Indagini informatiche e acquisizione della prova nel processo penale

Fabio Bravo[•]

Riassunto
Questo articolo si propone di esaminare le novità introdotte dalla Convenzione di Budapest sul *Cybercrime* e dalla legge italiana di ratifica (legge 48/2008). L'attenzione viene concentrata soprattutto sull'impatto relativo alle indagini informatiche ed all'acquisizione della prova nel processo penale. Viene passata in rassegna anche la giurisprudenza precedente all'entrata in vigore della legge. Le decisioni dell'autorità giudiziaria mostrano un andamento incerto ed altalenante, che non sempre aderisce alle istanze della *computer forensics*. Benché il legislatore abbia ora recepito in più articoli del codice di procedura penale i principi della *computer forensics*, occorrerà verificare come tali principi verranno attuati nella prassi.

Résumé
Cet article examine les innovations introduites par la Convention de Budapest sur la cybercriminalité et la ratification par la loi italienne (loi n° 48/2008). L'attention se porte principalement sur l'impact de cette loi sur les enquêtes informatiques et l'acquisition d'éléments de preuve dans un procès pénal. Après quoi, l'auteur passe en revue la jurisprudence avant l'entrée en vigueur de la loi. Les décisions des tribunaux sont très différentes et elles n'adhèrent pas toujours aux exigences des preuves informatiques («*computer forensics*»). Bien que loi italienne n° 48/2008 ait désormais mis en œuvre les principes de l'informatique judiciaire en créant plusieurs articles au sein du Code de procédure pénale («*computer forensics*»), il sera nécessaire de vérifier comment ces principes seront mis en pratique.

Abstract
This article aims to examine the new regulations introduced by the Budapest Convention on Cybercrime and the Italian Ratification Law No. 48/2008. Attention is focused primarily on the impact on computer investigation and the acquisition of evidence in criminal proceedings. The article also analyzes some relevant Italian Court decisions, in which we can find an uncertain and fluctuating trend as regards elements and principles of computer forensics. Although the Italian law has now implemented several articles of the Criminal Procedure Code, the principles of computer forensics, it will be necessary to verify how these principles will be implemented in practice.

[•] Avvocato esperto in diritto delle nuove tecnologie. Professore aggregato in «Criminalità e tecniche investigative» e ricercatore presso l'Università di Bologna. Dottore di ricerca in «Informatica giuridica e diritto dell'informatica» (www.fabiobravo.it)

1. Le novità introdotte dalla legge italiana di ratifica della Convenzione di Budapest sul *Cybercrime* (legge n. 48/2008).

La Convenzione di Budapest sulla criminalità informatica, com'è noto, è stata resa dal Consiglio d'Europa in data 23 novembre 2001 ed è stata ratificata ed attuata dall'Italia solamente in tempi recenti, con la legge 18 marzo 2008 n. 48, pubblicata in Gazzetta Ufficiale 4 aprile 2008 n. 80, S.O. n. 79[1].

Le principali novità introdotte nel nostro ordinamento hanno riguardato, tra l'altro:

a) l'omogeneizzazione delle scelte normative a livello internazionale, in ambito comunitario ma non solo, per il contrasto alla criminalità in generale e a quella informatica in particolare[2];

b) la riorganizzazione, nel codice penale, dei c.d. reati informatici (dopo la novellazione avutasi tramite la legge n. 547 del 1993[3]), con interventi ora modificativi ed integrativi[4], ora di introduzione *ex novo* di specifici illeciti[5];

c) l'estensione della responsabilità degli enti derivante da reato *ex* d.lgs. 231/201 a diverse ipotesi di reato informatico contemplate nel codice penale, così come novellate dalla legge n. 48/2008 di ratifica della Convenzione di Budapest[6];

---

[1] L'esigenza di rinnovamento volta a contrastare gli sviluppi tumultuosi della criminalità informatica è stata avvertita, prima ancora che in dottrina e a livello politico e legislativo, anche dagli operatori del settore. Si veda al riguardo, il contributo di Apruzzese A., "The present cybercrime: operational and instructive experiences", in Sette R., *Cases on technologies for teaching criminology and victimology. Methodologies and practices*, IGI Global – Information Science Reference, Hershey, 2010, pp. 195 e ss.

[2] Si noti che la Convenzione di Budapest contiene una serie di definizioni che, tuttavia, sono state volutamente messe dal legislatore italiano in sede di ratifica della Convenzione medesima. La riproduzione dell'assetto definitorio nelle legislazioni nazionali avrebbe avuto il merito di determinare un maggior grado di omogeneizzazione tra le normative dei vari Stati. La scelta italiana, tuttavia, sembra dipesa dal timore che le definizioni, in una materia suscettibile di rapida obsolescenza, avrebbe avuto l'effetto di imbrigliare eccessivamente l'interprete in sede di applicazione del dettato normativo. Si consideri, a tal fine, che il testo italiano di recepimento della Convenzione in parola è stato reso a quasi sette anni di distanza dall'emanazione della Convenzione e, in ambito tecnologico, l'arco temporale è estremamente significativo.

[3] Per una sintetica disamina si veda, al riguardo, Bravo F., "Crimini informatici e mezzi di ricerca della prova nella conduzione delle indagini", in *Rivista giuridica di polizia*, 1998, n. 6, pp. 711-738.

[4] Secondo un approccio ormai maturo, sia la Convenzione che la legge italiana di recepimento prendono atto ormai che la categoria dei reati informatici deve essere estesa anche ai c.d. *computer related crimes*, giacché anche i reati non strettamente informatici (es. peculato d'uso) possono essere commessi con l'uso di strumenti informatici.

[5] Quanto all'introduzione *ex novo* di reati ad opera della legge n. 48/2008 si veda ad esempio l'art. 640 *quinques* c.p., rubricato «*Frode informatica del soggetto che presta servizi di certificazione di firma elettronica*», ove si trova stabilito che «Il soggetto che presta servizi di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro».

[6] In relazione al tema della responsabilità degli enti derivante da reato, qualora commesso dai soggetti che si trovano nella struttura apicale o dai loro sottoposti, v'è da sottolineare che, con riferimento ai *computer crimes* o ai *computer related crimes*, potrebbe essere frequentemente applicata la norma, contenuta nell'art. 8 del d.lgs. 231/2001, in base alla quale la responsabilità sussiste anche ove non sia stato individuato l'autore dell'illecito. A tal fine sarebbe sufficiente, ad esempio in caso di reato commesso tramite Internet, individuare la macchina e l'utenza da cui le operazioni vengono effettuate, agevolmente identificabile attraverso il numero IP, anche dinamico, assegnato in un determinato momento dall'ISP (*Internet Service Provider*), a prescindere dall'individuazione del soggetto che effettivamente ha eseguito le operazioni costituenti illecito penale. Non

d) l'istituzione, nello stato di previsione del Ministero dell'Interno, del fondo per il contrasto della pedopornografia su Internet e per la protezione delle infrastrutture informatiche di interesse nazionale, con una dotazione di due milioni di Euro annui a partire dall'anno 2008[7];

e) la novellazione dell'art. 132 del d.lgs. 196/2003 (Codice in materia di protezione dei dati personali), con modifica significativa della disciplina della *data retention*, destinata tuttavia ad essere ulteriormente riformata a seguito dell'entrata in vigore dei provvedimenti legislativi annunciati dal governo in ottemperanza alla direttiva 2006/24/CE (c.d. Direttiva Frattini), con particolare riferimento al d.lgs. n. 109/2008 che ne ha dato attuazione;

f) la cooperazione e la mutua assistenza tra gli Stati aderenti alla Convenzione (Stati membri e altri Stati firmatari);

g) la modifica del codice di procedura penale, con introduzione di norme volte a disciplinare l'acquisizione della prova in ambiente informatico o telematico e l'utilizzo corretto degli strumenti di ricerca e di acquisizione della stessa, con evidenti conseguenze sui criteri che dovranno essere utilizzati dal giudice per la valutazione degli elementi probatori[8].

