006 emessa in data 6 ottobre 2006 e depositata in data 3 novembre 2006[26]. Il procedimento riguardava il reato di pubblicazioni e spettacoli osceni (art. 528 c.p.): l'imputato era accusato «perché attraverso apposita strumentazione informatica, server, che permettendo il reindirizzamento al sito Internet denominato www.vallecupa.com, metteva in circolazione immagini oscene ed,

[25] Per approfondimenti, si veda il commento, critico verso la decisione del Tribunale di Chieti, di Cajani F., *Alla ricerca del log (perduto)*, 2006, pp. 573 ss.

[26] Il testo della sentenza è reperibile sul sito *Ictlex*, all'indirizzo http://www.ictlex.net/index.php/2006/11/03/trib-pescara-sent-136906.

esattamente, foto dal contenuto pornografico senza adottare nessun tipo di restrizione (password o altri sistemi)». Le prove su cui si è basata la decisione del Tribunale sono consistite in primo luogo nell'esame dell'operante di polizia che aveva svolto le indagini su segnalazione della Guardia di Finanza riguardo il sito contenente immagini pornografiche. Le indagini erano consistite nella verifica che il sito, allocato negli U.S.A. tramite il fornitore di servizi di Web Hosting "50megs.com" era registrato a nome dell'imputato, e nella stampa delle pagine del sito. Inoltre è stato sentito in giudizio un altro teste, circa le operazioni di perquisizione e di sequestro preventivo effettuate nei confronti dell'imputato. Il teste ha riferito che nel corso della perquisizione erano stati rinvenuti su un PC utilizzato come server DNS due file di log, che erano stati acquisiti mediante copia su supporto CD. Uno dei due file conteneva le indicazioni degli indirizzi IP dei visitatori del sito e l'altro file, identificabile con il nome "vallecupa.com.dns", conteneva il reindirizzamento. Nel corso della perquisizione non veniva però rinvenuta nessuna immagine relativa al contenuto del sito www.vallecupa.com.
Sempre nel corso del dibattimento sono stati disposti degli accertamenti tecnici mediante perizia; la relazione del perito ha concluso per la scarsa valenza probatoria delle riproduzioni a stampa delle pagine web – che, peraltro, riportavano una data di stampa successiva alla data di contestazione del reato – a causa dell'impossibilità di svolgere considerazioni sul contenuto e sulle caratteristiche tecniche per la mancata acquisizione in formato digitale.
Il contesto probatorio così raggiunto è stato ritenuto insufficiente a fondare una condanna ed il Tribunale di Pescara ha quindi assolto l'imputato ai sensi dell'art. 530 co. 2 c.p.p.

2. Prassi e casistica degli ultimi anni d'indagine

2.1. Principali operazioni di indagine della Guardia di Finanza.

Di seguito, una veloce panoramica delle principali operazioni di contrasto alla criminalità informatica svolte dalla Guardia di Finanza dal 2002 al 2006, sulla base di un colloquio con Mario Piccinni, già Comandante della Compagnia Pronto Impiego della Guardia di Finanza di Milano, ora Comandante della Sezione Falsificazione Monetaria e Reati Informatici del Nucleo di Polizia Tributaria di Milano.

Operazione "mouse" (2002)
L'attività investigativa si è sviluppata attraverso l'intercettazione di caselle di posta elettronica utilizzate dagli indagati. Due sono stati i siti sottoposti a sequestro e messi off-line: www.onlysoft.cc e www.digilander.libero.it/rafok. Inoltre sono stati sequestrati oltre 250.000 mp3, oltre 15.000 programmi, 36 personal computer, 32 monitor, 32 tastiere, 7 videoregistratori, 40 masterizzatori, 12 scanner, 16 stampanti, 2 televisori, 16.011 supporti CD. I soggetti monitorati sono stati oltre 95.000; di questi, 181 sono stati identificati e segnalati all'Autorità Giudiziaria per violazione degli artt. 171-*ter* (che nel 2002 puniva varie condotte di violazione del diritto d'autore per uso non personale e con il fine di profitto) e 174-*bis* (che sanziona in via amministrativa le condotte di violazione del diritto d'autore, in aggiunta alle sanzioni penali) L. 633/1941 e 648 c.p. (ricettazione). Altri 31.977 account sono stati segnalati all'Autorità Giudiziaria per violazione dell'art. 174-*ter* L. 633/41 (che nel 2002 prevedeva le sanzioni amministrative accessorie della sospensione dell'esercizio o dell'attività, la cessazione temporanea dell'esercizio o dell'attività, la revoca della licenza di esercizio o dell'autorizzazione allo svolgimento dell'attività e che prevede oggi sanzioni amministrative per l'abusivo utilizzo, duplicazione, riproduzione di opere o materiali protetti e per l'acquisto o noleggio di supporti audiovisivi, fonografici, informatici o multimediali non conformi o di attrezzature, prodotti o componenti atti ad eludere misure di protezione tecnologiche). Infine, 10.327 account sono stati

segnalati per violazione degli artt. 171-*bis* (duplicazione ed altre azioni illecite su programmi per elaboratore e su banche dati), 171-*ter* L. 633/41 e 648 c.p. (ricettazione).
I dati di cui sopra sono stati successivamente inviati alle Procure competenti per territorio, affinché queste ultime ponessero in essere le attività investigative e repressive previste dalla norma.
Le investigazioni si sono incentrate nell'intercettazione dei flussi di comunicazione telematica intercorsi sugli account individuati e ritenuti interessanti dal punto di vista investigativo, con la predisposizione delle "caselle ombra"[27]. Inoltre sono stati tenuti sotto controllo dodici siti web.
L'attività di indagine ha consentito di smantellare una rete di vendita composta da veri e propri "professionisti" del settore: il volume di affari relativo al valore dei supporti CD o DVD realizzato è stato stimato in oltre 100 milioni di euro. Servendosi della Rete quale bacino di potenziali clienti, gli indagati pubblicizzavano la vendita di prodotti software e musicali a prezzi molto inferiori di quelli di mercato. Il soggetto principale della rete di produzione e vendita è stato individuato nella persona di un maresciallo dell'Arma dei Carabinieri. A seguito di perizia tecnica su di un personal computer portatile e su alcuni supporti CD-ROM e floppy sequestrati al maresciallo a seguito di perquisizione domiciliare, sono emersi i seguenti dati: 95.205 soggetti cui l'indagato avrebbe effettuato *spamming* dei prodotti illegali da lui venduti; 31.977 soggetti che presumibilmente avrebbero acquistato materiale tutelato dall'indagato; 10.327 "clienti" dell'indagato che verosimilmente avrebbero, a loro volta, rivenduto i CD illecitamente riprodotti.
Sono state effettuate ulteriori indagini sul territorio nazionale, anche con l'ausilio di personale tecnico appartenente alla B.S.A. (Business Software Alliance) e alla F.P.M. (Federazione contro la Pirateria Musicale), adottando tecniche di indagine quali la decriptazione di e-mail cifrati e messaggi in codice, l'analisi di indirizzi IP e l'analisi di file di log. Tra le tecniche di indagine, sono state, altresì, operate ricerche presso alcuni server provider nazionali e stranieri,

[27] Si tratta di apposite caselle di posta elettronica, predisposte in collaborazione con il provider, per il reindirizzamento e la duplicazione di tutti i messaggi relativi all'account dell'indagato; cfr. Ninni F., *Giudice penale e giudice minorile di fronte all'abuso sessuale,* cit., pag. 5.

a seguito delle quali venivano individuati i proprietari dei siti sottoposti a sequestro e posti off-line.

