CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

Articolo Scientifico

GARANZIE DIFENSIVE IN MATERIA DI CRIMINI INFORMATICI

Criticità della disciplina processualpenalistica sui reati informatici con particolare riferimento alle tutele di indagato ed imputato

di **Alberto Biancardo**
IUS/17 - DIRITTO PENALE
Estratto dal n. 7/2019 - ISSN 2532-9871

Direttore responsabile
Raffaele Giaquinto

Pubblicato, Mercoledì 31 Luglio 2019

CamminoDiritto.it
ISSN 2532-9871

Sommario: Abstract [ENG]; 1. La vigente disciplina processuale sui crimini informatici. – 2. Le carenze della normativa. – 3. Accertamenti tecnici ripetibili e irripetibili. – 4. Data retention. – 5. Mezzi di ricerca della prova. 6. Garanzie dell'indagato e recente giurisprudenza in materia di detenzione di materiale pedopornografico – 7. Sviluppi normativi.

Abstract. The law n. 48/2008 on computer crimes, amended the criminal procedure code, but didn't affect some aspects of primary importance, such as the respect for the privacy of the suspect or accused persons, and the boundaries in using the modes of evidence research. Indeed, the legislator has only implementing the 2001 Budapest Convention on cybercrime. Therefore, the existing regulation is not convincing, especially for not having created a valid structure of defensive guarantees that can adequately protect the suspect and the accused in IT crimes trials. The article highlights the innumerable critical points of the current legislation, focusing on possible improvements that can make it more adherent to the current needs.

1. La vigente disciplina processuale sui crimini informatici.

Negli ultimi anni si è avuto un incremento esponenziale delle cause penali per crimini informatici. Ciò sta a sottolineare non soltanto un aumento di tale tipologia di reato, ma anche una presa di coscienza dell'utente che ha subìto il crimine, e che, oggi più che nel passato, si affida alla magistratura denunciando i fatti illeciti. E' questo un chiaro sintomo che l'utente della rete, il fruitore di uno smartphone o il frequentatore dei "social network", non è più disposto a subire passivamente illeciti, più o meno gravi, perpetrati da altri soggetti che gravitano a diverso titolo nella "rete delle reti".

Fra gli illeciti informatici più comuni vi sono indubbiamente la violazione della privacy e il furto di identità, la sottrazione di dati, la diffamazione e la minaccia. Sono, tuttavia, in aumento reati di alto allarme sociale contro la persona quali la pedopornografia e il cyber stalking, e contro il patrimonio, come il cyber laudering e le estorsioni on line, ma anche gravi fenomeni diffusi fra i più giovani, quali il cyber bullismo e il c.d. blue whale.

Le due legislazioni più importanti in materia di reati informatici sono la legge n. 547 del 1993 e la legge n. 48 del 2008. Fino al 1993 vi erano solo due leggi riguardanti i cyber crimes: la prima del 1991 puniva la clonazione di carte di credito e la seconda, del 1992, puniva un non meglio definito crimine di pirateria informatica, ed era orientata esclusivamente alla tutela del diritto d'autore. La riforma del 1993 aggiunge al codice penale un corpus consistente di nuovi reati informatici, fra cui l'accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.), la frode informatica (art. 640 ter c.p.),

CamminoDiritto.it
ISSN 2532-9871

il cyber laudering o riciclaggio elettronico (art. 648 bis c.p.). Essa aveva però il limite di aver novellato solo marginalmente il codice di rito.

Nello specifico, il solo art. 11 della legge n. 547 ha aggiunto al codice di procedura penale l'art. 266 bis che consente l'intercettazione del flusso di comunicazioni informatiche o telematiche, mentre l'art. 12 ha novellato l'art. 268 c.p.p., riguardante l'esecuzione delle operazioni di intercettazione delle comunicazioni.[1] La ratio di tale scelta era dovuta alla convinzione del legislatore che la previgente normativa del codice fosse adeguata a disciplinare anche l'acquisizione della prova digitale, cosicché si evitò la creazione di nuove norme in favore di una mera estensione degli istituti tradizionali.

Specifiche innovazioni processualpenalistiche in materia di reati informatici sono quelle del 1996 con legge n. 66 e del 1998 con legge n. 269, per la repressione della violenza sessuale e della pedopornografia on line. Le suddette leggi sono dirette verso metodi investigativi più decisi di contrasto a tali reati, e orientate ad una specializzazione per i crimini informatici da parte della polizia giudiziaria. In particolare, l'art. 14 della legge n. 269 del 1998 ha regolato la discussa figura dell'agente provocatore e l'utilizzo dei c.d. siti civetta, necessari per il contrasto a quei reati di pedopornografia tassativamente elencati dallo stesso articolo.