---

varrebbe ad escludere la responsabilità dell'ente, infatti, la mancata individuazione del soggetto che sia stato materialmente autore della condotta integrante l'ipotesi di reato-presupposto considerata al fine dell'applicazione della responsabilità *ex* d.lgs. 231/201. Giova peraltro rimarcare che la responsabilità in questione richiede che l'ente abbia percepito o goduto di un vantaggio derivante dal reato-presupposto, il che non pare sia facilmente verificabile per tutti i reati-presupposto indicati dalla legge di ratifica della Convenzione di Budapest. Ciò non deve però portare a sottovalutare, con riferimento ai *computer crimes* ed ai *computer related crimes*, l'importanza dell'adozione di efficaci modelli organizzativi per la gestione e prevenzione dei rischi di commissione del reato, in quanto, al di là dell'efficacia scriminante, tali modelli possono comunque essere adottati per incrementare gli standard di sicurezza e di efficacia organizzativa interna, nonché per assestarsi su *policies* di CSR (*Corporate Social Responsibility*) di alto profilo.

[7] Il Centro Nazionale Anticrimini Informatici per la Protezione delle Infrastrutture Critiche (CNAIPIC) è stato istituito formalmente con il d.l. 144/205 (c.d. Decreto Pisanu), convertito in legge 155/2005. Per anni, tuttavia, la legge è rimasta lettera morta, in attesa della dotazione economica necessaria per il suo funzionamento. Tale dotazione è stata prevista proprio con la legge 48/2008 di recepimento della Convenzione di Budapest, a seguito della quale il CNAIPIC è divenuto operativo, per decreto del Capo della Polizia del 7 agosto 2008. L'istituzione del CNAIPIC ha come suo presupposto la constatazione della estrema vulnerabilità della nostra società, ormai basata sull'uso di sistemi informatici e telematici (*Information Society*). La gestione del rischio di attacchi criminali o terroristici, in quest'ottica, diventa un fattore determinante per la difesa dello Stato e degli interessi nazionali, nonché per la protezione dei cittadini e della sicurezza pubblica. Il CNAIPIC, dunque, prevede misure di controllo e monitoraggio della rete che finiscono per tradursi in un sofisticato sistema di controllo sociale di tipo tecnologico. La pervasività del sistema di controllo è notevole, se si pensa che l'azione del CNAIPIC è molto estesa e lascia margini ampi di discrezionalità al Ministro dell'Interno in ordine all'individuazione di obiettivi pubblici o privati, anche non tipizzati preventivamente. L'azione di controllo, tra l'altro, può essere esercitata *motu proprio* dal CNAIPIC, senza alcuna necessità di denuncia e, addirittura, si avvale della possibilità di impiegare strumenti investigativi preventivi, finanche a porre in essere intercettazioni, anche telematiche, precedenti alla commissione del reato o dell'attacco temuto o ipotizzato. Cfr., sul punto, le riflessioni dal sottoscritto già riportate su *Information Society & ICT Law* (www.informationsociety.it) all'URL http://internetsociety.wordpress.com/2009/05/23/centro-anticrimini-informatici-per-la-protezione-delle-infrastrutture-critiche-cnaipic/ (permalink consultato e verificato, da ultimo, in data 28.12.2009).

[8] La *computer forensics* richiede l'applicazione di corrette procedure per l'acquisizione della prova, tra le quali vi sono quelle volte alle seguenti attività: documentazione delle operazioni; individuazione univoca del *file* per garantire la non ripudiabilità; corretta conservazione, con particolare attenzione a tutta la c.d. catena della custodia; inalterabilità o immodificabilità o verifica della mancata alterazione e della mancata modificazione; rispetto delle garanzie di difesa, con riferimento, ad esempio, all'accertamento tecnico che, quantomeno per le particolari modalità con cui viene eseguito, dovesse essere tecnicamente ritenuto irripetibile ai sensi dell'art. 360 c.p.p. Per un inquadramento teorico sulla *computer forensics* si segnala Luparia L., Ziccardi G., *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Giuffrè,

Benché tutti gli evidenziati punti siano rilevanti ai fini del nostro discorso, gli aspetti su cui maggiormente devono incentrarsi le riflessioni relative all'impatto della normativa in esame sulla *digital forensics* sono gli ultimi tre, contrassegnati con le lett. e), f) e g).

Il più ampio tema della sicurezza nel settore ICT (*Information and Communication Technology*), invece, non può prescindere ora dalla predisposizione dei modelli organizzativi e dei sistemi di controllo di cui al d.lgs. 231/2001. Al riguardo la riforma impone di verificare in che modo gli stessi debbano essere predisposti e/o aggiornati per tener conto dell'esigenza di prevenzione (*rectius*, di gestione del rischio relativo alla possibile commissione) dei nuovi reati-presupposto indicati dalla legge di ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica. Sotto tale ultimo profilo rileverebbero gli argomenti individuati sub lett. *b)* e *c)*. In tema di sicurezza informatica, altresì, è di particolare importanza il riferimento alla protezione delle infrastrutture critiche informatiche di interesse nazionale di cui all'art. 7 del d.l. n. 144/2005, convertito con modificazione nella legge n. 155/2005, con riguardo al quale significativo è l'apporto economico garantito dal fondo istituito con la legge n. 48/2008, indicato alla lett. d), dell'elenco che precede.

2. L'orientamento della giurisprudenza italiana di fronte alle questioni probatorie connesse all'uso delle tecnologie informatiche e telematiche prima dell'entrata in vigore dalla legge n. 48/2008 di recepimento della Convenzione di Budapest sul Cybercrime.

Le pubbliche autorità deputate all'accertamento del crimine ed, in particolare, gli organi investigativi e di polizia giudiziaria non sempre purtroppo padroneggiano le *best practices* e le *guideline* suggerite dagli studiosi di *digital forensics*, il che si traduce spesso, per chi esercita l'azione penale, nell'impossibilità di sostenere il capo di imputazione in fase dibattimentale o, addirittura prima in sede di riesame avverso i provvedimenti relativi all'adozione ed all'esecuzione di misure cautelari reali (e talvolta personali), nell'impossibilità di sorreggere il risultato raggiunto in termini di reperimento ed acquisizione della prova[9].