Operazione "Web master" (2003-2005)
Si tratta di una complessa indagine finalizzata alla prevenzione ed alla repressione della pirateria informatica ed audiovisiva perpetrata attraverso *dialer*, programmi che configurano il computer dell'utente in modo che si disconnetta dal proprio Internet provider per collegarsi ad un altro fornitore di accesso: lo strumento, di per sé legale, permette a fornitori autorizzati di contenuti di far pagare l'accesso ad alcuni servizi telematici, ma può venire utilizzato illecitamente, effettuando connessioni a server con connessioni a prezzi elevati, senza il consenso dell'utente. Ad esempio, il fornitore di contenuti (content provider) X dispone di un sito Internet sul quale riceve numerose visite e sul quale mette a disposizione un servizio di vendita di suonerie per telefoni cellulari; il visitatore che decide di usufruire del servizio dovrà utilizzare un *dialer* che attiverà un collegamento su un numero di proprietà del service provider Y, che corrisponderà a X un compenso commisurato al traffico generato.
Le condotte illecite possono manifestarsi attraverso diverse modalità ed espedienti. In genere, il fulcro dell'attività criminosa consiste nella illecita diffusione di brani musicali tutelati dal diritto d'autore in formato mp3, attraverso due modalità: a) il *dialer* mette direttamente in comunicazione gli utenti attraverso un sito contenente file mp3 gestito dallo stesso content provider; b) il content provider fornisce un'intelligenza, cioè mette in collegamento gli utenti attraverso una selezione organizzata di link, mentre i brani musicali sono messi in rete da terzi o tramite siti gestiti da terzi o tramite motori di ricerca di brani musicali, sempre gestiti da terzi; in ogni caso, il content provider garantisce il reperimento del brano cercato, attraverso un costante monitoraggio della Rete e l'aggiornamento continuo dei link. Spesso il content provider opera in modo che l'utente non si accorga che sta scaricando un programma che modificherà i parametri di connessione con maggiorazione del costo di connessione. In alcuni casi il *dialer* viene impostato in modo da addebitare la connessione maggiorata anche quando l'utente non sta navigando su siti del content provider. A volte le modalità di connessione vengono organizzate in modo tale da amplificare in ogni caso i costi: ad esempio il content provider

prolunga fraudolentemente la connessione con una serie di espedienti, quali l'apertura automatica di finestre o altre tecniche finalizzate a far girare a vuoto l'utente.
L'indagine ha permesso di appurare che l'organizzazione criminale è imperniata su diversi livelli e strutturata in forma piramidale, al cui vertice si trovano gli organizzatori del servizio che offrono servizi a pagamento in Internet (service e content provider, o soli service provider). Al di sotto di tali società, vi sono una serie di soggetti che possono essere qualificati quali veri e propri procacciatori, che hanno il compito di individuare e contattare i soggetti potenzialmente interessati a promuovere presso gli utenti l'attività. All'ultimo gradino vi sono i web master, cioè i gestori dei siti, i quali si occupano di offrire il *dialer* in Rete fungendo da intermediari, in cambio di una percentuale sugli utili.
L'indagine ha interessato diciassette regioni e si è conclusa con la segnalazione all'Autorità Giudiziaria di cinquanta soggetti per violazione degli artt. 171-*bis*, 171-*ter* L. 633/1941, 640-*ter* (truffa informatica) e 648 c.p. Sono stati effettuati il sequestro di circa € 2.500.000,00, di trentadue conti correnti bancari, libretti di risparmio, carte di credito e libretti di assegni, nonché di ventotto personal computer e di sessanta siti web.

Operazione "Clone Attack" (2004)
Attraverso il monitoraggio delle principali piattaforme di condivisone dati la Guardia di Finanza ha individuato e denunciato trenta soggetti per violazione della L. 633/41, con messa off-line di sistemi informatici denominati "cloni di Napster". Sono stati sequestrati milioni di file mp3, programmi software e migliaia di file relativi ad opere cinematografiche. Inoltre, sono state segnalate nove persone all'Autorità Giudiziaria italiana e 150 soggetti stranieri all'Interpol, in relazione al reato di cui all'art. 600-*ter* c.p. (pedopornografia).

Phishing e cyber-riciclaggio (2004-2006)
Il *phishing* è oggi uno dei modi più comuni per mettere in atto un furto d'identità[28]. Il termine è una storpiatura dell'inglese *fishing*

[28] Per approfondimenti sul phishing: *Antiphishing Working Group*, http://www.antiphishing.org; *Trusted electronic communications forum*,

(pescare) ed è nato negli ambienti hacker alla fine degli anni '90, in particolare, in relazione ai trucchi escogitati per il furto di credenziali di accesso a sistemi informatici. È una moderna rivisitazione di una vecchia tecnica di *social engineering*: il sistema basa il proprio funzionamento soprattutto sul concetto di *mail-spoofing*, ossia l'invio di messaggi di posta elettronica, in genere realizzati su modello di una reale comunicazione di servizio, dal contenuto artefatto e con dati del mittente non veritieri e ingannevoli. In genere, l'*e-mail* truffaldino è un messaggio proveniente apparentemente dalla banca, dall'emittente della carta di credito o dall'assicurazione, che con una scusa qualsiasi, chiede all'utente di comunicare alcuni dati personali, tramite modulo da compilare o mediante reindirizzamento ad un sito civetta. Si sono successivamente diffusi *e-mail* che simulano offerte di acquisto e affari da cogliere al volo, provenienti – apparentemente – da affidabili siti di e-commerce.

In Italia è stata la Guardia di Finanza di Milano ad occuparsi dei primi casi di *phishing*, reato in crescita esponenziale in tutta la Rete. La complessa attività di indagine svolta tra il 2004 e il 2006 e denominata "*Phishing* e antiriciclaggio" ha riguardato un'organizzazione criminale dell'Est Europa che operava nel modo seguente:

1) *phisher* stranieri per conto di strutturate organizzazioni dell'Est Europa carpivano con l'inganno le credenziali di clienti di alcune tra le maggiori banche italiane trasferendo dai loro conti somme a favore di compiacenti beneficiari italiani;

2) successivamente, altri soggetti italiani riscuotevano le cifre che versavano a soggetti nei paesi dell'Est, previo storno delle percentuali di commissione pari al 5-20%.

