diritto internazionale
giurisprudenza catania

MARILENA ARENA

Il recepimento in Italia della Convenzione di Budapest La legge 18 marzo 2008 n. 48

2021-2.11

Fogli di lavoro
per il Diritto Internazionale

La Redazione di FLADI-FOGLI DI LAVORO *per il Diritto Internazionale*

Direzione scientifica: *Rosario Sapienza*

Coordinamento redazionale: *Elisabetta Mottese*

Comitato di Redazione: *Valentina Bonanno, Nancy Cannizzo, Federica Antonietta Gentile*, *Gemma Halliday*, *Salvo Emanuele Leotta, Giuseppe Matarazzo, Salvatore Andrea Viscuso*

Comitato dei Revisori*: Adriana Di Stefano, Elisabetta Mottese, Maria Manuela Pappalardo, Giuliana Quattrocchi, Grazia Vitale*

Testo chiuso nel mese di maggio 2021

FOGLI DI LAVORO *per il Diritto Internazionale* è *on line*
http://www.lex.unict.it/it/crio/fogli-di-lavoro

ISSN 1973-3585
Cattedra di Diritto Internazionale
Via Crociferi, 81 - 95124 Catania
E-mail: risorseinternazionali@lex.unict.it
Redazione: foglidilavoro@lex.unict.it

1. Introduzione

La legge 18 marzo 2008, n.48 autorizza alla ratifica ed esegue in Italia la Convenzione del Consiglio d'Europa sulla Criminalità informatica (cd. Convenzione di Budapest) del 23 novembre 2001.

L'obiettivo della legge, in ossequio al suo articolo 2, è quello di dare "*piena ed intera esecuzione*" alla Convenzione, con effetti di diritto internazionale solo dal 1° ottobre 2008, vale a dire dal primo giorno del mese successivo al termine di cui all'art. 36 della Convenzione.

Preliminarmente occorre evidenziare come le peculiari esigenze investigative scaturenti dall'irrompere delle tecnologie telematiche e informatiche pressoché in tutti settori della vita erano già state oggetto di precedenti interventi normativi. Il riferimento è alla legge 547/1993 "*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*" la quale, oltre a incidere sulla tutela apprestata attraverso la creazione di numerose fattispecie incriminatrici, aveva dedicato attenzione alle necessità di adeguamento degli strumenti d'indagine

La legge n. 48/2008 ha introdotto novità di grande rilievo.

In primo luogo, è intervenuta con importanti modifiche alle norme penali, sostanziali e processuali, in materia di reati informatici, tenendo conto sia dei principi sanciti dalla Convenzione sia delle esigenze di maggiore adeguamento della disciplina alle caratteristiche della criminalità informatica, già approfondite ampiamente nei capitoli precedenti.

In secondo luogo, la legge ha consentito, a distanza di oltre sette anni, al nostro Paese di adempiere agli obblighi assunti in sede internazionale con la sottoscrizione della Convenzione (entrata in vigore il 1° luglio 2004).

Gli aspetti sui quali la legge è intervenuta sono:

- Introduzione di sanzioni più rigorose;
- Previsione di fondi per il contrasto della pedopornografia e per la protezione di infrastrutture informatiche di interesse nazionale;
- Introduzione di un regime di responsabilità degli enti;
- Introduzione di nuovi strumenti di indagine per le forze dell'ordine;
- Previsione di tutele maggiori per la protezione dei dati personali;

Concentrando l'attenzione sui riflessi processual-penalistici della nuova disciplina e, precipuamente, sulle ricadute in materia di '*evidence'*, oggetto di analisi saranno, in questa sede, le novità introdotte in materia di misure investigative disponibili in relazione all'ampia tipologia di crimini informatici.
In particolare, le modifiche apportate alle norme del codice di rito sono intervenute sui mezzi di ricerca della prova e sulle indagini della PG, disciplinando le modalità di esecuzione di sequestri, ispezioni e perquisizioni relativi a materiale informatico, così da garantire, anche con la prescrizione di opportune regole di conservazione, l'intangibilità dei dati originali e la conformità delle copie durante un processo penale.
L'aspetto più delicato, che verrà analizzato con maggiore attenzione nei paragrafi successivi, ruota attorno all'esigenza di garantire la 'genuinità' della prova digitale.
Si tratta delle attività connesse alla disciplina della cd *digital forensics*, ossia quella disciplina il cui obiettivo principale è 'dar voce alle prove'[1]. Definita come "*use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of*

[1] C. Maioli, *Introduzione all'informatica forense* in P. Pozzi (a cura di), *La sicurezza preventiva dell'informazione e della comunicazione*, Franco Angeli 2004.

facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations", indica l'insieme delle attività volte all'analisi e alla soluzione dei casi legati alla criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un computer, diretti a un computer o in cui il computer può comunque rappresentare una fonte di prova [2].

2. Le norme del codice di procedura penale introdotte dalla legge 18 marzo 2008, n.48

La legge che ratifica la Convenzione consta di 14 articoli, divisi in quattro capi. Meritano attenzione le norme, contenute all'interno del Capo III, avente ad oggetto le "*Modifiche al codice di procedura penale e al codice di cui al d.lgs. n. 196/2003",* e composto da cinque articoli.

Seppur il legislatore si sia mosso cautamente nell'introdurre i nuovi principi per l'assunzione delle prove informatiche, non indicando cioè nel dettaglio le modalità esecutorie da applicare nell'utilizzo di tali istituti. L'attenzione si è focalizzata su due basilari aspetti, sicuramente più vincolati al risultato finale che non al metodo da utilizzare: la corretta procedura di copia dei dati utili alle indagini e la loro integrità e non alterabilità in sede di acquisizione.

In realtà gli artt. 8, 9 e 11 della legge n 48/2008 si sono limitati ad adeguare le disposizioni processuali già vigenti, tramite operazioni di 'chirurgia lessicale'. La tecnica emendativa, infatti, si è limitata a inserire espressioni che rimandano ad

[2] E. Casey, *Digital evidence and computer crime*, Elsevier, 2011, pag. 7: "*L'uso di metodi scientificamente derivati e comprovati per la conservazione, raccolta, convalida, identificazione, analisi, interpretazione, documentazione e presentazione di prove digitali derivate da fonti digitali allo scopo di facilitare o favorire la ricostruzione di eventi ritenuti criminali o di aiutare anticipare azioni non autorizzate che si sono rivelate dannose per le operazioni pianificate*".

attività connesse a "dati, informazioni e programmi informatici". Come si legge nella relazione al Progetto di legge, le novelle in materia processuale "*consistono in un adeguamento prevalentemente lessicale delle disposizioni processuali già vigenti, finalizzato a rendere esplicite le potenzialità applicative in campo informatico, che già oggi, peraltro, dottrina e giurisprudenza riconoscono agli istituti procedurali che ne sono interessati*"[3].