A tale situazione fa eco, spesso, anche una sottovalutazione, da parte di alcuni magistrati con funzioni giudicanti, dell'importanza si vagliare le prove alla luce degli standard, delle procedure, dei parametri, dei principi e delle acquisizioni teoriche della *computer forensics* (o, più in generale, della *digital forensics*), con conseguente

Milano, 2007. In materia si veda anche Ghirardini A., Fagioli G., *Computer forensics*, Apogeo, Milano, 2007.

[9] La *computer forensics* non è una disciplina che rileva solamente in occasione dei *computer crimes*, dei *cybercrimes* o dei *computer related crimes*, ma è una disciplina che rileva anche con riguardo ai reati comuni, addirittura l'omicidio o, ancora, al reato di associazione mafiosa *ex* art. 416 *bis* c.p., qualora l'indagine sugli strumenti elettronici sia necessaria a fini investigativi o difensivi. Si pensi, ad esempio, al ruolo nevralgico degli accertamenti tecnici di *computer forensics* sul *computer* di Alberto Stasi con riferimento all'omicidio di Chiara Poggi a Garlasco, al fine di verificare l'alibi invocato dalla difesa (Stasi, infatti, aveva sostenuto di aver lavorato alla sua tesi con il *computer* nell'ora in cui la vittima era stata uccisa). Si pensi, ancora, al caso relativo all'accertamento tecnico eseguito sulla copia dei *files* estratti dall'*hard disk* del *computer* di un soggetto indagato per il reato di cui all'art 416 *bis* c.p. in quanto ritenuto appartenente al Clan camorristico dei Casalesi, nei cui confronti erano stati ritenuti sussistenti i gravi indizi di colpevolezza necessari per l'applicazione della misura della custodia cautelare in carcere. Si veda, *amplius*, le brevi annotazioni alla sentenza della C. Cass. n. 14511/2009, di cui si darà conto nel prosieguo.

compressione delle effettive garanzie di difesa dell'indagato o dell'imputato.

Altri giudici, invece, si sono mostrati ben più attenti all'impostazione suggerita dalla disciplina della *digital forensics*, escludendo la rilevanza probatoria di elementi acquisiti in maniera superficiale e senza il rispetto delle minime esigenze di garanzia in ordine alla individuazione e corretta acquisizione, conservazione, custodia ed immodificabilità della prova.

L'esame della casistica giurisprudenziale denota, infatti, atteggiamenti altalenanti, non univoci ed ondivaghi sul punto[10].

Si pensi, ad esempio, alla valutazione processuale:

a) della stampa su carta di pagine Web;

b) dei *file* di *log* e di altri dati, relativi al numero IP assegnato all'utente (anche ove si tratti di IP dinamico), all'individuazione dell'identità dell'utente a cui tale IP risulti assegnato in un dato momento, ai tempi di connessione, all'individuazione delle pagine visitate e dei loro contenuti, *etc.*, forniti dagli *Internet Service Providers* (ISP) o dai gestori di telecomunicazione, anche telefonici, a richiesta delle autorità, senza l'effettuazione di specifici controlli e senza contraddittorio dell'indagato o dell'imputato;

c) ecc.

Si pensi, poi, ai casi di perquisizione e sequestro di materiale informatico, con riferimento:

a) all'intero *hard disk* o altre unità di memoria (es.: *pen drive*) usati dall'indagato o da terzi;

b) all'intero sistema informatico (es.: PC, *Server*);

c) all'intero sito Web (o dell'intero *forum*) in caso di diffamazione o altri illeciti penali, compreso quelli inerenti alla messa a disposizione del pubblico di opere protette dalla normativa sul diritto d'autore su sistemi di *filesharing* (*Peer-to-Peer*; *Bit-Torrent*), senza il consenso degli aventi diritto[11];

---

[10] L'analisi delle pronunce giurisprudenziali va apprezzato, nell'ambito del discorso che si sta conducendo, come un prezioso metodo di ricerca con analisi di tipo qualitativo, in grado di far emergere l'approccio e l'efficacia degli strumenti di accertamento della criminalità con riferimento ai reati nei quali entra in rilievo, a diverso titolo, lo strumento elettronico. Ovviamente il metodo di ricerca è utile per condurre un esame interdisciplinare, che coinvolga sia la prospettiva criminologica, sia la prospettiva giuridica, sia la prospettiva informatico-giuridica *tout court*.

[11] Peraltro, proprio in materia di sequestro di sito Internet utilizzato per consentire da parte degli utenti il *filesharing* di opere protette dal diritto d'autore, senza gli aventi diritto, ottenendo profitto sia dall'esposizione di *banners* pubblicitari (di imprenditori attratti dall'elevatissimo numero di utenti che visitavano il sito), sia da quanti erano disposti a versare somme, ancorché di lieve entità, per derogare favorevolmente alle *policies* di utilizzo del servizio offerto dal sito, è celebre il caso noto come «*The Pirate Bay*», su cui recentemente si è espressa la Corte Suprema di Cassazione con sentenza n. 49437/2009, ammettendo la liceità della statuizione con cui l'autorità giudiziaria, in sede di sequestro *ex* art. 321 c.p.p., ha ordinato a tutti gli *Internet Service Providers* (ISP) italiani, di inibire tecnicamente il traffico Internet dei propri rispettivi clienti verso il sito oggetto di sequestro. Stante la tipicità della misura cautelare reale, tuttavia, la Corte ha ricondotto l'inibitoria agli artt. 14, 15 e 16 del d.lgs 70/2003, di attuazione della direttiva 2000/31/CE (c.d. direttiva sul «commercio elettronico»). Segnatamente, nelle motivazioni della citata sentenza del Supremo Collegio si trova testualmente affermato che «in questa specifica materia (della circolazione di dati sulla rete informatica Internet) uno speciale potere inibitorio è assegnato all'autorità giudiziaria dagli artt. 14-16 d.lgs. 9 aprile 2003 n. 70, di attuazione della direttiva 2000/31/CE relativa ai servizi della società dell'informazione. Tale normativa speciale, nel prevedere in generale la libera circolazione (...) di tali servizi, quali quelli prestati dai provider per l'accesso alla rete informatica Internet, contempla anche, come deroga a tale principio, che la libera circolazione di un determinato servizio possa essere limitata con provvedimento dell'autorità giudiziaria per motivi attinenti all'opera di prevenzione, investigazione, individuazione e perseguimento di reati. In particolare gli art. 14, comma 3, 15, comma 3, e 16, comma 3, prevedono che l'autorità giudiziaria possa esigere, anche in via d'urgenza, che il prestatore del servizio impedisca o ponga fine alle violazioni commesse». Tali

d) ecc.

Si pensi, ancora, alla illegittimità o meno della duplicazione integrale (c.d. «clonazione», mediante *bitstream image*) del contenuto dell'intero *hard disk* fatto oggetto di sequestro probatorio, al fine di restituire l'*hard disk* originale al suo titolare, ma con apprensione di dati ed informazioni non pertinenti all'ipotesi di reato, suscettibili di rientrare nell'ambito della tutela accordata ai diritti fondamentali della persona, quali il diritto alla protezione dei dati personali ed alla riservatezza.