Pertanto, per taluni reati di pedopornografia indicati dalla legge, gli ufficiali di polizia giudiziaria possono procedere all'acquisto simulato di materiale pedopornografico, nell'ambito di operazioni autorizzate dall'autorità giudiziaria. Se tali delitti sono effettuati con un sistema telematico, le indagini sono attribuite alla sola polizia postale in un'ottica di specializzazione e l'agente provocatore può agire solo su richiesta dell'autorità giudiziaria. L'attività dell'agente provocatore rimane scriminata solo ove vengano rispettati i limiti fissati dal legislatore e il suo intervento costituisca mera attività di osservazione, mentre è punibile a titolo di concorso se la sua condotta si inserisce con rilevanza causale nel delitto. Crimini del pedofilo differenti da quelli tassativamente previsti non potranno essere perseguiti dall'agente provocatore, ed in tali casi gli elementi di prova diverranno inutilizzabili anche nella fase pre-processuale delle indagini preliminari.

Più consistenti e incisive della normativa del 1993 sono state le modifiche al codice di procedura penale, apportate dalla legge n. 48 del 2008 di "ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno".

Tali integrazioni hanno interessato l'adozione di misure volte ad assicurare l'acquisizione, protezione e conservazione dei dati informatici, con particolare riferimento ad ispezioni,

CamminoDiritto.it
ISSN 2532-9871

perquisizioni e sequestri. Il legislatore del 2008 ha aggiornato le disposizioni in tema di mezzi di ricerca della prova estendendole ai sistemi informatici o telematici con riguardo alla conservazione e non alterabilità dei dati. Specifica rilevanza è stata attribuita alla computer forensics e alla conservazione e inalterabilità delle digital evidence nella fase delle indagini. In rispondenza a quanto disposto dalla Convenzione di Budapest, è stato finalmente attribuito degno rilievo alla caratteristica di a-territorialità e di transnazionalità dei reati informatici e di globalizzazione della rete.

E' stata altresì favorita una concertazione fra i Paesi firmatari, armonizzazione a livello legislativo, cooperazione e collaborazione giudiziaria (come ad esempio l'accesso transfrontaliero ai file, che permette ai magistrati di acquisire materiale probatorio da server situati in altri Paesi). L'art. 11 della suddetta legge ha novellato, inoltre, l'art. 51 c.p.p. attribuendo la competenza per i crimini informatici all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente.

L'accentramento di tali competenze può essere comprensibile per i reati di criminalità organizzata o il contrasto ad organizzazioni terroristiche, giacché favorisce il coordinamento delle indagini e la formazione di gruppi di lavoro specializzati nello sradicamento di fenomeni unitari quali le infiltrazioni mafiose sul territorio, ma l'estensione, anche ai crimini informatici, di una deroga al principio di rango costituzionale del giudice naturale precostituito per legge, appare indubbiamente sproporzionata, rischiando, fra l'altro, di rallentare l'attività delle procure del capoluogo del distretto, creando un eccessivo sovraccarico. Notevoli sono, inoltre, le contraddizioni di tale norma: innanzitutto nell'enucleazione dei reati informatici è stato omesso inspiegabilmente l'art. 635 quinquies c.p., inoltre l'accentramento di attribuzioni alle procure, non è stato inizialmente associato ad analogo accentramento delle competenze del G.I.P. e del G.U.P, per cui si è resa necessaria una novella (legge n. 125 del 2008) onde correggere la suddetta discrasia.

La legge del 2008 ha, infine, all'art. 12, previsto l'istituzione di un fondo per il contrasto della pedopornografia su Internet e per la protezione delle infrastrutture informatiche di interesse nazionale.

Modifiche al codice di rito in tema di pedofilia on line, sono state successivamente inserite con legge 172/2012 di ratifica della Convenzione di Lanzarote del 2007: fra queste, l'aumento delle competenze della procura distrettuale per reati associativi di sfruttamento e abuso sessuale contro i minori, aumento della durata delle indagini preliminari per tale tipologia di crimine, arresto obbligatorio in flagranza di reato e aumento delle ipotesi di allontanamento dalla famiglia.

CamminoDiritto.it
ISSN 2532-9871

2. Le carenze della normativa.

La legge n. 48 del 2008 nasce dalla consapevolezza del legislatore che il dato informatico non possa essere considerato alla stregua di qualsiasi altro elemento probatorio. Obiettivo primario della disciplina del 2008 e successive modifiche, è stata, perciò, l'esigenza di regolamentare la genuina acquisizione di elementi di prova durante le indagini preliminari.