L'attività investigativa della Guardia di Finanza ha consentito di ottenere i nominativi dei beneficiari italiani e le relative coordinate bancarie. Le indagini, svoltesi anche grazie ad un continuo e permanente scambio informativo e di *intelligence* tra gli organi inquirenti degli Stati coinvolti, si sono quindi sviluppate attraverso il

---

http://www.tecf.org; *Websense Security Labs*, http://www.websensesecuritylabs.com; *Federal Trade Commission – Deter. Detect. Defend. Avoid ID Theft*, http://www.ftc.gov/bcp/edu/microsites/idtheft.

blocco delle transazioni Italia–Est Europa, con istituzione di una *black list* relativa ai nominativi italiani e stranieri e agli importi.

Operazione "Wild Sharer" (2006)

Sempre nell'ambito delle indagini espletate su piattaforme di *file sharing*, la Guardia di Finanza di Milano è giunta all'individuazione di una vasta rete di scambio e messa in condivisione illegale di opere dell'ingegno tutelate da copyright (film, software, brani musicali, etc.), nonché di filmati e foto a carattere pedo-pornografico. L'attività di indagine, la prima condotta su connessioni in banda larga, si è conclusa con la denuncia all'Autorità Giudiziaria di 61 soggetti per violazione della L. 633/41 e degli artt. 600-*ter* (pedopornografia) e 600-*quater* c.p. (detenzione di materiale pedopornografico) e ha permesso di smantellare la comunità di riferimento del *file sharing* in Italia. Nel complesso la Guardia di Finanza di Milano ha eseguito 57 decreti di perquisizione locale e ha sottoposto a sequestro 97 personal computer, 84 hard disk, circa 20.000 supporti ottici (CD e DVD) contenenti opere dell'ingegno tutelate, foto e video a contenuto pedopornografico, e oltre 200 milioni (pari a 890 terabyte) di file mp3; inoltre sono state poste off-line tre web radio che trasmettevano illegalmente contenuti su rete telematica, e sono stati sottoposti a sequestro due siti Internet (www.freeazzurra.com, www.freeazzurra.it). Infine, 71 soggetti stranieri sono stati segnalati all'Interpol in relazione al reato di pedopornografia.

2.2. Fase di indagine, collaborazioni, mezzi di ricerca della prova digitale[29].

Come si individuano i siti che diffondono illecitamente materiale protetto dal diritto d'autore e materiale pedopornografico?
Piccinni: Per ciò che attiene le attività investigative on-line, non vi sono metodologie standard codificate. Gli indirizzi dei siti che diffondono materiale pedopornografico o protetto da copyright non sono reperibili compiendo un semplice *find* sui motori di ricerca: gli URL di questi siti circolano nei forum, sulle chat, nelle liste di distribuzione, passando di mano in mano attraverso il meccanismo del "passaparola", adesso rivisitato in versione elettronica. Non è sufficiente, difatti, la semplice iscrizione alle comunità virtuali per ottenere gli indirizzi: bisogna entrare a far parte della *community*, disporre di qualcuno già inserito che ti presenti ad essa, come una sorta di raccomandazione che serve agli utenti che già ne fanno parte a scongiurare il pericolo di infiltrazione di componenti pericolosi all'interno del gruppo, quali ad esempio le forze di polizia.
Per operare in questo particolare contesto, la L. 269/1998, *Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù,* ha previsto istituti importanti come quello dell'agente provocatore per le indagini in relazione ai reati di prostituzione minorile (art. 600-*bis* c.p.), pornografia minorile (art. 600-*ter* c.p.) e iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-*quinquies* c.p.).

Come si rintracciano gli utenti che condividono file protetti dal diritto d'autore e gli utenti che condividono materiale pedopornografico?
Piccinni: In entrambi i casi il metodo parte dall'acquisizione dell'IP associato in maniera univoca alla macchina utilizzata in Internet dal soggetto che commette il reato. L'identificazione degli elaboratori

[29] Sulla base di colloqui con Mario Piccinni, già Comandante della Compagnia Pronto Impiego della Guardia di Finanza di Milano, ora Comandante della Sezione Falsificazione Monetaria e Reati Informatici del Nucleo di Polizia Tributaria di Milano, e con Marco Signorelli, tecnico informatico di F.P.M., Federazione contro la Pirateria Musicale.

connessi al web è difatti garantita dalla univocità del loro indirizzo IP, una stringa di numeri composta da quattro serie di cifre. All'atto della richiesta di connessione ad Internet, il service provider assegnerà uno degli indirizzi IP di cui dispone all'utente richiedente, il quale ne usufruirà per l'intera sessione di collegamento. Accertato a quale utente risulta abbinato un determinato indirizzo IP nel momento in cui l'attività illegale risulta posta in essere, andranno richiesti al service provider i file di log, ovvero le informazioni necessarie ad individuare il punto di connessione dal quale ha avuto origine l'entrata nel web del terminale attraverso il quale è stato commesso il reato. Si tratta, in buona sostanza, di informazioni di tempo ed identità memorizzate dal server per identificare i fruitori. Va sottolineato, per completezza, che l'acquisizione dei file di log con decreto del P.M., alla luce della attuale normativa, è possibile solo per un periodo di tempo di sei mesi, mentre con richiesta di autorizzazione al GIP entro dodici mesi dall'evento (coincidente con l'obbligo di conservazione per il gestore)[30].

Come viene accertato un accesso abusivo a un sistema informatico? Come viene appurata la riconducibilità di un accesso abusivo ad una data persona?
Piccinni: Tutte le azioni che si compiono su Internet lasciano traccia: navigazioni, e-mail, invio di file, qualsiasi attività sul web viene tracciata dal provider o dal gestore del sito Internet. È attraverso l'analisi di queste tracce informatiche, sia sul computer della vittima sia, in una fase successiva, sulla macchina dell'attaccante, che si giunge all'accertamento della violazione e si riconduce l'attacco informatico ad un determinata persona.

Dati sull'attività di indagine: numero di sequestri, materiali sequestrati, sanzioni comminate.
Piccinni: La Guardia di Finanza nell'attività di contrasto alla pirateria ha operato, per il solo triennio 2003-2005, oltre 21.000 interventi sull'intero territorio nazionale. Nel 2003 si sono registrati

[30] Vedasi art. 132 D.lgs. 196/2003, *Codice in materia di protezione dei dati personali*, modificato dapprima con D.l. 345/2003 (conv. con modificazioni dalla l. 45/2004) e successivamente dal c.d. decreto Pisanu (D.l. 144/2005 conv. con modificazioni dalla L. 155/2005).