Tra i casi che si sono registrati nella prassi, alcuni dei quali recentemente approdati anche in cassazione, si segnalano, a titolo esemplificativo, i seguenti:

(1) caso vertente in materia di acquisizione di *files* di *log* da parte della polizia giudiziaria, mediante richiesta all'*Internet Service Provider* (ISP), con consegna da parte di quest'ultimo dei dati senza alcuna formale acquisizione e senza alcuna verifica in ordine alle modalità di conservazione degli stessi allo scopo di assicurare la genuinità e l'attendibilità nel tempo (Tribunale di Chieti, sentenza n. 175/2005. Il giudice non ha ritenuto attendibili, sotto il profilo probatorio, i *file* di *log* in questione ed i dati in essi contenuti);

(2) caso di mera riproduzione a stampa, effettuata dalla polizia giudiziaria, di pagine Web relative a materiale osceno (Tribunale di Pescara, sentenza n. 1369/2006. Il giudice ha ritenuto che le

---

disposizioni, precisa ulteriormente la Corte, «vanno lette unitamente al successivo art. 17; il quale esclude sì un generale obbligo di sorveglianza nel senso che il provider non è tenuto a verificare i dati che trasmette concretino un'attività illecita (...), ma – congiuntamente all'obbligo di denunciare l'attività illecita, ove il prestatore del servizio ne sia comunque venuto a conoscenza, e di fornire le informazioni dirette all'identificazione dell'autore dell'attività illecita – contempla che l'autorità giudiziaria possa richiedere al prestatore di tali servizi di impedire l'accesso al contenuto illecito (art. 17, comma 3)». Sulla scorte di tale ragionamento la Corte di Cassazione giunge dunque a sostenere che «La lettura congiunta di tali disposizioni consente di affermare che sussiste un potere inibitorio dell'autorità giudiziaria penale avente il contenuto di un ordine ai provider dei servizi suddetti di precludere l'accesso alla rete informatica Internet al solo fine di impedire la prosecuzione della perpetrazione del reato», che nella specie è stato ravvisato nell'art. 171-*ter*, co. 2, lett. *a-bis)*, della legge sul diritto d'autore. Al riguardo va però rammentato che nelle motivazioni del decreto dell'1 agosto 2008, con cui il G.I.P. del Tribunale di Bergamo ha disposto il sequestro preventivo ex art. 321 c.p.p. del sito Internet in questione, con ordine di inibizione del traffico di rete a tutti i *Providers*, dopo aver ricondotto l'attività di gestione del sito www.thepiratebay.org e simili «al paradigma delittuoso *ex* art. 171-*ter* [*sott.*: della legge sul diritto d'autore] con specifico riferimento alle previsioni del comma 2, lettera *a bis)*, di tale previsione incriminatrice», alla luce della considerazioni sulle modalità concrete di svolgimento del servizio di *filesharing*, accompagnato dal perseguimento delle finalità lucrative, ha ritenuto di aggiungere, altresì, che «(...) con riferimento alla posizione degli odierni indagati, può ravvisarsi almeno il *fumus* del reato di associazione per delinquere, in considerazione della chiara sussistenza di un sodalizio criminoso tra essi, con una ripartizione dei ruoli tendenzialmente definita e l'adozione di un preciso programma criminoso, precisato nei presupposti ideologici, nei contenuti, nella portata e nelle modalità operative. In relazione a tale ipotesi delittuosa, tuttavia, non vi sono attualmente elementi per ritenere la competenza territoriale dell'Autorità giudiziaria italiana. La struttura organizzativa, invero, appare organizzata e realizzata interamente all'estero, in quanto gli apparati informatici dei server come risulta dalle informazioni di pubblico dominio reperibili in Internet sono stati materialmente collocati dapprima in Svezia, quindi in Olanda e comunque, al momento, non vi è prova di una loro collocazione almeno parziale in territorio Italiano. Non può escludersi, invece, la competenza dell'Autorità giudiziaria italiana in ordine al reato di cui alla superiore incolpazione [*sott.*: art. 171-*ter*, co. 2, lett. *a-bis)*, della legge sul diritto d'autore], non essendo noto il luogo di consumazione delle singole condotte di illecito scambio e potendo ritenersi che almeno una parte degli scambi coinvolga utenti di nazionalità italiana o comunque operanti in Italia (il sito è agevolmente accessibile da qualsivoglia apparato informativo collocato nel territorio dello Stato, purché collegato alla rete Internet e le statistiche danno conto di una diffusione degli accessi su scala mondiale). Una simile considerazione appare vieppiù confortata dall'informativa della Guardia di Finanza di Bergamo datata 4 giugno 2008 (...)». Per uno specifico approfondimento su questi temi, in questo lavoro

riproduzioni a stampa, ancorché effettuate da ufficiali di polizia giudiziaria, sono da considerarsi di scarsa valenza probatoria, in quanto, trattandosi di copie originali presenti in forma digitale, ai fini della loro acquisizione e conservazione, per accertarne l'autenticità e l'integrità, si sarebbero dovute rispettare le **regole** tecniche dettate dall'AIPA, ora CNIPA. Stando alle motivazioni riportate nella citata sentenza, le stampe cartacee di pagine Web non possono essere qualificate, infatti, come originali analogici ma, a rigore, come copie di *files* digitali prodotte senza alcuna garanzia in ordine alla conformità agli originali medesimi, che invece si sarebbe potuta ottenere eventualmente usando la firma digitale);

(3) altro caso di riproduzione a stampa, effettuata dalla polizia giudiziaria, di pagine *web* contenenti un annuncio pubblicitario offensivo (Cass. Pen., sent. n. 46668/2007 del 14 dicembre 2007. La Corte ha ritenuto valida l'acquisizione delle pagine *web* effettuata dalla polizia giudiziaria nell'esercizio delle sue funzioni. La Corte, infatti, ha dichiarato in sentenza di non comprendere le doglianze della difesa con le quali la stessa, lamentandosi del mancato rispetto delle corrette procedure e delle corrette tecniche di P.G., adduceva che la copia di un qualsiasi documento, cartaceo o informatico, può essere oggetto di contraffazione e che le pagine Web possono essere generate e modificate con qualsiasi programma di videoscrittura, il che avrebbe consigliato al giudice del merito di acquisire la prova disponendo direttamente sul *server* dell'*Internet Service Provider* il sequestro dei *files* interessati);

(4) caso in materia di sequestro probatorio di un intero sistema informatico (PC e periferiche), in relazione al reato di detenzione di materiale pedopornografico scaricato da un sito Internet (Cass. Pen., sez. III, sent. n. 1778 del 18 novembre 2003, depositata il 3 febbraio 2004. La Corte ha ritenuto che, trattandosi di sequestro probatorio di cose pertinenti al reato e non di corpo del reato, la valutazione delle finalità probatorie in rapporto al reato ipotizzato esclude che possa essere assoggettato a sequestro il materiale informatico del tutto *neutro* rispetto alle indagini, quale, ad esempio, *scanner*, stampante, schermo. È stato invece ritenuto assoggettabile a sequestro il materiale consistente nella memoria fissa del PC, nonché nelle altre memorie o supporti contenenti elementi utili alle indagini, come *floppy* e CD-ROM, eventualmente rinvenibili. La Corte ha dunque ristretto il sequestro alla sola memoria, non anche alle altre parti, interne ed esterne, di cui si compone il *computer*);