Nonostante l'assunto di partenza sia ampiamente condivisibile, essa suscita notevoli dubbi, soprattutto in riferimento al fatto che si sia limitata ad adeguare le disposizioni previgenti anche ai dati informatici, con particolare riferimento alla loro conservazione,[2] custodia ed analisi, senza considerare la diversa natura del bene da tutelare e senza prevedere un apparato di garanzie difensive che consenta un controllo sull'operato degli inquirenti. Manca, invero, qualsivoglia riferimento al rispetto dei protocolli e alle best practice di computer forensics.

Il legislatore ha, infatti, stabilito soltanto che debbano essere adottate le prescrizioni necessarie ad assicurare la conservazione e ad impedire l'alterazione del dato informatico, senza specificare le procedure e il loro iter e senza alcun accenno al modus operandi degli investigatori e alle modalità di duplicazione delle evidenze digitali. Ciò rappresenta un considerevole limite della attuale normativa. Sarebbe stato invece opportuno un riferimento preciso ai protocolli e alle best practice da seguire, come è invece condivisibilmente avvenuto con la legge Gelli-Bianco del 2017 in materia di colpa medica.

Secondo il parere dello scrivente, l'assenza di riferimenti alle metodologie da seguire per l'accertamento accresce in maniera eccessiva la discrezionalità degli inquirenti, a nocumento di un procedimento penale che dovrebbe invece essere basato sulle garanzie dell'indagato e dell'imputato. Certamente il riferimento alle metodologie non deve consistere in un particolareggiato elenco di operazioni tecniche e pratiche da seguire pedissequamente senza alcun margine di discrezionalità per l'inquirente, ma deve al minimo prevedere il rispetto di quelle prassi e operazioni di base che tutelino l'indagato nei confronti di atti dolosi o colposi che possano inquinare le evidenze informatiche durante tutta la fase delle indagini dall'acquisizione del dato fino all'archiviazione dello stesso.[3]

Ciò in quanto, proprio il dato informatico, più di qualunque altro, è soggetto ad alterazioni ed 'inquinamenti' di vario tipo, siano essi volontari ma soprattutto involontari. L'indeterminatezza delle procedure di acquisizione delle digital evidence crea anche

CamminoDiritto.it
ISSN 2532-9871

difficoltà al giudice in caso di contestazione da parte della difesa sull'ammissibilità di una prova. Il magistrato non avrà, infatti, alcun parametro su cui basarsi, se non il verbale compilato dagli stessi investigatori, per poter ponderare e decidere se vi sia stato il rispetto delle procedure e se il dato possa considerarsi alterato o meno.

Assolutamente non condivisibile è l'orientamento della **Cassazione (Sez. Penale I, 18/3/2009 n. 11863)** che considera aprioristicamente l'accertamento da parte della polizia giudiziaria durante le indagini compiuto «da personale esperto perfettamente in grado di evitare la perdita dei dati medesimi».

Si arriva, in tal modo, addirittura ad una presunzione della correttezza dell'iter di acquisizione del dato informatico. Non appare una metodologia valida con riguardo al rispetto delle regole del processo e del contraddittorio, quella di non fissare dei limiti ad un organo, con la giustificazione che lo stesso ha competenza e professionalità tali da non commettere errori e non eccedere nell'utilizzo del potere di cui dispone. Se valesse tale assunto verrebbe ad essere disconosciuto, in quanto superfluo, lo stesso principio della separazione dei poteri. Suscitano dubbi, peraltro, alcune sentenze secondo le quali deve essere a carico della difesa la dimostrazione dell'alterazione del dato digitale, specialmente in presenza di atti urgenti compiuti senza la partecipazione del difensore, che non avrebbe, a tal riguardo, alcuno strumento a supporto delle proprie contestazioni.

Fortemente criticabile è anche quella corrente giurisprudenziale secondo cui l'art. 192 c.p.p. consentirebbe al giudice di valutare anche evidenze digitali acquisite in violazione di criteri scientifici.[4] Non deve, infatti, essere equivocata la libertà di valutazione della prova con l'acquisizione della prova stessa, che deve invece rispettare le regole del contraddittorio, senza eludere i principi del diritto processuale penale. Una cosa è la libera valutazione della prova da parte del giudice, mentre cosa diversa, e non tollerabile in un processo tendenzialmente accusatorio e basato sul contraddittorio, è la presunta libertà del giudice di poter valutare prove acquisite illegalmente.

Ma la maggior criticità della attuale normativa processuale sui cyber crimes riguarda la conciliabilità fra l'attività di ricerca della prova durante le indagini e la struttura del nostro processo penale, basata sul contraddittorio fra le parti in dibattimento. Nell'accertamento del fatto sono, infatti, cambiati gli equilibri fra gli elementi che conducono il giudice alla formazione del proprio convincimento.[5] Le indagini informatiche rischiano di alterare le caratteristiche del processo accusatorio limitando la centralità del contraddittorio, giacché le prove vengono raccolte nella fase delle indagini e portate al processo già cristallizzate.