5.142 interventi, 5.714 soggetti verbalizzati, di cui 124 tratti in arresto, a fronte di 5.061 violazioni riscontrate. Nel 2004 si sono registrati 6.933 interventi, 7.773 soggetti verbalizzati, di cui 104 tratti in arresto, a fronte di 6.753 violazioni riscontrate. Nel 2005 si sono registrati 9.135 interventi, 10.298 soggetti verbalizzati, di cui 242 tratti in arresto, a fronte di 8.989 violazioni riscontrate.
A testimonianza del fatto che il fenomeno ha ormai assunto le dimensioni di una vera e propria attività industriale ed imprenditoriale su scala internazionale, va evidenziato che nel solo biennio 2003-2004, i "pezzi" illegali sequestrati dalla Guardia di Finanza in Italia ammontano ad oltre 129 milioni.
Signorelli: Per quanto riguarda le operazioni in relazione alle quali abbiamo fatto da consulenti alla Guardia di Finanza, le persone denunciate sono circa 140. Molte sono le operazioni condotte autonomamente dalle forze dell'ordine. Quanto al numero di file condivisi o di GB di materiali, la statistica è più difficile perché le comunicazioni della G.d.F. parlano a volte di numero di GB condivisi ed altre di numero di file. Durante l'ultima operazione si è parlato di volume di terabytes condivisi dall'intera comunità indagata su di un singolo server.

Di quali mezzi tecnici ci si avvale?
Piccinni: Esistono diversi strumenti tecnici, anche gratuiti e facilmente reperibili on-line che, attraverso attività di investigazione sia tipiche sia atipiche, consentono di arrivare alla determinazione di "chi ha compiuto cosa". Fondamentale, però, resta lo strumento legislativo: avvalendosi di esso, difatti, l'autorità giudiziaria, attraverso gli accertamenti che la polizia giudiziaria esperisce presso i fornitori dei servizi Internet e soprattutto la documentazione di interesse investigativo prodotta, ha il potere di acquisire le fonti di prova di un crimine.
Signorelli: Nelle operazioni di indagine che svolgiamo per l'autorità giudiziaria quali ausiliari di P.G., innanzitutto cerchiamo di essere aggiornati sui vari programmi di *file sharing* disponibili, programmi di *screenshot* che permettono di "fotografare" un determinato evento nel momento stesso in cui appare a video, e da ultimo programmi di *sniffing* per monitorare il traffico di Rete. Altro programma sicuramente utilissimo ai nostri fini è "*Smart Whois*", che permette di associare un determinato IP all'intestatario o al service

provider di appartenenza. Particolarità di questo programma è l'aggiornamento praticamente quotidiano grazie al collegamento con i server dei vari ISP: in questo modo permette di avere sempre informazioni aggiornatissime sugli intestatari degli IP e sui server provider che andiamo ad analizzare. Per quanto riguarda lo *sniffing* del traffico di Rete, viene utilizzato un programma che permette il *traceroute*[31] attraverso *backdoor*: viene "fotografato" l'istante e salvato su di un file, il quale contiene oltre alle informazioni sul traffico di rete, una attestazione temporale. Solitamente basta questa come copia. Qualora il Pubblico Ministero lo richieda, si completa il download del file che si sta scaricando e lo si conserva come ulteriore prova. In genere si entra sul server condividendo un minimo di *share*, solitamente materiale non protetto dal diritto d'autore e si prova a scaricare dagli altri finché l'amministratore del server non se ne accorge e si viene bannati da quel determinato server: infatti i programmi di DirectConnect permettono all'amministratore del server di impostare alcuni parametri ed alcuni filtri, attraverso i quali coloro che condividono file indesiderati, o non condividono abbastanza file del genere che interessa al gruppo di scambio, vengono automaticamente bannati. Su programmi di P2P come Kazaa giravano intere liste di IP da bannare automaticamente, tra i quali gli indirizzi di B.S.A., F.P.M., Interpool, G.d.F. e altre forze di polizia internazionali. Ogni tanto veniamo contattati per dirigere operazioni simili nel campo della lotta alla pedopornografia on-line.

Con che mezzi, modalità e finalità vengono effettuate le collaborazioni tecniche tra Guardia di Finanza e B.S.A. e F.P.M.?
Piccinni: La Guardia di Finanza combatte il fenomeno della pirateria con eccellenti risultati attraverso i propri reparti territoriali. Le associazioni di settore che combattono la pirateria (FAPAV, F.P.M. e B.S.A.), per quanto di propria competenza ed ognuna nel proprio

[31] Da Wikipedia (http://wikipedia.it/): si tratta di «un'applicazione, scritta in qualunque linguaggio, che si occupa di ricavare il percorso seguito dai pacchetti sulle reti informatiche, ovvero l'indirizzo IP di ogni router attraversato per raggiungere il destinatario. Il termine traceroute indica, oltre all'applicazione, anche il percorso restituito dall'applicazione stessa» (http://wikipedia.it/wiki/wiki/Traceroute?#Applicazioni_di_traceroute).

specifico campo di intervento, forniscono supporto tecnico alle forze di polizia e promuovono iniziative di sensibilizzazione. Queste associazioni si occupano di monitorare il mercato, identificando i casi di pirateria e segnalandoli alle forze dell'ordine ed alla magistratura; promuovono in campo investigativo e giudiziario le azioni che si rendono opportune per la tutela dei diritti d'autore; collaborano sul piano tecnico; danno adeguata pubblicizzazione alle operazioni anti-pirateria e promuovono la crescita dell'industria attraverso iniziative di sensibilizzazione, di educazione pubblica e mediante azioni legali. Il supporto tecnico fornito alla Guardia di Finanza si estrinseca attraverso la messa a disposizione, nel corso di specifiche operazioni di polizia giudiziaria (perquisizioni e sequestri), di personale altamente specializzato, che viene per l'occasione nominato ausiliario di P.G. *ex* art. 348 c.p.p. Le stesse associazioni di settore, infine, organizzano corsi di formazione volti ad aggiornare le forze dell'ordine su come contrastare il fenomeno della pirateria, come identificare prodotti contraffatti e rintracciare siti pirata in Internet.
Signorelli: Viene fatta attività di consulenza alla G.d.F., soprattutto per quanto riguarda le dinamiche di utilizzo di programmi di *file sharing,* eventuale attività di monitoraggio e, qualora il P.M. lo richieda, attività finalizzata alla raccolta delle prove.