L'unica vera e propria novità introdotta dal legislatore è la procedura di "*conservazione rapida dei dati*", cd '*freezing'*, prevista dall'art. 16 della Convenzione, mediante l'aggiunta di commi all'art. 132 del cd Codice della privacy.

A livello sistematico, il legislatore è intervenuto sul titolo III del libro III, relativo ai mezzi di ricerca della prova, e sul titolo IV del libro V, dedicato alle indagini su iniziativa della polizia giudiziaria.

In tema di *ispezioni informatiche*, con le modifiche aggiuntive all'art. 244 c.p.p., co. 2, secondo periodo, è previsto che l'autorità giudiziaria possa 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[4].

In ambito di *perquisizione informatica*, invece, la modifica ha interessato l'art. 247 c.p.p., tramite l'aggiunta di un nuovo comma 1-bis, il quale stabilisce che ove si ha 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, deve esserne disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione[5].

---

[3] A. Vitale, La nuova disciplina delle ispezioni e perquisizioni in ambiente informatico o telematico, in *Diritto dell'internet*, 2008

[4] Art. 244 co 2 cpp, "Casi e forme delle ispezioni".

[5] Art. 247 co 1 bis, "Casi e forme della perquisizione".

Per i casi di urgenza, è stata altresì prevista una modifica all'art. 352 c.p.p. in materia di perquisizioni.

In tutte le ipotesi di flagranza del reato, ovvero nei casi di cui al comma 2 dello stesso articolo, quando sussistono i presupposti e le altre condizioni previste, gli ufficiali di polizia giudiziaria possono adottare misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione e procedere altresì alla perquisizione di sistemi informatici o telematici quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellate o disperse.

In tema di *sequestro di corrispondenza*, invece, la ratifica ha modificato l'art. 254 c.p.p e inserito l'art. 254-bis c.p.p. relativo alla possibilità di sequestrare dati informatici presso i fornitori di servizi informatici, telematici e di telecomunicazioni.

È previsto 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 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".*

Sempre in relazione al sequestro, è stata inserita la disposizione di cui all'art. 259 comma 2 c.p.p. per regolare il problema, di grande rilevanza, relativo alla custodia delle cose sequestrate.

Inoltre con la modifica dell'art. 260 comma 2 c.p.p. vengono introdotte alcune garanzie circa il sequestro e la custodia di cose deperibili[6].

L'art. 9 comma 3, l. n. 48 del 2008 ha, infine, integrato il comma 2 dell'art. 354 c.p.p., estendendo il potere della polizia giudiziaria di compiere *accertamenti urgenti*, finalizzati a conservare tracce e cose pertinenti al reato o ad evitare l'alterazione di luoghi e cose, ai dati, alle informazioni, ai programmi informatici e ai sistemi informatici o telematici.

Tutto questo può essere effettuato, ove possibile, attraverso la duplicazione, mediante una procedura tale da assicurare la conformità della copia all'originale e la sua immodificabilità, dei dati, delle informazioni o dei programmi informatici.

A chiusura del capo III, l'art. 11 prevede la modifica all'art. 51 del codice di procedura penale in materia di competenza.

È stato aggiunto il nuovo comma 3 - quinquies in cui si prevede che "*Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 600-bis, 600-ter, 600-quater, 600-quinquies, 615-ter, 615-quater, 615-quinquies, 617-quater, 617-quinquies, 617-sexies, 635-bis, 635-ter, 635-quater, 640-ter e 640-quinquies del codice penale, le funzioni indicate nel comma 1, lettera a), del presente articolo sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente",* il cui fine è creare "Procure Informatiche Distrettuali".

L'ambito di intervento del nuovo sistema, infatti, si spinge oltre il terreno del cybercrime, trovando applicazione con riferimento a qualsiasi tipologia di reato per cui si proceda, in perfetta aderenza con il dettato internazionale della Convenzione di Budapest, il quale all'art. 14 dispone che: "*each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:*

[6] S. Aterno, Le investigazioni informatiche e l'acquisizione della prova digitale, in *Giur. merito*, fasc.4, 2013

a) the criminal offences established in accordance with articles 2 through 11 of this Convention;

b) other criminal offences committed by means of a computer system;

c) the collection of evidence in electronic form of a criminal offence".

Per concludere, con la legge 18 marzo 2008, n. 48, che ratifica ed esegue la Convenzione di Budapest del 2001, il legislatore italiano, pur in ritardo, è intervenuto sull'impianto codicistico originario, introducendo una vera e propria disciplina ad hoc relativa al trattamento della c.d. '*Digital evidence*'.

Plurimi sono i profili di delicatezza in materia di indagini informatiche. Esse si fondano su un reperto assai peculiare, le cui caratteristiche essenziali sono l'immaterialità, la fragilità e il rischio di 'contaminazione' dovuto ad un cattivo uso degli strumenti informatici ovvero alla scarsa conoscenza del sistema e delle sue funzioni.

La disciplina relativa al trattamento della prova informatica ruota attorno al "*dovere di non alterare il dato originale*": le tecniche utilizzate per gestire gli elementi digitali devono essere in grado di lasciare inalterato l'originale, sia nella fase di acquisizione, che nella fase successiva di conservazione.

3. Competenza

La scelta del legislatore italiano del 2008 è di affidare, ai sensi dell'art 51 cpp co 3 quinquies, agli uffici della procura della Repubblica presso il tribunale del capoluogo di distretto della Corte d'appello la legittimazione allo svolgimento delle

indagini in relazione ai procedimenti riguardanti una serie di reati elencati nella disposizione oggetto di disamina[7].

Normalmente la *reductio ad unitatem* dell'attività investigativa in capo ad un singolo ufficio deriva dalla considerazione che il fenomeno criminoso di riferimento, nonostante la diversificazione delle sue articolazioni, si caratterizza per una spiccata unitarietà[8]. Senza considerare che, la scissione dell'attività giudiziaria in una pluralità di procedimenti costituisce di per sé un enorme costo a discapito dell'incisività delle indagini, con inevitabile dispersione delle conoscenze indispensabili a consentire adeguati sviluppi investigativi[9].

In materia di criminalità informatica, tuttavia, la vera ragione della scelta di concentrare le indagini in capo ad un unico ufficio si giustifica, esclusivamente, per le esigenze delle attività investigative, il cui espletamento necessita inquirenti altamente specializzati sul piano tecnologico. Si mira a consentire la formazione di gruppi di lavoro altamente specializzati in ciascuno dei 26 distretti del territorio nazionale.