(5) caso in cui viene negato il dissequestro, anche parziale, del materiale informatico c.d. «neutro» (tastiere, *mouse*, stampante, fax, *router*), nonostante tale materiale sia stato considerato alla stregua di cose pertinenti al reato ed oggetto a sequestro probatorio (Cass. Pen., sent. n. 13792 del 5 marzo 2008, depositata il 3 aprile 2008);

(6) caso di sequestro probatorio di *pen drive* (Cass. Pen., sent. n. 18897 ddel 2 aprile 2008, depositata il 9 maggio 2008);

(7) caso relativo a perquisizione e analisi tecniche dei contenuti di un disco rigido senza adottare procedure e misure tecniche volte ad assicurare la ripetibilità delle operazioni (Tribunale di Bologna,

solamente accennati stante le esigenze di economia del presente discorso, si rinvia fin d'ora ad altra sede.

sent. n. 1823/2005, ove si è sostenuto che, in assenza di allegazione, da parte della difesa, dei fatti e degli elementi da cui desumere che vi siano state alterazioni dei dati sul sistema, non v'è ragione di mettere in dubbio la validità probatoria dei risultati a cui la polizia giudiziaria e gli ausiliari del giudice pervengono utilizzando tecniche forensi diverse da quelle ritenute scientificamente più corrette. Il caso affrontato dal Tribunale di Bologna, noto come «caso Vierika», è successivamente approdato in Corte di Appello. All'esito del secondo grado di giudizio la Corte di Appello di Bologna ha reso la sentenza n. 369/2008 con la quale, pur mitigando la condanna in revisione del giudizio di primo grado non ritenendo sussistente l'aggravante del danneggiamento di sistemi informatici di cui all'art. 615 *ter* c.p., ha rigettato i motivi di appello basati sulla mancata osservanza delle migliori procedure di *computer forensics*, negando l'ammissibilità della perizia, dando rilievo probatorio soddisfacente alle dichiarazioni della polizia giudiziaria ed alle deposizioni tecniche del personale del *provider*, ed ai dati consegnati dal *provider* alla polizia giudiziaria, che la Corte di Appello, nonostante le contestazioni della difesa, ha ritenuto incontestabili perché pacificamente accettati dal medesimo imputato in occasione della sua audizione in fase dibattimentale);

(8) caso relativo ad accertamento tecnico eseguito sulla copia di documenti informatici (*files*) estratti dall'*hard disk* di un *computer* in assenza delle garanzie previste dall'art. 360 c.p.p. per l'accertamento tecnico non ripetibile. In particolare la Corte di Cassazione, con sentenza n. 14511/2009 (depositata in cancelleria il 2 aprile 2009), aveva rigettato il ricorso avverso l'ordinanza del Tribunale del Riesame di Napoli con la quale, respingendo la richiesta di riesame, aveva confermato l'ordinanza con cui era stata disposta la misura della *custodia cautelare in carcere* per il ricorrente, in relazione all'ipotesi di associazione di tipo mafioso e simili, di cui all'art. 416 *bis* c.p., per il quale era indagato. Nella fattispecie, a supporto della decisione presa dal Tribunale del Riesame, erano stati ritenuti sussistenti i gravi indizi di colpevolezza richiesti per l'applicazione della misura cautelare personale non solo sulla base delle dichiarazioni di alcuni collaboratori di giustizia e di talune sentenze, acquisite ai sensi dell'art. 238 *bis* c.p.p., che attestavano l'operatività del gruppo camorristico denominato «Clan dei Casalesi» (al quale apparteneva il soggetto nei cui confronti era stata disposta la misura cautelare personale), ma anche sulla base delle risultanze della *perquisizione domiciliare*, nell'ambito della quale erano stati rinvenuti anche numerosi rilevanti *documenti su supporto informatico*. Questi ultimi, stando a quanto riportato in sentenza, erano stati considerati indicativi «della corresponsione periodica e sistematica di somme di denaro ad alcuni soggetti – tra cui il ricorrente, indicato con la sigla "A. 1500 sorveglianza" – i cui nominativi erano ordinatamente suddivisi per sottogruppi di appartenenza, nonché di missive ed annotazioni concernenti la corrispondenza intrattenuta da S.V., detto "*(omissis)*" , con altri sodali, avente ad oggetto consigli e informazioni sulle vicende dei vari membri del gruppo, indicazioni relative ad attività estorsione e controllo dei giuochi d'azzardo ed altri aspetti attinenti alla operatività dell'associazione». Tra i principali motivi del ricorso – proposto innanzi al Tribunale del

Riesame e poi reiterato anche innanzi alla Corte di Cassazione sotto il profilo sia della violazione di legge, con riguardo agli artt. 360 c.p.p. e 117 disp. att. c.p.p., sia del difetto di motivazione – v'era proprio quello concernente l'asserita natura irripetibile degli accertamenti svolti, consistenti nell'attività di estrazione di copia di *files* dal *computer*. La procura, infatti, aveva proceduto all'estrazione di copia della documentazione informatica (*files*) dall'*hard disk* del *computer* del ricorrente, senza osservare le garanzie previste dagli articoli sopra citati. Le doglianze della difesa, passate al vaglio della Suprema Corte, non hanno però retto, dal momento che la stessa, nella sentenza in parola, ha affermato il principio secondo cui «è da escludere che l'attività di estrazione di copia di *file* da un *computer* costituisca un atto irripetibile (...), atteso che non comporta alcuna attività di carattere valutativo su base tecnico-scientifica né determina alcuna alterazione dello stato delle cose, tale da recare pregiudizio alla genuinità del contributo conoscitivo nella prospettiva dibattimentale, essendo sempre comunque assicurata la riproducibilità di informazioni identiche a quelle contenute nell'originale» (C. Cass., sent. n. 14511/2009)[12].

La casistica potrebbe continuare.

È chiaro che un simile altalenante ed incerto modo di procedere da parte della giurisprudenza deve essere corretto a livello legislativo, non solo per il nostro ordinamento giuridico, ma anche nell'ottica della cooperazione internazionale quantomeno su scala europea, tentando di rendere omogenee procedure, prassi, decisioni, che aprano la strada ad un più rigoroso recupero del principio di certezza del diritto o, se non altro, ad un più serio standard di valutazione della prova, a garanzia dei diritti fondamentali del cittadino e del migliore funzionamento della giustizia.

3. Mutamenti dello scenario investigativo e processuale a seguito dell'entrata in vigore della legge n. 48/2008 di recepimento della Convenzione di Budapest sul *cybercrime*.