Esistono e come sono strutturate le collaborazioni con organismi internazionali?
Piccinni: Tenuto conto dei sempre crescenti interessi delle organizzazioni criminali nell'individuare e localizzare nuove aree di investimento, al fine di operare una valida azione di contrasto alle attività criminose nel campo economico e finanziario, il Corpo della Guardia di Finanza ha conferito fondamentale importanza alla collaborazione internazionale. Al fine di perseguire le violazioni in materia economica e finanziaria perpetrate a danno del Bilancio dello Stato e dell'Unione Europea, secondo quanto stabilito con il D.lgs. 68/2001, la Guardia di Finanza può destinare proprio personale militare presso rappresentanze diplomatiche, uffici consolari e sedi istituzionali competenti in materia in ambito europeo ed internazionale. I rapporti di collaborazione con gli organismi collaterali esterni (http://www.gdf.it/link/linkeu.htm) sono tenuti direttamente dal Comando Generale, il quale mantiene tutti i rapporti interna-

zionali che il Corpo instaura con Organi di Polizia, Amministrazioni Doganali e Finanziarie, Enti ed Agenzie di altri Paesi, compresi i Servizi dell'Unione Europea gli Organi centrali di Polizia nazionali con competenze estere. La Guardia di Finanza infine concorre, unitamente ad organismi internazionali quali Europol, OIPC Interpol, Organizzazione Mondiale delle Dogane, Ufficio Europeo per la Lotta Antifrode, all'attività di contrasto degli illeciti in ambito internazionale.

Che conseguenze ha la mancanza nel nostro ordinamento di una definizione e della disciplina della prova informatica, caratterizzata dalla immaterialità?

Piccinni: Purtroppo è vero: nel nostro Paese non esiste una legge che disciplini la prova informatica. In questo caso, ed il perché è facile da intuire, si seguono gli orientamenti dettati dalla giurisprudenza statunitense. In ogni caso, da qualche anno a questa parte si sta iniziando a porre maggiore attenzione all'acquisizione ed alla successiva conservazione ed analisi della prova informatica. Quello che non si percepisce è l'importanza di conservare il dato in maniera che non venga in alcun modo alterato: quando viene rinvenuta un'arma sulla scena di un delitto, a nessuno verrebbe in mente di toccare a mani nude tale oggetto, quando però si è dinnanzi un computer da cui o attraverso il quale è stato commesso un crimine, non ci si rende conto che ogni azione operata su quel PC non fa altro che confondere ed inquinare le prove con ulteriori tracce non inerenti il reato per cui si procede. Da un esperimento è risultato che durante il solo avvio di Windows vengono modificati 243 file e creati 7 nuovi file. Da ciò è facile intuire quanto fragili siano le prove informatiche e quanto tecnicamente preparato debba essere l'operatore che in sede di investigazione è deputato al loro prelevamento e quindi alla loro difesa da una possibile modifica.

Signorelli: Nella mia esperienza, per quello che mi hanno richiesto i vari P.M. nelle deleghe, non ci sono mai stati grandi problemi nella ricerca della prova, anche se si tratta spesso di prove informatiche e dunque immateriali. Ad esempio, come già detto, non tutti i P.M. richiedono che venga anche effettuato almeno un download di materiale illecito da uno dei partecipanti al gruppo di scambio. Viene ritenuta prova anche solo lo *screenshot* del momento consumativo dello scambio di file protetti dal diritto d'autore. Altre volte si ri-

chiede anche il file di log che dimostra il traffico di rete tra gli utenti di un determinato scambio.

È sentita l'esigenza di un protocollo unitario sulla computer forensics?
Piccinni: L'esigenza di un di protocollo unitario sulla *computer forensics* è ovviamente fortemente sentita: consentirebbe una auspicabile maggiore specializzazione degli organi di polizia che operano nel settore ma soprattutto una standardizzazione delle procedure.
Signorelli: Come detto, spesso le richieste dei P.M. sono differenti in base alla loro provenienza. Tuttavia, quello che viene richiesto ad un ausiliario di PG è una serie di operazioni abbastanza circoscritta. Noi ci atteniamo a quello che viene scritto nel decreto del P.M. e di conseguenza lo facciamo. I problemi di solidità della prova riguardano più i soggetti, G.d.F. prima e pubblici ministeri dopo, che dovranno utilizzare la prova stessa. Se poi si formulassero delle *best practices* in questo campo, noi avremmo sicuramente il lavoro facilitato.

Ci sono delle regole o prassi procedurali per l'acquisizione della prova informatica? Da dove provengono?
Piccinni: Le regole ci sono ma non sono mai state accolte e codificate in una legge che le rendesse ufficialmente valide nel nostro Paese[32]. In ogni caso, tali regole vengono seguite dagli investigatori informatici ed accettate dai magistrati chiamati a giudicare i fatti. Negli USA esistono da diverso tempo apposite linee guida per la *computer forensics*. Dal 1990 è in attività la IACIS (*International Association of Computer Investigative Specialists*); nel 1997, in ambito G8, è stata affrontata ufficialmente la tematica delle prove

[32] NDR: Se è vero che il codice di procedura penale nulla prevede in relazione alle prove digitali e che un aggiornamento delle norme è auspicabile, l'ipotesi di cristallizzare in legge le regole e le procedure informatiche desta perplessità. È certamente sentita la necessità di un adeguamento del codice con l'inserimento di principi generali in materia di valutazione e requisiti della prova digitale, di cui è necessario garantire certezza, genuinità e paternità; le specifiche tecniche, tuttavia, anche in considerazione della continua necessità di aggiornamento, non possono che essere lasciate alla comunità scientifica (cfr. Costabile G., *Ecco come procedono al sequestro del PC*, Punto Informatico, 2006).

digitali ed è stato formato lo IOCE. Dal 1998 il *National Cybercrime Training Patnership*, il *Law Enforcement Standards* ed il *National Institute of Justice* collaborano, dettando ed aggiornando alcune linee guida. In Europa, l'ITCIM (*Information Tecnology Crime Investigation Manual*), redatto inizialmente dall'Interpol e adesso affidato all'*European Working Party on Information Tecnology Crime*, si propone di stilare un manuale operativo per i crimini tecnologici.

Quali sono gli strumenti ed i mezzi per le perizie?
Piccinni: Perizia e consulenza tecnica ruotano attorno alle specifiche competenze *ex* art. 220 c.p.p. Secondo la norma, 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. Gli strumenti da utilizzare per le perizie sono maggiormente standardizzati dalle procedure e provengono prevalentemente dagli Stati Uniti e dalla Gran Bretagna. Programmi come *Encase*, *Forensic Tool Kit* e, solo per le forze di polizia, *Ilook*, sono oggi lo standard utilizzato per le analisi di informatica forense. Esistono poi tutta una serie di macchinari ed accessori, tipo *FRED*, *Ultrakit*, *Logicube* e *Shadow Drive*, che aiutano non poco l'attività di investigazione.