Da precisare che la specializzazione 'informatica' delle procure della Repubblica riguarda anche il settore della criminalità d'impresa, in quanto l'art. 7 della legge di autorizzazione alla ratifica ed esecuzione della Convenzione di Budapest ha introdotto la responsabilità dipendente da reato delle imprese e degli altri soggetti collettivi.

---

[7] Art. 11 legge 48/2008: "*1. All'articolo 51 del codice di procedura penale è aggiunto, in fine, il seguente comma: 3-quinquies. Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 600-bis, 600-ter, 600-quater, 600-quater.1, 600-quinquies, 615-ter, 615-quater, 615-quinquies, 617-bis, 617-ter, 617-quater, 617-quinquies, 617-sexies, 635-bis, 635-ter, 635-quater, 640-ter e 640-quinquies del codice penale, le funzioni indicate nel comma 1, lettera a), del presente articolo sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente*".

[8] A. Nappi, *Guida al codice di procedura penale,* X ed., Milano, 2007, p. 64.

[9] G. Melillo, *Procedimenti connessi e coordinamento delle indagini in materia di delitti di criminalità organizzata,* in Cass. pen., 1999, 2415 ss.;

Il riferimento normativo in tema di '*competenza*' è l'art. 11 della legge 48/2008. La rubrica è fuorviante. In primo luogo, la competenza è nozione tradizionalmente riferita alla posizione del giudice, dal quale il pubblico ministero ripete la propria legittimazione. Parlare di competenza del pubblico ministero è errato[10].

In secondo luogo, la sua determinazione è un profilo piuttosto problematico, se si considerano le difficoltà d'individuazione del locus commissi delicti in relazione a reati commessi in rete.

I criteri tradizionali di attribuzione della giurisdizione, da tempo previsti dal nostro codice penale, ed in parte ripresi dalla stessa Convenzione di Budapest, sono inadatti alle indagini informatiche, o comunque hanno una natura autarchica: non eliminano il pericolo della sovrapposizione di procedimenti in rapporto ai medesimi fatti.

Di questi aspetti critici si è già occupata la Convenzione, in particolare nella disposizione di cui all'art. 22 CCC. In essa si fa riferimento al concetto di competenza non in senso tecnico, ma quale equivalente della nostra nozione di giurisdizione al fine di offrire adeguati criteri comuni[11].

Queste considerazioni fanno pensare che il legislatore italiano ha voluto creare una disciplina ad hoc, che specifichi criteri particolari di attribuzione della competenza per territorio nell'ambito della criminalità informatica. Tuttavia, è evidente come la normativa interna in nulla modifica gli ordinari criteri di attribuzione della competenza per territorio, la cui individuazione in concreto sarà effettuata facendo leva sui criteri suppletivi sanciti dall'art. 9 c.p.p., tutte le volte in

[10] E. De Nicola, Art. 51, in M. Chiavario, *Commento al nuovo codice di procedura penale*, vol. I, 1989, 264; E. Fortuna, Pubblico ministero, in Enc. giur. Treccani, Roma, 1991, vol. XXV.

[11] M. Guernelli, *La convenzione sul cyber-crime e la decisione quadro relativa agli attacchi informatici: significato e portata per il sistema penale interno*, in Studium juris, 2007, p. 292.

cui il carattere 'virtuale' del reato informatico non consenta l'individuazione del luogo di consumazione del reato[12].

4. Ricerca della prova digitale: la novella in tema di Ispezioni e Perquisizioni informatiche

Durante le indagini volte alla ricerca di mezzi di prova informatici, prioritaria è l'esigenza di intervenire immediatamente, sfruttando il c.d 'effetto a sorpresa'.
Alla base della scelta legislativa che permette lo svolgimento di operazioni come la perquisizione o l'ispezione vi sono ragioni di ordine pratico.
I dati digitali sono caratterizzati da una durata (c.d. *data persistence*) che può essere alquanto limitata: ne discende che un accertamento investigativo effettuato sul sistema a distanza di tempo potrebbe risultare superfluo, mentre avrebbe un'evidente utilità se fosse svolto immediatamente (*real time*)[13].
A titolo esemplificativo si pensi all'ipotesi in cui, sulla scena del crimine, sia rinvenuto un notebook acceso: in tal caso, potrebbe essere indispensabile verificare il contenuto della ram, le connessioni di rete aperte, i programmi in esecuzione o le attività di download in corso, e potrebbe essere altresì necessario compiere tale disamina *illico et immediate.*

---

[12] Finora risulta oltremodo esigua la giurisprudenza che affronta il problema del locus commissi delicti in materia di criminalità informatica. In relazione ad un'ipotesi di associazione a delinquere finalizzata all'accesso abusivo a sistemi informatici e alle frode informatiche - mediante ingresso in rete telefonica, attraverso un'utenza dalla quale venivano abusivamente raggiunte, in modo fraudolento e reiterato, utenze estere - si è ritenuto territorialmente competente il giudice del luogo dell'ultima telefonata: Cass., sez. VI, 4 ottobre 1999, Piersanti, in Cass. pen., 2000, 2990 ss., con commenti di S. Aterno, Sull'accesso abusivo a un sistema informatico, e di L. Cuomo, La tutela penale del domicilio informatico. In un precedente più recente, relativo al reato di pornografia minorile, si è individuato il luogo di consumazione del reato nella località ove è stato digitato il comando di invio nella rete del materiale pedopornografico: Cass., sez. III, 2 dicembre 2004, Ongari, in Cass. pen., 2006, 1820.
[13] L. Cuomo - R. Razzante, *La disciplina dei reati informatici*, Torino, 2007, p. 41.

Tradizionalmente, ispezione e perquisizione, sono operazioni classiche di ricerca della prova.

L'attività tipica dell'*inspicere* si sostanzia nell'osservazione di persone, luoghi, cose e mira all'accertamento di tracce o altri effetti materiali del reato (art. 244, comma 1 cpp); di contro, l'attività tipica del *perquirere* si caratterizza dell'individuazione e acquisizione del corpo del reato o delle cose ad esso pertinenti, spesso qualificandosi come attività prodromica rispetto al sequestro probatorio (art. 247, comma 1 cpp).

La Novella ha interessato entrambe le disposizioni.

La legge che ratifica la Convenzione sul Cybercrime, ha modificato l'ultima parte del 2° comma dell'art. 244 c.p.p., disponendo espressamente che: "*in relazione a sistemi informatici o telematici, devono essere adottate misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*".

Ma cosa significa ispezionare i dati digitali?

È preliminare dedicare attenzione alla possibilità stessa di configurare, in astratto, un'ispezione su un sistema informatico.