Lo scenario investigativo e processuale, caratterizzato da prassi e indirizzi giurisprudenziali ondivaghi ed oscillanti, è stato stravolto da alcuni principi chiaramente ricavabili dalle norme penalprocessualistiche novellate dalla legge n. 48/2008, che costringe ora l'interprete in generale ed il magistrato in particolare a confrontarsi con indicazioni che appaiono orientate in maniera evidente al recepimento di istanze provenienti dalla cultura scientifica della *computer forensics*.

[12] Significativamente la Suprema Corte di Cassazione, nelle motivazioni della sentenza n. 14511/2009, ha altresì aggiunto il rilievo secondo cui «Il provvedimento di acquisizione di copia di *file* ritenuti utili ai fini delle indagini è disciplinato dall'art. 258 c.p.p. ed ha natura autonoma e distinta rispetto alla misura cautelare reale del sequestro (Cass., Sez. Un., 24 aprile 2008, n. 18253). Nell'ipotesi in cui la capacità rappresentativa della *res* sia fornita dal contenuto dell'atto o del documento, l'Autorità giudiziaria procedente acquisisce al procedimento le copie di detti atti o documenti, disponendo la restituzione degli originali; laddove, invece, l'elemento probatorio sia infungibilmente rappresentato dall'originale del supporto cartaceo o magnetico, si determinano i presupposti per il mantenimento del sequestro. Dal disposto dell'art. 258 c.p.p. non è, comunque, ricavabile un'impostazione legislativa ispirata alla regola della *best evidence*, per la quale dovrebbe essere privilegiata l'acquisizione dei documenti in originale. Relativamente all'estrazione di copie non è esperibile una procedura incidentale di controllo di legittimità, in quanto non si è in presenza di un vincolo di indisponibilità del bene equipollente al sequestro. È, però, sempre possibile per la parte far valere eventuali nullità relative all'osservanza delle forme previste a garanzia dell'esercizio dei diritti di difesa nella fase in cui i predetti documenti vengono

Nel fornire una ricostruzione dei principi desumibili dalle norme in questione, si propone la seguente classificazione, delineata per elementi tematici fondamentali, volta a cogliere gli aspetti che ci sembrano maggiormente rilevanti delle novità apportate dalla legge italiana di ratifica della Convenzione di Budapest:

(1) **cooperazione internazionale.** In particolare, in tema di *data retention*, l'art. 132, co. 4 *ter*, d.lgs. 196/2003 (Codice di protezione dei dati personali), così come novellato dalla legge n. 48/2008 di recepimento della Convenzione sul *cybercrime*, prevede che il Ministro dell'interno, in proprio o tramite i soggetti delegati (quali i soggetti responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei Carabinieri e del Corpo della Guardia di Finanza, salvo altri), anche su eventuali richieste avanzate dalle autorità investigative straniere, possa ordinare ai fornitori ed agli operatori di servizi informativi o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, salvo proroga fino a complessivi sei mesi per motivate esigenze, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive ovvero di accertamento e repressione di specifici reati[13];

(2) **competenza nello svolgimento delle indagini e nell'esercizio dell'azione penale** (per i reati previsti dagli artt. 600 *bis*, *ter*, *quater*, *quater.1*, *quinquies*; 615 *ter*, *quater*, *quinquies*; 617 *bis*, *ter*, *quater*, *quinquies*, *sexies*; 635 *bis*, *ter*, *quater*; 640 *ter*, *quinquies*). Lo svolgimento delle indagini e dell'esercizio dell'azione penale in capo all'Ufficio del Pubblico Ministero presso il Tribunale del Capoluogo del distretto di Corte di Appello nel quale ha sede il giudice competente, appare ordinato ad ottenere un migliore coordinamento delle azioni investigative e penali per contrastare i reati informatici. Sarebbe stato preferibile, però, accompagnare tale previsione con l'istituzione di un ufficio di coordinamento investigativo centrale a livello nazionale, similmente a quanto avviene per la lotta alla mafia[14]. Vistose criticità si sono registrate sul

utilizzati come mezzo di prova (Cass., Sez. 6, 15 settembre 1995, in Cass. pen. 1996, p. 2328)».

[13] Il tema della cooperazione internazionale nell'ambito della criminalità informatica è stato indagato, recentemente, da Colombo E., "La cooperazione internazionale nella prevenzione e lotta alla criminalità informatica: dalla Convenzione di Budapest alle disposizioni nazionali", in *Ciberspazio e diritto*, 2009, n. 3/4, pp. 285-304, a cui *amplius* si rinvia.

[14] Sulla competenza delle procure distrettuali per i reati informatici si veda, *amplius*, Corasaniti G., "Commento all'art. 11 (Competenza) della legge 48/2008", in Corasaniti G., Corrias Lucente G. (a cura di), *Cybercrime, responsabilità degli enti, prova digitale. Commento alla Legge 18 marzo 2008, n. 48*, Cedam, Padova, 2009, pp. 245 e ss., il quale rimarca come l'intervento normativo abbia ricalcato, «in buona sostanza, il contenuto dell'art. 51, comma 3 *quater*, del codice di procedura penale (introdotto dall'art, 10 *bis* del D.L. n. 374/2001, convertito in legge n. 438/2001), che ha attribuito alle Procure Distrettuali la competenza per i reati di terrorismo in tutto il territorio del distretto, alla stregua di quanto previsto dall'art. 51 comma 3 *bis* del codice di procedura penale, introdotto dalla legge 20 gennaio 1992 n. 8 che ha istituito le procure distrettuali antimafia. Già con l'istituzione delle procure distrettuali in materia di terrorismo (art. 10 *bis* della legge 15 dicembre 2001 n. 438), si era anche manifestata immediatamente l'esigenza di realizzare una banca dati in grado di gestire tutte le informazioni acquisite nell'ambito dell'attività investigativa, con specifico riguardo alle attività di gruppi legati al terrorismo internazionale. Anche per tali organismi è stata più volte sollecitata l'esigenza di un efficace coordinamento informativo a livello interno in modo da realizzare esigenze investigative comuni e di non frammentare eccessivamente le iniziative processuali, garantendo nel contempo l'interscambio di informazioni essenziali agli inquirenti». Precisa altresì l'A. cit. che «Il legislatore ha forse perso l'occasione della istituzione di un organismo centrale di coordinamento unico, che sembra ancor più indispensabile nella materia della criminalità