Quali sono i tempi di una perizia?
Piccinni: Non esiste un tempo prestabilito per operare una perizia. Molto dipende dalla quantità di dati da analizzare e dalla complessità dei sistemi presi in esame: si pensi, ad esempio, a quanto complesso può risultare periziare dati elaborati da programmi di crittografia. A seconda dei casi una perizia approfondita si può risolvere in un mese oppure in un anno.
Signorelli: Dipendono dalla quantità di materiale sequestrato, nonché dalla tipologia della perizia. Quelle effettuate non in contraddittorio e dunque quali atti ripetibili, devono avere maggiori garanzie e necessitano naturalmente di molto più tempo. Vengono effettuate le copie tecniche degli HD, e questa operazione può richiedere anche intere giornate di attività.

In Italia come si risolve il problema dell'analisi di grosse quantità di dati?

Piccinni: Nell'ambito di attività investigative informatiche il problema dell'analisi di grosse quantità di dati viene risolto operando delle analisi parametriche, ovvero delle ricerche mirate al ritrovamento esclusivo di quanto interessa ai fini dell'indagine di cui ci si sta occupando.
Signorelli: Non viene effettuato un controllo a campione, si procede comunque a constatare l'effettiva illegalità di tutti i file presenti sul PC, anche in ragione del fatto che solitamente il lavoro è facilitato perché i file sono ordinati in cartelle per nome dell'autore o dell'opera interamente contraffatta. Vengono eliminati i file parziali e quelli *freeware* di cui è lecita la detenzione ma non la distribuzione. Quando ci troviamo dinanzi a grosse quantità di file ne vengono estratti a campione alcuni da ogni cartella e questo viene considerato un controllo valido.

Che efficacia può avere l'analisi a campione dei file incriminati?
Piccinni: La valenza e l'opportunità di effettuare analisi a campione ha valore esclusivamente quando, come nel caso di violazioni al diritto d'autore, non importa tanto il contenuto dei file ma l'esclusivo possesso illegale degli stessi. Così come avviene per i reati di copyright, non c'è bisogno di analizzare tutti i file contenuti nell'hard disk dell'indagato. Basta analizzare il contenuto a campione dei file per incriminare una persona di tale condotta[33].

Nelle perizie viene svolta una verifica delle licenze dei file incriminati? Come? Viene anche svolta per file distribuiti con licenze freeware ma con esclusione della possibilità di condivisione?
Signorelli: Noi personalmente controlliamo che quel determinato file non venga posto nella cartella di condivisione e non si verifichi quindi attività di distribuzione. Sarà poi la G.d.F., qualora interessata, a controllare che il soggetto abbia l'originale del software oppure possa dimostrare il legittimo possesso della copia privata.

[33] NDR: Sicuramente la quantità di file non incide sulla affermazione di responsabilità penale ma incide, oltre che in sede amministrativa per la determinazione delle relative sanzioni, sulla determinazione della pena, sulla applicabilità della circostanza aggravante della rilevante gravità (art. 171-*bis* L. 633/1941) e della diminuente di cui all'art. 171-*ter* co. 3 (particolare tenuità del fatto): tali determinazioni non possono evidentemente essere effettuate su dati "a campione".

Come avviene e su cosa si basa la formazione dell'esperto informatico?
Piccinni: Gli esperti vengono formati attraverso corsi di formazione, specializzazione e certificazione. Nella Guardia di Finanza i militari impiegati nello specifico settore vengono sottoposti ad un aggiornamento costante. La finalità è quella di conferire loro una base di conoscenza generale ed impartire le norme di comportamento da tenere di fronte ad un personal computer fonte di prova.
Signorelli: Si basa principalmente sulle esperienze tecniche del perito. Io, ad esempio, arrivo da una esperienza come service provider. È possibile anche che venga utilizzato l'aiuto di "hacker pentiti" che in seguito passano a collaborare con gli inquirenti.

Le norme del codice di procedura penale in tema di mezzi di ricerca della prova sono adattabili alla realtà informatica?
Piccinni: In generale si può affermare che dinnanzi alle repentine trasformazioni della Rete, la normativa penale italiana palesa seri limiti soprattutto riguardo la internazionalizzazione del fenomeno telematico. Le innovazioni introdotte dalla L. 547/93 sembrano non aver rispecchiato l'esigenza dell'adozione di un lessico maggiormente peculiarizzato in virtù dello specifico settore. L'esperienza operativa spingerebbe ad affermare che per ciò che attiene la realtà informatica sarebbe auspicabile la creazione di una raccolta normativa *ad hoc*, capace di cogliere e soprattutto adeguarsi ai continui mutamenti del pianeta telematico stesso, evitando di approcciare il problema con il condizionamento di dover adattare istituti propri del codice penale e del codice di procedura penale.

Quali sono le peculiarità dell'attività di perquisizioni "informatiche"? Nella perquisizione finalizzata, ad esempio, al sequestro di un pc si procede ad uno studio o esame preliminare dello stesso, oppure, individuato il mezzo informatico, si sequestra tout court?
Piccinni: Nella *computer forensics* non si effettuano perquisizioni nel senso classico così come definite dal codice di procedura penale. Le ispezioni, al contrario, si effettuano mediante l'utilizzo di programmi ed apparecchiature idonee al fine di non modificare il contenuto dell'hard disk. Uno di questi strumenti è il già richiamato *Shadow Drive*, che consente di avviare il sistema operativo presen-

te sull'HD oggetto di indagine senza modificare alcun file presente nello stesso. Le ispezioni sono da compiersi in contraddittorio, in presenza della parte, e danno atto all'acquisizione di copia e non al sequestro dei file ritenuti importanti ai fini investigativi. Si sottopone a sequestro il supporto informatico solo quando vi si trova memorizzato il corpo del reato e/o la quantità di dati da analizzare è tale da rendere impossibile l'esame entro limiti di tempo ragionevoli. In tal caso, al fine di non pregiudicare l'eventuale esercizio di attività commerciali (si pensi alle banche, agli avvocati, agli studi commercialisti, etc.), in accordo con il magistrato che ha emesso il relativo decreto, si procede alla copia dei dati su supporto compatibile ed al sequestro del disco originale.
Signorelli: Le operazioni avvengono sempre sotto la guida di ufficiali della G.d.F. Data la non pericolosità dei soggetti, solitamente si instaura subito un clima molto *friendly*, cercando di mettere a proprio agio il soggetto perquisito. Se si potesse operare in campo civile per il risarcimento, non ci sarebbe nemmeno bisogno del sequestro susseguente ad una perquisizione. Basterebbe recarsi dal giudice con i file di log che comprovano una movimentazione di materiale coperto dal diritto d'autore relativo ad un indirizzo IP, e chiedere che un ufficiale giudiziario si rechi dal soggetto per chiedere una compensazione stragiudiziale, minacciando una vera e propria azione legale volta al risarcimento del danno provocato alle majors. In campo penale sarebbe più veloce procedere ad una ispezione accurata in presenza della parte, senza effettuare il sequestro del computer, piuttosto che sequestrare tutto e poi a distanza di tempo esperire attività di perizia sul materiale sequestrato. Questo purtroppo è un problema legato al *modus operandi* tipico dei sequestri avvenuti in Italia negli anni passati, fin dai primi sequestri relativi ai tabacchi, etc. Se è presente un ausiliario di PG od il perito del P.M., viene sempre esperita attività di accertamento nell'immediato (ispezione) e poi si procede al sequestro. Oppure viene addirittura richiesto al soggetto stesso di intervenire sul PC.