Nell'ispezione tradizionale la ricerca si traduce in osservazione e constatazione, senza alcuna interferenza fisica dell'operatore sullo stato delle cose. È difficile ipotizzare un'operazione su un sistema informatico che si limiti ad una mera verifica esterna dello stesso, senza alcun accesso ai dati contenuti al suo interno. Infatti, osservare un file significa 'mettere le mani' sul dispositivo di memorizzazione, almeno al fine di verificarne la presenza. Così, in ambito informatico osservazione e ricerca (attività quest'ultima tipica nella perquisizione) sembrano avere il medesimo contenuto in sede di attuazione.

Il diverso ambito di applicazione dei due mezzi di ricerca della prova è stato oggetto di un acceso dibattito.

Una parte della dottrina sostiene che rientra nell'ambito dell'attività ispettiva la visione dei file privi di password, mentre tutte le volte in cui la lettura del file

richiede particolari sistemi di autenticazione il mezzo di prova da utilizzare sarà la perquisizione[14].

Secondo altri studiosi, e questa è la teoria più accreditata, il discrimine tra i due istituti è la *scena criminis informatica*:

"*L'attività ispettiva in ambiente informatico dovrebbe limitarsi ad osservare il sistema descrivendolo nei suoi particolari, ad esempio rilevando la presenza di periferiche collegate, accesso alla rete attivo, presenza di software in funzione, partizioni logiche nascoste e rese visibili da meccanismi di autorizzazione connessi allo status dell'utilizzatore*"[15].

Passando alla perquisizione, si noti come essa consiste in un'attività di ricerca diligente[16].

La legge 48/2008 ha introdotto un nuovo comma 1 bis all'art. 247 cpp il quale 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".*

In ambito informatico, la perquisizione consiste nella ricerca, all'interno del dispositivo, dei file utili all'indagine e presuppone, una 'intrusione' all'interno del dispositivo.

Intrusione al sistema informatico che è sintomatica della seguente considerazione: se, tradizionalmente, la perquisizione costituisce l'antecedente logico e giuridico

[14] C. Maioli - E. Sanguedolce, *I "nuovi" mezzi di ricerca della prova fra informatica forense e L. 48/2008*, www.altalex.com, 30 novembre 2015.
[15] Ibidem.
[16] F. Cordero, Procedura penale, 8^ ed., cit., p. 832

del sequestro, quella informatica, invece, si presta a essere eseguita non prima ma dopo il sequestro dell'apparecchiatura [17].

La ricerca, infatti, si traduce inevitabilmente in un'attività in grado di alterare il dato originale, sicché il suo espletamento deve avere ad oggetto la copia forense e mai l'originale, pena la violazione degli art. 247 e 352 c.p.p., così come modificati dalla riforma del 2008.

Queste norme sono etichettate alla stregua di "*norme processuali in bianco*", poiché implicitamente richiamano le best practices del settore, senza però indicare a quale, fra le molteplici esistenti, ci si debba riferire[18].

In definitiva, si procede con l'ispezione di un sistema informatico o telematico qualora occorre accertare le tracce o gli altri effetti materiali del reato e procedere dalla descrizione dello stato dell'apparecchiatura, inclusa l'eventuale presenza di periferiche collegate al sistema, fino alla verifica dei processi in corso.

L'attività degli inquirenti in sede di perquisizione, invece, va oltre, poiché essi possono compiere operazioni sui dati contenuti nell'apparecchiatura, come, ad esempio, l'apertura di cartelle e programmi.

5. Le misure volte alla salvaguardia della genuinità della prova digitale

Se i mezzi di ricerca della prova analizzati al paragrafo precedente sono utilizzati da personale 'incompetente', vi è il rischio che i dati, e di conseguenza le possibili fonti di prova, siano alterati, venendo meno la possibilità di un loro utilizzo in un processo penale.

---

[17] F.M. Molinari, *Questioni in tema di perquisizione e sequestro di materiale informatico*, in Cass. pen., 2012, p. 708.

[18] G. Braghò, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici* in L. Lupària , *Sistema penale e criminalità informatica*, Giuffrè, 2009.

Per evitare tali inconvenienti il legislatore ha introdotto le disposizioni di cui agli art. 244 co. 2 c.p.p., art. 247 co. 1 bis c.p.p e art. 252 co. 1 bis cpp.

Queste norme prevedono la necessità di adottare "*misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione"*[19].

Apparentemente, questa precisazione appare superflua, in considerazione dell'ovvietà del suo contenuto.

Infatti, quando si procede a perquisizione, ispezione o sequestro, è normale che gli inquirenti devono porre in essere ogni accorgimento al fine d'evitare la contaminazione della scena del crimine.

È necessario, tuttavia, capire realmente la portata di questa previsione. La chiave di lettura è l'art. 15 CCC, norma estremamente travagliata: essa elenca talune disposizioni comuni, riferite alle condizioni e alle tutele di tipo processuale, che i singoli Stati devono tenere presente in sede di ratifica. Da una lettura delle disposizioni in tema di ispezioni, perquisizioni o sequestro in senso conforme alla Convenzione, si evince che il legislatore ha voluto rendere nota la regola per cui tali mezzi di ricerca dell prova (cioè atti, normalmente, irripetibili) concernenti supporti informatici o telematici vanno sempre rese alla stregua di attività ripetibili in futuro. Naturalmente, ciò è realizzabile solo se si agisce in una dimensione digitale, giacché, nel mondo reale, ciò non è possibile[20].

---

[19] L'interesse di garantire l'integrità e l'attendibilità delle prove elettroniche anche in occasione della loro raccolta era già stato presente in seno al Consiglio d'Europa, come risulta dalla Recommendation n. R (95) 13 of the Committee of Ministers to Member States concerning problems of criminal procedural law connected with information technology: "*V. Electronic evidence. - 13. The common need to collect, preserve and present electronic evidence in ways that best ensure and reflect their integrity and irrefutable authenticity, both for the purposes of domestic prosecution and international cooperation, should be recognised. Therefore, procedures and technical methods for handling electronic evidence should be further developed, and particularly in such a way as to ensure their compatibility between states. Criminal procedural law provisions on evidence relating to traditional documents should similarly apply to data stored in a computer syste."*

[20] A. Vitale, La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico, in *Diritto dell'internet* n. 5/2008.