piano investigativo, nel primissimo periodo di applicazione della legge, per le indagini in corso, in quanto inizialmente la legge 48/2008, nel modificare la competenza, non ha provveduto ad emanare norme transitorie che assicurassero il mantenimento della competenza per le indagini in corso agli Uffici del Pubblico Ministero presso i Tribunali locali, secondo le norme previgenti. A porre rimedio a tale inconveniente, frutto della disattenzione del legislatore, è intervenuta la legge 24 luglio 2008 n. 125, la quale, nel convertire in legge con modificazioni il decreto legge 23 maggio 2008 n. 92, ha introdotto l'art. 11 *bis* con cui si è stabilito che le nuove norme sulla competenza, previste ora dall'art. 51, co. 3-*quinquies*, c.p.p. «si applicano solo ai procedimenti iscritti nel registro di cui all'art. 335 del codice di procedura penale successivamente alla data di entrata in vigore della (...) legge» n. 48/2008, di recepimento ed attuazione della Convenzione di Budapest sul *Cybercrime*. Tuttavia, nell'originario testo di tale legge «risultava mancante ogni riferimento al Giudice [sia] per le indagine preliminare che per l'udienza preliminare, così come ogni riferimento a meccanismi di possibile decentramento predibattimentale o dibattimentale, alla stregua delle previsioni dell'art. 51, comma 3-*ter*, (introdotto proprio dalla normativa antimafia) che prevede che nei casi previsti dal comma 3-*bis*, se ne fa richiesta il procuratore distrettuale, il procuratore generale presso la Corte di Appello può, per giustificati motivi, disporre che le funzioni di pubblico ministero per il dibattimento siano esercitate da un magistrato designato dal procuratore della Repubblica presso il giudice competente. Tale prescrizione è stata introdotta solo più tardi con l'art. 2, 1° comma, della Legge 24 luglio 2008, n. 125 "Conversione in legge, con modificazioni, del decreto-legge 23 maggio 2008,

informatica. La stessa qualificazione dei magistrati appartenenti al gruppo lascia trasparire una forte esigenza di specializzazione tecnica, peraltro, richiesta dal Consiglio d'Europa sin dal 1995 con la Raccomandazione n. R (95) 13 dell'11.9.95 del Consiglio dei Ministri agli Stati membri relativa ai problemi di procedura penale legati alla tecnologia dell'informazione (...). È ben evidente che la Raccomandazione del 1995 non può risolversi solo con un mero richiamo generico alla formazione di unità di polizia giudiziaria specializzate, la cui esistenza peraltro è assolutamente indispensabile, ma implica una *specializzazione tecnica e giuridica della magistratura inquirente*, chiamata a confrontarsi con le tecnologie in evoluzione e con reati commessi in ambiente transnazionale, ai fini dell'efficace esercizio dell'azione penale e della non dispersione delle preziose esigenze di indagine, motivazioni peraltro già riconosciute in Italia con la creazione delle Procure antimafia istituite sia a livello nazionale che a livello distrettuale con la legge 20 gennaio 1992 n. 8 con il compito di coordinare, in ambito nazionale, le indagini relative alla criminalità organizzata, nell'ambito del disegno organizzativo fortemente voluto da Giovanni Falcone». La connessione tra lotta alla criminalità informatica, nei suoi più moderni connotati, e lotta alla criminalità organizzata è messa in evidenza con forza anche nelle ulteriori righe dell'A. poc'anzi citato, il quale ci tiene ad aggiungere che «D'altronde vi è una chiara implicazione tra la qualificazione "tecnica" delle indagini giudiziarie che non può limitarsi solamente alla criminalità informatica "tradizionale", ma coinvolge settori in costante espansione economica e richiede i medesimi metodi già adottati efficacemente per la criminalità organizzata ed il terrorismo, e efficacia delle indagini medesime. Solo la particolare qualificazione tecnico giuridica dei magistrati inquirenti può, del resto, assicurare quel tempestivo raccordo con la polizia giudiziaria, altrettanto specializzata, che si risolve nella comprensione immediata del fenomeno denunciato e nella predisposizione, altrettanto rapida, dei necessari approfondimenti investigativi in un quadro tanto complesso che transnazionale. Solo la composizione altamente specializzata delle procure distrettuali può assicurare alle ordinarie attività degli uffici del pubblico ministero, specie nei centri urbani maggiormente interessati al fenomeno, quell'interscambio informativo che appare indispensabile per non sottovalutare sul nascere fenomeni criminali in espansione che si avvalgono delle tecnologie informatiche per conseguire o distribuire il profitto delle attività criminali ordinarie o per commettere in modo coordinato e ripetuto reati, coinvolgendo fasce sempre più ampie di popolazione (...)».

n. 92, recante misure urgenti in materia di sicurezza pubblica"»[15]. Tale legge, all'art. 2, ha inoltre «modificato (...) anche l'art. 328 c.p.p. introducendoci un comma 1-*quater*, che prevede che quando si tratta di procedimenti per i delitti indicati nell'art. 51, comma 3-*quinquies*, le funzioni di giudice per le indagini preliminari e le funzioni di giudice per l'udienza preliminare sono esercitate, salve specifiche disposizioni di legge, da un magistrato del tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente (...)»[16];

(3) **fornitori di servizi** (non solo postali, ma anche e soprattutto telegrafici, telematici e di telecomunicazioni). La legge in esame considera correttamente in maniera peculiare la posizione dei fornitori dei servizi postali, telegrafici, telematici e di telecomunicazioni, ben percependo il ruolo chiave che gli stessi possono svolgere nelle azioni di contrasto alla criminalità informatica (ma non solo) e nell'acquisizione della prova informatica. Al riguardo i principali interventi posti in essere dalla legge italiana di ratifica della Convenzione sul *cybercrime* riguardano:

a) la ***data retention*** (con riferimento all'obbligo di conservazione dei dati di traffico telefonico, dei dati relativi alle chiamate senza risposta e dei dati di traffico telematico; con riferimento altresì alla possibile soggezione ai provvedimenti del Ministero dell'interno, anche tramite i soggetti delegati, in ordine alla conservazione e protezione dei dati di traffico informatico e telematico per fini investigativi e di accertamento e repressione dei reati);

b) il **sequestro di corrispondenza** (con riferimento alla possibilità di procedere, presso tutti i fornitori di servizi – postali, telegrafici, telematici, di telecomunicazioni – al sequestro di qualunque oggetto spedito – lettere, pacchi, telegrammi, valori, altri oggetti di corrispondenza – anche se inoltrati per via telematica, non solo se v'è il sospetto che siano stati inviati dall'indagato o siano a lui spediti, anche sotto altro nome o tramite altre persone, ma anche qualora si ritenga che il predetto materiale possa avere una qualche relazione con il reato, anche se concernenti altri soggetti terzi come mittente e come destinatario)[17];

c) il **sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazione** (con particolare riferimento alla parte in cui la legge consente all'autorità giudiziaria di stabilire, per esigenze legate alla regolare fornitura dei servizi, che l'acquisizione dei dati sottoposti a sequestro «avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità», con contestuale obbligo del fornitore di «conservare e proteggere adeguatamente i dati originali»)[18];

[15] Corasaniti G., *op. cit.*, p. 249.
[16] Corasaniti G., *op. cit.*, p. 249.

[17] Cfr., al riguardo, l'art. 254, co. 1, c.p.c., così come modificato dalla legge n. 48/2008, ai sensi del quale «Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, *o* che *comunque* possono avere relazione con il reato».