In particolare, quali sono le procedure da seguire se lo strumento informatico da sequestrare è spento? Si controlla presenza di

floppy, CD*/DVD, disco fisso? Si procede ad inventario dettagliato dei dischi fissi?*[34]
Piccinni: Se ci si trova dinnanzi ad un PC spento ed il supporto è da sequestrare, si procede al semplice smontaggio ed al sequestro del solo HD. Se il computer è un server, occorre considerare che tali calcolatori hanno spesso hard disk configurati in modalità SCSI. Molto spesso, in questi casi, è necessario procedere al sequestro anche della scheda di controllo ed alla lettura ed al riordino dei file contenuti. Si procede ad inventario dettagliato dei dischi fissi.

Le procedure sono diverse per la perquisizione di macchine in uso?
Piccinni: Ovviamente le procedure sono differenti. Il sequestro di un HD va fatto a macchina spenta, quindi, se il PC è acceso, si dovrà provvedere dapprima allo spegnimento, che però non va operato, nel caso ad esempio di computer con sistema operativo Windows, eseguendo uno *shutdown* classico (start – chiudi sessione – arresta sistema). Così come nel caso dell'accensione illustrato in precedenza, una simile procedura comporterebbe una modifica dei file di sistema tale da rendere inutilizzabile la prova. Sarà quindi necessario spegnere la macchina estraendo il cavo di alimentazione: in tal modo, nulla sarà alterato e modificato rispetto a quella che era la situazione precedente l'accesso.

Quando si procede tramite un accertamento tecnico non ripetibile ex art. 360 c.p.p.?
Piccinni: A seconda del reato per cui si procede e della necessità per l'autorità giudiziaria di mantenere inalterate le fonti di prova, si può procedere o meno ai sensi dell'art. 360 c.p.p. Solitamente si preferisce non ricorrere spesso all'accertamento tecnico non ripetibile al fine di rendere nuovamente eseguibile l'accertamento anche alla difesa. L'accertamento ripetibile, infine, non comportando l'alterazione dei dati fonte di prova, ne consente la genuina conservazione, tenuto conto dell'immaterialità e dell'alta propensione alla modificazione del dato informatico. L'accertamento non ripeti-

[34] NDR: Un problema evidenziato è, ad esempio, la presenza di più hard disk che non vengano inventariati al momento del sequestro. Sul punto, Chirizzi L., *Computer forensic. Il reperimento della fonte di prova informatica*, 2006, pp. 22-24.

bile, invece, determina una modifica irreversibile dei dati sottoposti ad analisi: si pensi alla sola data ed ora di apertura del file. Nel caso di accertamenti ripetibili, tutte le analisi forensi si eseguono su una "copia lavoro" dell'hard disk originale. Come in precedenza sottolineato, preservare il dato informatico originale è l'imperativo.

In tema di sequestro probatorio di materiale informatico, è dibattuta la necessità di mantenere il vincolo su tutto il pc ed eventuali periferiche e supporti, anziché limitare il sequestro al solo hard disk. È praticabile – e, in caso affermativo, a quali condizioni - la soluzione del sequestro limitato al solo hard disk? È ipotizzabile il solo sequestro della copia "sicura" dell'hard disk?
Piccinni: Nel caso il reato contestato sia stato commesso mediante le apparecchiature collegate al PC si deve sottoporre sequestro tutto l'hardware. Nel caso, ad esempio, venga scoperto un laboratorio che stampa denaro falso, si sequestra sia il pc sia l'attrezzatura utilizzata per la stampa. In tutti gli altri casi, procedere al sequestro del materiale definito neutro al fini del reato è pressoché inutile, oltre che dispendioso, così come chiarito dalla sentenza della Corte di cassazione, Sezione III Penale, n. 1778 del 18.10.2003. In tale sentenza, infatti, non vengono indicate esigenze probatorie che legittimino il permanere del vincolo del sequestro sul materiale neutro e viene specificato, altresì, che la prova sarebbe tutelabile anche con il solo sequestro dell'hard disk e dei CD/floppy.

Qual è la realtà della prassi italiana in questa materia con particolare riferimento alla procedura dell'analisi dei supporti e delle procedure di copia "sicura"?
Piccinni: Per l'analisi dei supporti si procede all'acquisizione dell'originale ed alla ricerca delle prove sulla "copia lavoro", la quale altro non è che un'immagine dell'HD originale. Esistono diverse procedure, tutte valide e riconosciute dalle Procure della Repubblica, che permettono di acquisire la fonte di prova: dal comando "dd" dei sistemi *UNIX like*, all'acquisizione tramite il software *Encase*, all'utilizzo di sistemi hardware appositi come il *Logicube Forensics* o il più moderno *Talon*. In particolare, il *Logicube Forensics* ed il *Talon*, oltre a clonare l'hard disk, sono in grado di generare un report contenente un'impronta digitale del contenuto dei due HD (originale e copia) mediante algoritmi di *hashing* MD5 e SHA1. Al

termine delle operazioni, il sistema opera un confronto tra i due valori MD5/SHA1 evidenziando eventuali discrasie ovvero palesando il buon fine dell'operazione; in quest'ultimo caso, si avrà la sicurezza di aver realizzato una esatta copia di tutto quanto contenuto nell'hard disk originale. Per ciò che attiene le analisi, i già citati sistemi di analisi *Encase*, *Forensic Tool Kit*, *Ilook*, etc., rappresentano oggi lo standard utilizzato per le analisi di informatica forense sugli HD.

Qual è l'effettivo ricorso alle intercettazioni informatiche e telematiche?
Piccinni: Nonostante un sempre più frequente ricorso a questo tipo di strumento investigativo, le intercettazioni telematiche restano, comunque, quantitativamente meno rilevanti rispetto a quelle telefoniche e riguardano sia comunicazioni transitanti attraverso caselle di posta elettronica sia il traffico IP sviluppato su linee telefoniche o collegamenti a banda larga.