Motivo per cui s'impone di conservare i dati originali e d'impedirne l'alterazione, con la conseguenza di notevole importanza che il contenuto originario è disponibile in ogni momento del processo.
Occorre riflettere, inoltre, sul fatto che queste salvaguardie sono richieste dal legislatore anche quando si procede con ispezione e perquisizione tradizionale. Ma nel momento in cui tali procedure hanno ad oggetto un sistema informatico, l'adozione delle citate misure di salvaguardia rappresenta uno speciale requisito (con finalità garantiste), che va sempre rispettato: tale procedura, in altre parole, si configura come un elemento costitutivo di queste tre fattispecie, con l'ovvia conseguenza che il mezzo di ricerca della prova in sua assenza sarebbe invalido.
Ad esempio, il valore probatorio dell'arma del delitto è indifferente alla maniera con cui è avvenuta '*l'adprehensio*' della res; viceversa, la veridicità e la genuinità di un determinato file dipendono direttamente dal modo con cui esso è stato individuato e acquisito.
È opportuno, prima di concludere, constatare come nel caso in cui non siano attuate le misure di conservazione e salvaguardia dei dati originali, la conseguenza immediata è la nullita dell'ispezione o della perquisizione; la nullità si estende, in tal caso, anche alle prove acquisite, le quali non possono essere poste a fondamento di alcuna decisione giudiziale.

6. Acquisizione della prova: il sequestro

La Convenzione di Budapest, dopo le disposizioni comuni e le regole sulla conservazione e la divulgazione di dati informatici immagazzinati in sistemi informatici e di quelli relativi al traffico, al titolo IV, e nello specifico all'art. 19, regolamenta il sequestro dei dati.
È' ammessa la possibilità, per le autorità competenti degli Stati aderenti di sequestrare o acquisire un sistema informatico o parte di esso o un supporto per: a) il

sequestro o l'acquisizione di sistemi informatici, di parte di questi o di supporti idonei alla conservazione di dati; b) il trattenimento di copia delle informazioni raccolte; c) la conservazione dell'integrità dei dati in tal guisa memorizzati; d) la segretazione nei confronti di terzi o, addirittura, la rimozione dal sistema sequestrato di tutti i dati pertinenti al procedimento penale[21].

Il recepimento avvenuto ad opera della legge del 2008 con l'art. 8, che ha ratificato ed attuato le direttive contenute nell'art. 19 comma 3 CCC., ha la modificato gli artt. 254, 256, 259 e 260 c.p.p. e inserito l'art. 254 bis c.p.p., la cui disciplina verrà qui di seguito analizzata.

Le novità apportate dalla l. 48/2008 all'art. 254 c.p.p., relativo al *sequestro di corrispondenza*, rilevano sotto tre profili.

In primo luogo, è stato ampliato il novero dei soggetti destinatari del provvedimento di sequestro, "*fornitori di servizi postali, telegrafici e telematici".*

In secondo luogo, è stata ampliata la corrispondenza oggetto di acquisizione (ossia la corrispondenza telematica). È del tutto legittimo un provvedimento di sequestro dell'autorità giudiziaria su ogni comunicazione pertinente al reato inviata o ricevuta dall'indagato con strumenti elettronici.

L'unico limite previsto dalla norma attiene alla sussistenza del rapporto di pertinenza: è richiesta una stretta correlazione tra il bene da sottoporre a sequestro e le esigenze probatorie che il sequestro deve soddisfare.

Ultimo profilo interessato dalla novella riguarda l'inserimento del criterio della '*non alterabilità*' del reperto.

Il secondo intervento della l.48/2008 riguarda la creazione ex novo dell'art. 254-bis c.p.p., rubricato "Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni".

[21] A. Macrillò, Le nuove disposizioni in tema di sequestro probatorio e di custodia e assicurazione dei dati informatici, *in Diritto dell'internet* 05/2008.

La disposizione prescrive 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 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.*".

Destinatari sono i fornitori di servizi di telecomunicazione; devono essere esclusi tutti gli altri soggetti che non rientrano in questa categoria, come ad esempio le aziende private, gli enti pubblici e la pubblica amministrazione.

Il legislatore ha voluto ribadire *expressis verbis*, la generale sottoponibilità a tale mezzo istruttorio di tutti i dati informatici in possesso dei gestori ed ha altresì, indicato mediante l'utilizzo della locuzione "*quando dispone*", le precise modalità con cui tale operazione, invero già concepita dal nuovo testo dell'art 254 con riferimento alla corrispondenza, deve avvenire[22].

Sono state previste appunto delle precise indicazioni sulla necessità di assicurare l'acquisizione e la copia dei dati su adeguato supporto, tramite una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. Al contempo si è imposto al fornitore dei servizi di telefonia e di connessione internet una conservazione e protezione adeguata dei dati originali: da ciò si evince che la disposizione mira ad evitare turbative alla regolare fornitura dei dati oggetto dell'interesse investigativo.

Grazie a tale disposizione si possono acquisire, con provvedimento di sequestro e con le garanzie necessarie, *i file di log*, se ancora esistenti, con effetti positivi su un triplice piano: si garantiscono sia la regolare fornitura del servizio da parte del

[22] A.Macrillò, op. cit. p. 145, p. 503

Provider (che può continuare le normali attività nonostante il provvedimento di sequestro), sia le esigenze di indagine, sia l'adempimento degli obblighi derivanti dalla normativa sulla *data retention* (d.lg. n. 109 del 2008 e art. 132 d.lg. n. 196 del 2003)[23].

La disciplina nazionale, tuttavia, non sembra abbastanza precisa sulle modalità di applicazione dell'art. 254 bis cpp, dato che il dato normativo si limita a prevedere che l'autorità giudiziaria 'possa' stabilire che i dati siano acquisiti mediante copia. In questa direzione, una lettura costituzionalmente orientata della norma e conforme ai principi della Convenzione, porterebbe a preferire la soluzione della clonazione del dato informatico secondo i protocolli scientifici.

In particolare, l'effettuazione della 'copia' rappresenta il giusto contemperamento tra le esigenze di accertamento penale, di genuinità del dato informatico e la salvaguardia delle libertà costituzionalmente garantite[24].

Per concludere, la norma è stata voluta allo scopo di indicare una metodologia di acquisizione.

Lo scopo non è definire le *cd. best practis* sulla miglior procedura da seguire per un corretto sequestro dei dati informatici, bensì quello di tracciare la procedura generale da utilizzare in materia di acquisizione dei dati informatici all'origine, ossia nel luogo dove essi si formano e in cui vengono conservati per brevissimo tempo.

---

[23] Aterno S., *Le investigazioni informatiche e l'acquisizione della prova digitale*, Giur. merito, fasc.4, 2013.

[24] S.Venturini, *Sequestro probatorio e fornitori di servizi telematici*, dal testo Internet provider di L.Lùparia, Giuffrè 2009.

7. L'attività investigativa della polizia giudiziaria: l'accertamento tecnico urgente

Gli interventi di autorizzazione alla ratifica ed esecuzione della Convenzione di Budapest hanno interessato sia le norme relative alle indagini e in particolare i mezzi di ricerca della prova, sia le norme relative agli atti a iniziativa della polizia giudiziaria, che saranno, di seguito, oggetto di trattazione.

