L'Indagine Digitale

I. PREMESSE

L'indagine 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 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 informatici). 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].

---

[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».

[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.

[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.

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 Nucleo 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.

II. 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.

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 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

[6] Per approfondimenti, vedere il sito Servizio polizia postale e delle comunicazioni, http://www.poliziadistato.it/pds/informatica. Per una panoramica 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.

[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.

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 particolare 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».

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. 600ter 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

[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.
[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).

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.

III. 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.

III.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 nome 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».

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

[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.

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

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.

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 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:

---

[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.

[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.

- 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 farsi 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.

III.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. 615ter, 615-quater, 615-quinquies, 617-bis, 617-quater, 617quinquies, 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 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

[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.

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

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

"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 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].

III.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, 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.

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.

[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.

[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.

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_ab out/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.p df, 2006.