Come e con che mezzi si svolgono ? È frequente il ricorso ad impianti privati ? Se sì, quali?[35]
Piccinni: Tecnicamente le intercettazioni telematiche sono rappresentate da intercettazioni di linee dedicate alla trasmissione di dati. Dal punto di vista tecnico operativo, la procedura formale per avviare l'intercettazione telematica è simile a quella per le intercettazioni telefoniche. Ricevuta la delega dal Pubblico Ministero (l'autorizzazione all'intercettazione telefonica normalmente è richiesta dal P.M. e autorizzata dal giudice per le indagini preliminari) la polizia giudiziaria realizza una "griglia", cioè un documento nel quale sono contenuti in maniera sintetica tutti i dati tecnici che devono essere forniti al gestore del servizio per potere eseguire materialmente l'intercettazione, e che viene notificata, unitamente al decreto di intercettazione, all'Internet service provider. Per questo tipo di intercettazioni è necessario utilizzare le sonde, apparecchiature informatiche che vengono attestate sugli snodi, sulle porte

[35] Quando si procede a intercettazione di comunicazioni informatiche o telematiche, il pubblico ministero può disporre che le operazioni siano compiute anche mediante impianti appartenenti a privati (art. 268 co. 3-bis c.p.p.).

d'ingresso del sistema di gestione del provider. La sonda registra tutti i dati della trasmissione e li rimanda su una linea RES, cioè una linea telefonica fornita alla polizia giudiziaria e dedicata allo sviluppo dell'attività di intercettazione. Può anche esservi il caso che i dati siano catturati direttamente dentro la sonda e scaricati presso la Procura. Spesso bisogna reperire i dati direttamente dalla sonda e copiarli, perché si tratta di tecnologie diverse e abbastanza nuove. Esistono poi apparecchiature, chiamate *telemonitor*, che vengono poste come osservatori sulle varie linee utilizzate dalle persone oggetto di intercettazione telefonica. L'utente di un servizio Internet, infatti, può accedere alla Rete da qualsiasi punto (da casa sua, da un amico, da un Internet point, da un'altra città). Per poter individuare, e quindi tracciare, questa comunicazione bisogna presidiare sul territorio un numero maggiore di punti del provider presso cui il soggetto ha un account.
La linea per operare le intercettazioni può essere presa a noleggio da parte della Procura presso il gestore, oppure presso società private o consorzi che dispongono a loro volta di un certo numero di linee che mettono a disposizione della Procura e della polizia giudiziaria, insieme alle altre apparecchiature tecniche necessarie per le intercettazioni. Oggi le tecnologie di telecomunicazione registrano un progresso continuo. Le ditte che dispongono di apparecchiature per le intercettazioni, da un lato rincorrono le nuove tecnologie del settore e nello stesso tempo progrediscono, cercando di fornire sempre servizi più qualificati e tecnologicamente più evoluti per svolgere l'attività di intercettazione telefonica in maniera particolarmente efficace: si tratta di un'attività tipicamente privata, aziendale. L'imprenditore investe in un prodotto più qualificato, più sofisticato, per gareggiare e battere la concorrenza, per proporre apparecchiature che offrano un servizio migliore rispetto agli altri[36].

[36] NDR: In tema di collaborazione tra privati e pubblica autorità, è stato recentemente presentato (16 ottobre 2006) il progetto tra la Polizia Postale e la Microsoft: la multinazionale americana ha messo a disposizione gratuitamente il software CETS, *Child Exploitation Tracking System* (sistema di tracciamento contro la pedopornografia), sviluppato in collaborazione con le forze dell'ordine di diversi paesi e già utilizzato in Canada ed in Indonesia. Per approfondimenti, si vedano il sito *Polizia di Stato*, all'indirizzo
http://www.poliziadistato.it/pds/primapagina/pedofilia/microsoft.html; e

L'opzione contraria, che in linea di principio è correttissima, cioè che sia l'organo che gestisce l'intercettazione telefonica, la Procura o la polizia giudiziaria, a dotarsi di questi strumenti, richiederebbe investimenti folli, prima di tutto senza competizione.

Punto Informatico, all'indirizzo http://punto-informatico.it/p.aspx?id=1702453.

BIBLIOGRAFIA

Chirizzi Luca, *Computer Forensic. Il reperimento della fonte di prova informatica*, Roma, Laurus Robuffo, 2006.

Cajani Francesco, *Alla ricerca del log (perduto), commento a Tribunale di Chieti, Sez. Pen. - 30 maggio 2006 n. 139*. In: "Diritto dell'Internet" 6 (2006), pp. 573-582.

Coliva Daniele, *Quando sequestrarono i tappetini dei mouse*. In: Interlex, http://www.interlex.it/attualit/coliva34.htm, 2004.

Costabile Gerardo, *Scena criminis, documento informatico e formazione della prova penale*. In: Altalex – Quotidiano di informazione giuridica, http://www.altalex.com/index.php?idnot=7429, 2004.

Costabile Gerardo, *Ecco come procedono al sequestro del PC*. In Punto Informatico, http://punto-informatico.it/p.aspx?id=1494286, 2006.

De Riso Angelo, Scuto Salvatore, *I reati su sistemi informatici: accesso abusivo a sistema informatico e frode informatica*. In: "Il Sole 24 Ore – Ventiquattrore Avvocato", 7/8 (2005), pp. 72-84.

Luparia Luca, *Diffusione di virus e accesso abusivo a sistemi telematici. Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova penale digitale – I profili processuali*. In: "Diritto dell'Internet" 2 (2006), pp. 153-160.

Levy Steven, *CRYPTO I ribelli del codice in difesa della privacy*, Milano, Shake Edizioni, 2002.

Ninni Filippo, *Giudice penale e giudice minorile di fronte all'abuso sessuale*. In: Consiglio Superiore della Magistratura, http://appinter.csm.it/incontri/relaz/6872.pdf, 2001.

Perri Pierluigi, La *computer forensics*. In: *Manuale breve di Informatica Giuridica*, Milano, Giuffrè Editore, 2006 pagg. 199 – 212.

Tonini Paolo, *Lineamenti di Diritto Processuale Penale*, Milano, Giuffrè Editore, 2005.

Valeri Lorenzo, Rathmell Andrew, Robinson Neil, Servida Andrea, *Handbook of Legislative Procedures of Computer and Network Misure in EU Countries - Study for the European Commission Directorate-General Information Society*, In: Europa – Information Society, http://europa.eu.int/information_society/eeurope/2005/doc/all_about/csirt_handbook_v1.pdf, 2003.

Valeri Lorenzo, Somers Geert, Robinson Neil, Graux Hans, Dumortier Jos, *CSIRT Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries*. In: Rand Corporation, http://www.rand.org/pubs/technical_reports/2006/RAND_TR337.pdf, 2006.