Nell'ambito degli atti a iniziativa della polizia giudiziaria, previsti dall'art. 347 e ss., sono state integrate le norme riguardanti le perquisizioni (art. 352, c. 1-bis), l'acquisizioni di plichi o di corrispondenza (art. 353, c. 2 e 3), gli accertamenti urgenti sui luoghi, sulle cose e sulle persone, sequestro (art. 354, c. 2), nonché l'articolo 132 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

Si procede con l'analisi delle disposizioni relative agli atti a iniziativa della PG, che hanno attuato la Convenzione di Budapest.

Le novità introdotte della legge del 2008 hanno riguardato, anzitutto, l'art. 352 cpp in materia di perquisizioni, tramite l'introduzione di un primo comma bis, il quale prevede la possibilità di perquisire o, più correttamente, di accedere a un sistema informatico o telematico e di acquisire e conservare i dati in esso eventualmente contenuti.

La possibilità di procedere a perquisizione di sistemi informatici o telematici è subordinata all'esistenza dei presupposti descritti nei commi 1 e 2 dell'art. 352 c.p.p: il primo comma dell'art. 352 c.p.p. disciplina le perquisizioni personali o locali ad iniziativa degli ufficiali di polizia giudiziaria nei casi di flagranza del reato o in caso di evasione, finalizzate alla ricerca di cose o tracce pertinenti al reato che possono essere cancellate o disperse ovvero alla ricerca della persona sottoposta alle indagini o dell'evaso; il secondo comma, dello stesso articolo, prevede, inoltre, la possibilità di procedere a perquisizione personale o locale quando

si deve eseguire un'ordinanza che dispone la custodia cautelare o un ordine che dispone la carcerazione per uno dei delitti per i quali è previsto l'arresto obbligatorio in flagranza, ovvero quando si procede al fermo di indiziato di delitto, sempre che sussistano il pericolo di dispersione o cancellazione indicati nel precedente comma e ricorrano particolari ragioni di urgenza che non consentono l'emissione di un tempestivo decreto di perquisizione da parte dell'autorità giudiziaria.

Il primo comma bis rappresenta l'attuazione dell'art. 19 comma 1 della Convenzione di Budapest, riguardante appunto le misure legislative da adottare per consentire alle autorità competenti di ciascuno Stato di "perquisire o accedere in modo simile a un sistema informatico o parte di esso e ai dati informatici ivi immagazzinati" o "a un supporto per la conservazione dei dati informatici".

L'art. 9 comma 2 della l. 48/2008 ha novellato il secondo e terzo comma dell'art. 353 c.p.p. in materia di acquisizione di plichi o di corrispondenza ad opera della polizia giudiziaria, prevedendo la possibilità, per la polizia giudiziaria, di accertare, su autorizzazione del pubblico ministero, il contenuto della corrispondenza.

È opportuno sottolineare che la disposizione oggetto di disamina opera non con riferimento alle e-mail eventualmente registrate o conservate nella memoria del computer oggetto di accertamento da parte della polizia giudiziaria (una tale attività sarebbe da ricondurre al novero di quelle descritte dagli artt. 352 e 354 c.p.p., come novellati), bensì alle e mail il cui processo di trasmissione telematica non sia ancora completo, oppure alle e mail inviate nell'ambito del servizio di spedizione online di telegrammi, corrispondenza ordinaria o raccomandata offerto dagli uffici postali[25].

La novella ha esteso il potere della polizia giudiziaria fino ad ammettere la possibilità di compiere accertamenti urgenti, finalizzati a conservare tracce e cose

[25] A. Barbieri, Le attività d'indagine della polizia giudiziaria ui sistemi informatici e telematici, *in Diritto dell'interne*t, 05/2008.

pertinenti al reato o ad evitare l'alterazione di luoghi e cose, ai dati, alle informazioni, ai programmi informatici e ai sistemi informatici o telematici.

Nel codice di procedura penale il termine accertamento è più volte richiamato e spesso si genera confusione tra il significato da attribuire a tale concetto e quello del rilievo.

Per risolvere queste carenze definitorie, la giurisprudenza è intervenuta con due pronunce che meritano di essere qui accennate: con il termine accertamento ha per lo più ritenuto lo studio e la relativa elaborazione critica di dati materiali pertinenti ai reati e quindi analisi soggettive e risultanze assunte su basi tecnico scientifiche (Cass. 9 febbraio 1990, n. 301, in Ced Cass., n. 183648), mentre con il termine rilievi ha definito tutte quelle attività che si esauriscono in una costatazione, raccolta e in semplici operazioni di carattere materiale (Cass. 10 novembre 1992, n. 4523, Arena, in Ced Cass., n. 192570).

In breve, con riferimento ai 'rilievi', si deve generalmente intendere, un'attività di individuazione e rilevazione di dati materiali; mentre per 'accertamenti' si deve intendere un'attività di studio, di analisi e di giudizio di quegli stessi dati.

È evidente come l'accertamento assume oggi un ruolo ancora più importante e centrale in qualsiasi tipo di indagini, dal momento che la polizia giudiziaria giungendo per prima, sulla *scena criminis*, in moltissimi casi rinviene una notevole quantità di supporti informatici e di materiale informatico, memorie e banche dati digitali utili per le indagini.

Ciò che qualifica, quindi, l'urgenza negli 'atti a sorpresa' *ex* art. 354, co. 2 c.p.p. è l'indifferibilità dell'atto, il quale non può che essere svolto nell'immediatezza dei fatti, pena l'impossibilità del suo successivo svolgimento.

Per attuare le disposizioni della Convenzione, il legislatore ha stabilito che in relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici ritenuti interessanti, gli ufficiali della polizia giudiziaria adottino le misure tecniche o impartiscano le prescrizioni necessarie ad assicurare la

conservazione e ad impedirne l'alterazione e l'accesso, e provvedano, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità. Sarà quindi opportuno che la Polizia Giudiziaria adotti tutte le necessarie cautele per evitare il rischio di alterare il dato digitale, in assenza di una precisa delega del Pubblico Ministero.

La disciplina ha sollevato una serie di criticità che verranno qui di seguito analizzate, e che fondamentalmente ruotano attorno a due problematiche di fondo: la possibilità per la P.G. di compiere '*attività valutative tecniche'* di propria iniziativa e, conseguentemente, la '*natura ripetibile o irripetibile'* dell'accertamento informatico.

La natura irripetibile delle operazioni descritte e regolate nell'art. 354 comma 2 c.p.p. non è affatto pacifica.