[18] L'art. 254 *bis* c.p.p. prevede, infatti, che «L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per

(4) **procedure e tecniche di *computer forensics*.** La recente legge nostrana di ratifica e di esecuzione della Convenzione sul *cybercrime* fissa per la prima volta l'attenzione sulle modalità di acquisizione della prova informatica, alla luce delle conoscenze e delle metodologie a cui è pervenuta la disciplina scientifica della *computer forensics*. In particolare, si nota che:

a*)* nel *sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazione* si richiede che:

2. l'acquisizione avvenga mediante copia dei dati;
3. la copia dei dati informatici sia effettuata su adeguato supporto;
4. venga adottata ed osservata una procedura (un protocollo);
5. la procedura scelta assicuri la conformità dei dati copiati ai dati originali;
6. la procedura scelta assicuri l'immodificabilità dei dati copiati;
7. i dati originali siano conservati e protetti adeguatamente[19];

b) con riferimento al *dovere di esibizione e segreti* di cui all'art 256 c.p.p., come novellato dalla legge n. 48/2008, si richiede invece che la *copia dei dati, delle informazioni e dei programmi informatici* richiesti dall'autorità giudiziaria alle persone tenute al segreto (indicate negli artt. 200 e 201 c.p.p.) debba avvenire:

- su adeguato supporto;
- senza specificazione di altre modalità, tecniche e procedure da seguire o risultati da conseguire (diversamente dall'acquisizione dei dati dai fornitori di servizi informatici, telematici e di telecomunicazione)[20];

c) per ciò che attiene alle *operazioni connesse al sequestro*, l'art. 260 c.p.p. prevede l'apposizione del *sigillo* dell'ufficio giudiziario e delle *sottoscrizioni* dell'autorità giudiziaria e dell'ausiliario che la assiste, ma, in considerazione della particolare natura del sequestro attinente a *dati*, *informazioni* e *programmi informatici*, l'apposizione del sigillo e delle sottoscrizioni autografe può essere sostituita da:

- altro mezzo, anche di carattere elettronico o informatico;
- idoneo a indicare il vincolo imposto a fini di giustizia;

esigenze legate alla regolare fornitura dei medesimi servizi, che la loro *acquisizione* avvenga mediante *copia* di essi su *adeguato supporto*, con una procedura che assicuri la *conformità* dei dati acquisiti a quelli originali e la loro *immodificabilità*. In questo caso è, comunque, ordinato al fornitore dei servizi di *conservare* e *proteggere adeguatamente* i dati *originali*».

[19] Cfr., al riguardo, l'art. 254 *bis* c.p.p., già citato in nota, nonché, in senso pressoché analogo quanto agli adempimenti richiesti per soddisfare esigenze di *computer forensics*, l'attuale art. 260, co. 2, c.p.p., con cui si è stabilito che «L'autorità giudiziaria fa estrarre copia dei documenti e fa eseguire fotografie o altre riproduzioni delle cose sequestrate che possono alterarsi o che sono di difficile custodia, le unisce agli atti e fa custodire in cancelleria o segreteria gli originali dei documenti, disponendo, quanto alle cose, in conformità dell'art. 259. Quando si tratta di *dati*, di *informazioni* o di *programmi informatici*, la *copia* deve essere *realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità*; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria».

[20] Giova qui richiamare l'art. 256 c.p.p., ai sensi del quale, infatti, «Le persone indicate negli artt. 200 e 201 devono consegnare immediatamente all'autorità giudiziaria, che ne faccia richiesta, gli atti e i documenti, anche in originale se così è ordinato, nonché i *dati*, le *informazioni* e i *programmi informatici*, anche mediante *copia* di essi *su adeguato supporto*, e ogni altra cosa esistente presso di esse per ragioni del loro ufficio, incarico, ministero, professione o arte, salvo che dichiarino per iscritto che si tratti di segreto di Stato ovvero di segreto inerente al loro ufficio o professione».

d) in tema di *ispezioni e perquisizioni relative a sistemi informatici e telematici*, poi, gli artt. 244, co. 2, e 247, co. 1 *bis*, c.p.p. richiedono:

- che vengano adottate misure tecniche;
- che le misure tecniche assicurino la conservazione dei dati originali;
- che le misure tecniche impediscano l'alterazione dei dati (originali)[21].

Tali norme, che segnano una indiscutibile apertura alla *computer forensics*, fissano alcuni importanti paletti e, se si vuole, indefettibili *deliverables* che devono essere soddisfatti nelle dinamiche investigative e verificati in quelle processuali.

Si apre però la strada al discorso più propriamente tecnico dell'informatica giuridica, al cui cospetto tali principi, tali prescrizioni e, quindi, tali *deliverables* indefettibili, ora normativamente fissati, acquistano contenuti più certi, da sperimentare nella prassi e da mantenere aggiornati al vaglio del progresso scientifico e tecnologico, portando di volta in volta a sperimentare la tenuta e la validazione del dettato normativo finora considerato, alla scoperta di quei *bugs* che condurranno sicuramente a nuove migliori *releases* del testo di legge sul *cybercrime*.

[21] L'art. 244, co. 2, prevede infatti che in caso di ispezioni, ove il reato non abbia lasciato tracce o effetti materiali o qualora siano stati cancellati o rimossi, «L'autorità giudiziaria (...) può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a *sistemi informatici o telematici*, *adottando misure tecniche* dirette ad assicurare la *conservazione dei dati originali* e ad *impedirne l'alterazione*». In tema di *perquisizioni*, invece, l'art. 247, co. 1 *bis*, c.p.p. dispone che «Quando vi è fondato motivo di ritenere che *dati*, *informazioni*, *programmi informatici* o *tracce* comunque pertinenti al reato si trovino in un *sistema informatico o telematico*, *ancorché protetto da misure di sicurezza*, ne è disposta la *perquisizione*, *adottando misure tecniche* dirette ad assicurare la *conservazione dei dati originali* e ad *impedirne l'alterazione*». Si noti come, a differenza di quanto contemplato per l'*ispezione*, nella *perquisizione* si precisa in maniera esplicita che le attività investigative possono essere svolte sul *sistema informatico* nonostante la presenza di *misure di sicurezza*.

Bibliografia.

- Apruzzese A., "The present cybercrime: operational and instructive experiences", in Sette R., *Cases on technologies for teaching criminology and victimology. Methodologies and practices*, IGI Global – Information Science Reference, Hershey, 2010, pp. 195 e ss.
- Bravo F., "Crimini informatici e mezzi di ricerca della prova nella conduzione delle indagini", in *Rivista giuridica di polizia*, 1998, n. 6, pp. 711-738.
- Bravo F., "Internet e gli illeciti penali riguardanti lo sfruttamento sessuale dei minori: aspetti tecnici, criminologici e giuridici", in *Rivista giuridica di polizia*, 2002, n. 1, pp. 9-35.
- Colombo E., "La cooperazione internazionale nella prevenzione e lotta alla criminalità informatica: dalla Convenzione di Budapest alle disposizioni nazionali", in *Ciberspazio e diritto*, 2009, n. 3/4, pp. 285-304.
- Corasaniti G., Corrias Lucente G. (a cura di), *Cybercrime, responsabilità degli enti, prova digitale. Commento alla Legge 18 marzo 2008, n. 48*, Cedam, Padova, 2009.
- Ghirardini A., Fagioli G., *Computer forensics*, Apogeo, Milano, 2007.
- Luparia L., Ziccardi G., *Investigazione penale e tecnologie informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Giuffrè, Milano, 2007.