Parte della dottrina, propendendo per l'irripetibilità dell'atto, ritiene necessario il compimento degli accertamenti nelle forme di cui di cui all'art. 360 cpp, al fine di garantire il diritto di difesa.

Altra parte della dottrina ha evidenziato che la tecnologia consente una duplicazione relativa al contenuto del computer senza determinare una perdita o alterazione dei dati originari[26].

Infatti, è stato ribadito che le operazioni urgenti compiute dagli ufficiali di P.G. di fronte ad un elemento di prova digitale dovrebbero essere (ove sia tecnicamente possibile) operazioni materiali e tecniche di conservazione del dato nella sua integrità, in modo tale da rendere l'operazione di duplicazione ripetibile nel futuro, salvaguardando quindi l'integrità del dato sul supporto originale, mentre nel caso in cui ciò non fosse possibile, l'atto sarebbe qualificato come irripetibile[27].

---

[26] A. Barbieri, op. cit. p.150.

[27] S. Aterno, *Acquisizione e analisi della prova informatica*, in Dir. pen. Proc., 2008, 61 ss..

Per concludere, la natura ripetibile o irripetibile dell'atto è controversa con inevitabili problemi di tutela del diritto di difesa; problemi che potrebbero essere stati risolti qualora il legislatore avesse esteso, come invece non è avvenuto, le garanzie previste per legge agli accertamenti tecnici non ripetibili.

8. Conservazione preventiva dei dati informatici: la *'quick freeze procedure'*

Per quanto concerne il mezzo di ricerca della prova disciplinato dall'art. 254-bis, si è avuto modo di notare nei paragrafi precedenti che esso ha ad oggetto dati informatici (detenuti dai *providers*) costituenti corpo del reato o cose pertinenti al medesimo.

Questa è la caratteristica che lo contraddistingue rispetto all'attività 'preventiva' disciplinata dall'art. 132 d.lgs. 196/2003, cosi come novellato a seguito della ratifica della Convenzione di Budapest sulla cybercriminalità del 2001, e i cui risultati, come si avrà modo di specificare in seguito, non sono utilizzabili nel procedimento penale.

L'art. 132 d.lgs. 196/2003 ("Codice in materia di protezione dei dati personali") costituisce un'eccezione rispetto al generale divieto di conservare i dati relativi al traffico, prevedendone una conservazione temporanea per esclusive finalità di accertamento e repressione dei reati.

Tale disposizione è stata oggetto di svariati interventi normativi che si sono susseguiti nel tempo.

L'art. 10 l. 18 marzo 2008, n. 48 ha inserito i commi 4 ter, 4 quater e 4 quinquies all'interno dell'art. 132 d.lgs. 30 giugno 2003, n. 196 e dà esecuzione agli artt. 16, 17 e 18 della Convenzione di Budapest, i quali disciplinano misure coattive e

d'urgenza volte a garantire la conservazione di dati informatici e di traffico, anche se detenuti presso terzi, con conseguente obbligo di proteggere e mantenerne l'integrità.

In particolare, l'art. 10 della legge n. 48/2008 ha dato esecuzione all'art. 16 CCC che impone alle Parti contraenti di adottare misure legislative e di altra natura per consentire la protezione rapida di specifici dati informatici, quando vi è motivo di ritenere che gli stessi siano particolarmente vulnerabili e soggetti a cancellazione o modificazione.

La novella ha previsto una procedura di 'congelamento' dei dati, conosciuta come "*quick freeze procedure"* la quale prevede che: "*Il Ministro dell'interno o, su sua delega, i 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, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi*"[28].

[28] Art. 132 co 4 ter Codice in materia di protezione dei dati personali.

I provvedimenti adottati sono comunicati entro quarantotto ore al Pubblico Ministero del luogo di esecuzione che, se ne ricorrono i presupposti, li convalida.
In caso di mancata convalida, i provvedimenti assunti perdono ogni efficacia.
Si tratta di un'attività a carattere eccezionale ed urgente, esercitabile su iniziativa della polizia giudiziaria, che può essere svolta preventivamente e, quindi, anche in assenza di una *notitia criminis*, finalizzata alla conservazione e protezione di dati relativi al traffico telematico, per un periodo di novanta giorni, prorogabile fino a sei mesi[29].
Occorre evidenziare le differenze, di non poco conto, tra la procedura in esame e quella prevista al primo comma dell'art. 132:
"*Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione"*[30].
La procedura di cui al comma 4 ter è molto più invasiva del diritto alla riservatezza personale, rispetto alla disciplina di cui al comma 1 della medesima disposizione, in quanto ha ad oggetto dati assimilabili ai 'contenuti' delle comunicazioni.
Infatti, la nuova disposizione ha come destinatari, oltre che i fornitori di una rete pubblica di comunicazioni, anche i soggetti che offrono direttamente o indirettamente servizi di comunicazione elettronica, i gestori di siti internet che diffondono contenuti sulla rete ed i gestori dei motori di ricerca.

[29] C.Fatta, La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo, *in Dir. dell'inf. e dell'inform.*, 2008, p. 395 ss
[30] Art. 132 co. 1 Codice in materia di protezione dei dati personali.

Le attività svolte da tali soggetti consentono un vero e proprio tracciamento delle operazioni svolte in rete, con la possibilità di intaccare la comunicazione anche nel suo contenuto.

Inoltre, il c.d. 'congelamento' dei dati telematici, essendo un'attività a carattere urgente, è finalizzata espressamente allo svolgimento delle indagini pre-procedimentali, con conseguente inutilizzabilità, nel procedimento penale vero e proprio. Trattasi, quest'ultima, di un ulteriore differenza rispetto alla conservazione di cui al primo comma, essendo tale procedura finalizzata ad una successiva acquisizione probatoria: infatti, il terzo comma stabilisce che i dati sono acquisiti presso il fornitore con decreto motivato del pubblico ministero.

A rafforzamento di quanto appena detto, si noti che le categorie di dati trattati dal comma 4 ter non sono individuate, mentre lo stesso non può dirsi per i dati presi di mira dal comma 1, oggetto di un'apposita opera di individuazione svolta dall'art. 3 d.l. 30 maggio 2008, n. 109[31].

In tal senso, il richiamo nel testo della disposizione alle attività di investigazione preventiva di cui all'art. 226 delle norme di cui al decreto legislativo n. 271 del 1989, deve essere interpretato come un divieto di utilizzazione di tali dati nel processo penale.

Da notare che lo scopo della disposizione, ovvero "*la finalità di accertamento e repressione di specifici reati",* accompagnata dalla mancata indicazione dei reati per i quali è esperibile questo meccanismo, comporta la creazione di una sorta di 'zona franca' in cui la polizia può conservare preventivamente dati digitali, anche

[31]Sotto la rubrica "categorie di dati da conservare per gli operatori di telefonia e di comunicazione elettronica" l'art. 3 del d.lgs. 30 maggio 2008, n. 109 individua le seguenti categorie: a) i dati necessari per rintracciare e identificare la fonte di una comunicazione; b) i dati necessari per rintracciare e identificare la destinazione di una comunicazione; c) i dati necessari per determinare la data, l'ora e la durata di una comunicazione; d) i dati necessari per determinare il tipo di comunicazione; e) i dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature; f) i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile.

laddove le finalità di giustizia non giustificano la compressione del diritto alla riservatezza.

Così parte della dottrina ha sostenuto che, in prospettiva *de lege ferenda*, dovrebbero introdursi dei limiti all'ammissibilità della procedura, nonché indicare con maggiore rigore le modalità esecutive della stessa[32].

9. Considerazioni conclusive. Aspetti critici della legge 48/2008

Al fine di "*consentire l'adeguamento dell'ordinamento italiano alla normativa internazionale*", la scelta dei redattori è stata quella di introdurre 'frettolosamente' le nuove disposizioni consci del fatto che le criticità della materia fossero molteplici e nella convinzione che la magistratura avrebbe saputo risolverle in via interpretativa[33].

Il nostro Paese poteva vantare, ben prima del 2001, di un eccellente punto di partenza, ovvero le norme introdotte dalla Legge 23 dicembre 1993 n. 547 recante "*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*": una peculiarità tutta italiana che avrebbe dovuto rendere agevole una rapida attuazione della Convenzione per concentrarsi invece su altri aspetti problematici legati al cyberspazio[34].

Ciò puntualmente non è avvenuto. Infatti, come si è già detto in precedenza gli art. 8, 9 e 11 si sono limitati ad adeguare la disciplina alle peculiarità dei sistemi informatici e telematici tramite delle operazioni a livello lessicale. Solo l'art. 10

---

[32] F. De Leo, *Il pubblico ministero tra completezza investigativa e ricerca dei reati*, in Cass. pen., 1995, 1444.

[33] L. Picotti, Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo, *in Diritto dell'internet*, n. 5/2008.

[34] F. Cajani, La Convenzione di Budapest nell'insostenibile salto all'indietro del Legislatore italiano, owero: quello che le norme non dicono, in *Ciberspazio e Diritto 20 10*, Vol. 1 1, n. 1, pp. 185-2 10

legge n. 48/2008 avrebbe realmente introdotto un nuovo istituto, quello della "conservazione rapida" dei dati, previsto dall'art. 16 Convenzione, mediante l'aggiunta di alcuni commi all'art. 132 del Codice della privacy (d.lgs. 30 giugno 2003, n. 196).

Da condividere il severo giudizio di L. Picotti nelle conclusioni del suo articolo, che descrive la legge di recepimento della Convenzione come una frettolosa legge di autorizzazione alla ratifica che rappresenti:

"…un intervento solo parziale e frammentario in cui l'urgenza vada a scapito della qualità tecnica e sistematica della normativa interna, non garantisce affatto il raggiungimento delle finalità d'armonizzazione legislativa ed il collegamento della cooperazione internazionale fra gli Stati e le loro attività inquirenti e giudicanti, che costituiscono la ragione d'essere degli strumenti internazionali"[35].

Un primo aspetto critico, rilevato sin da subito, è la mancanza di una disciplina transitoria rispetto all'entrata in vigore della l. 48/08, per cui si verificarono casi in cui gli elementi di prova furono raccolti prima della novella o nel periodo di *vacatio legis*, e casi in cui l'acquisizione avvenne successivamente all'entrata in vigore della legge, e quindi secondo modalità giuridiche più affidabili rispetto a quelle precedenti, con inevitabile disparità di trattamento e violazione del principio di uguaglianza.

Altro aspetto sottovalutato dal legislatore è la mancata previsione di inutilizzabilità o di nullità dei mezzi di prova acquisiti in violazione delle procedure previste dalle norme introdotte con la l. 48/08.

Inoltre, non è stato attuato il fondamentale precetto previsto dalla Convenzione di Budapest secondo il quale, a fronte dell'adozione delle nuove tecniche che minacciano i diritti e le libertà individuali, si impone il rafforzamento delle tutele

[35] L. Picotti, op. cit. p. 56.

degli indagati. Al contrario, è evidente come il nuovo assetto abbia ampliato ulteriormente le asimmetrie tra i poteri inquirenti e le facoltà difensive.

Ma vi è di più. Dal testo della Convenzione sul Cybercrime, ed in specie dai suoi artt. 14, par. 2, che apre la sezione dedicata alle misure processuali, e 23, par. 1, che apre il capitolo dedicato alla cooperazione internazionale, si evince che l'operatività dei nuovi strumenti riguarda, non solo i delitti che abbiano ad oggetto o la cui commissione avvenga per mezzo di sistemi o dati informatici (c.d. reati informatici in senso stretto ed in senso ampio), ma anche, più in generale, "*la raccolta delle prove elettroniche di qualsiasi altro reato*". È evidente, così, l'ampio raggio operativo delle indagini informatiche, a cui però non ha fatto seguito un adeguamento completo della disciplina processuale.

In materia di cooperazione internazionale, è mancato quasi del tutto il parallelismo tra la legge italiana e la Convezione di Budapest considerata la mancata attuazione degli artt. 26. 28, 30, 31, 32, 33, 34 CCC.

Da notare che la l. 48/2008 introduce anche profili che la Convenzione di Budapest non prevede: a titolo esemplificativo, si pensi alla disposizione di cui all'art. 12 relativa al Fondo per il contrasto della pedopornografia su internet o alla norma di cui all'art. 11 in tema di competenza, laddove la Convenzione all'art. 22 intende, invece, far riferimento ai ben diversi problemi di giurisdizione in materia crimini informatici.

In definitiva, l'esame degli emendamenti previsti dalla legge di autorizzazione alla ratifica ed esecuzione della Convenzione sul Cybercrime mostra come l'intervento del legislatore, benché apprezzabile non sia stato del tutto soddisfacente e convincente.

Nonostante le criticità appena analizzate, sarebbe errato concludere che la legge italiana non è riuscita totalmente a raggiungere l'obiettivo prefissato. La ratifica deve essere valutata con favore, ma occorre una precisazione: la legge 48/2008 rappresenta un primo passo verso l'adeguamento del sistema penale alle sfide che

vengono lanciate da questa nuova forma di criminalità in incessante evoluzione. Dunque essa deve essere collocata all'interno di una più ampia prospettiva di politica criminale.