Il nostro attuale processo penale dovrebbe essere basato sul principio di oralità e sul confronto tra le parti nel dibattimento, luogo di formazione della prova. Quest'ultima non

CamminoDiritto.it
ISSN 2532-9871

dovrebbe, perciò, essere prodotta nella fase delle indagini, in ossequio al principio del contraddittorio, dell'oralità e nel rispetto dell'art. 111 della Costituzione nella sua nuova formulazione.[6] Tuttavia, la fase delle indagini è divenuta sempre più il fulcro del procedimento penale, ove vengono raccolti gli elementi che saranno poi alla base della decisione del giudice, in particolar modo ove vi siano accertamenti scientifici e prove tecnologiche, come nelle ipotesi riguardanti i reati informatici. Sempre più spesso i difensori, in dibattimento, basano la propria tesi difensiva sulla contestazione dell'attività d'indagine per la formazione della prova.

Tale attività investigativa comprovata dai verbali, definita "catena di custodia"[7] si scinde nelle fasi dell'acquisizione, dell'analisi e della conservazione del dato. Ciascuna di esse presenta delle criticità, che sempre più spesso sono alla base del confronto in dibattimento fra accusa e difesa, con riguardo alla loro ammissibilità. Si rischia, così, un predominio della prova scientifica, ed in particolare quella digitale, all'esito delle indagini, che di fatto limita il libero convincimento del giudice, il quale raramente riesce a discostarsi dal risultato scientifico. Questi dovrebbe invece valutare discrezionalmente l'efficacia probatoria del mezzo istruttorio: le prove digitali acquisite durante le indagini dovrebbero solo essere un aiuto alla decisione, senza mai stravolgere o anche solo alterare l'assetto processuale.

L'acquisizione sistematica di prove già formate e inserite nel fascicolo del dibattimento in applicazione dell'art. 431 c.p.p. comma 1 lettere b) e c) sembra, invero, più consona al vecchio sistema inquisitorio e non a quello attuale. Per evitare pericolose derive del processo penale, è perciò necessario che il giudice ponga in essere una valutazione del dato informatico equilibrata, senza considerare le argomentazioni tecniche prodotte durante le indagini come una prova già formata ed inconfutabile.

Le prove acquisite senza garanzia di genuinità ed in assenza del rispetto dei protocolli dovrebbero, inoltre, essere dichiarate inammissibili dal giudicante, senza possibilità di essere valutate discrezionalmente dallo stesso come elementi indiziari. L'eccessiva discrezionalità degli inquirenti durante la fase delle indagini nell'acquisizione della prova e del giudice in dibattimento nella valutazione della stessa, sono indubitabilmente frutto di una carenza legislativa, ed in particolare dell'assenza di sanzioni quali l'inutilizzabilità della prova in caso di mancato rispetto dei protocolli.

3. Accertamenti tecnici ripetibili e irripetibili.

Gli accertamenti tecnici, disciplinati nel codice di rito nel titolo V riguardante l'attività del pubblico ministero, si distinguono in ripetibili (art. 359 c.p.p.) e non ripetibili (art. 360 c.p.p.). Questi ultimi, a differenza dei primi, coinvolgono persone, cose o luoghi il cui

CamminoDiritto.it
ISSN 2532-9871

stato è soggetto a modificazioni. La distinzione è di particolare importanza in quanto solo i verbali degli atti non ripetibili, compiuti in presenza di precise garanzie difensive, possono essere raccolti nel fascicolo per il dibattimento (art. 431 comma 1 lett. b) e c). In considerazione della struttura del nostro procedimento penale, difatti, gli atti di indagine sono inidonei a produrre risultati probatori, in quanto dovrebbero esaurire la propria funzione nella fase preliminare, finalizzata solo al reperimento e conservazione delle fonti di prova.

Secondo le regole del contraddittorio, la formazione della prova deve infatti avvenire in dibattimento, davanti al giudice terzo. Tale principio è però limitato da alcune eccezioni. Durante le indagini può, infatti, aver luogo un incidente probatorio (artt. 392 - 404 c.p.p.), con cui può procedersi all'assunzione anticipata del mezzo di prova. Se non è possibile la ripetizione di un atto di indagine, i verbali relativi vengono inseriti nel fascicolo dibattimentale costituendo fonte di prova (art. 431 c.p.p. lett. b e c). Bisogna poi considerare i riti speciali come il giudizio abbreviato, ove i risultati delle indagini costituiscono gli unici elementi a disposizione del giudice per la decisione, in quanto non è previsto il dibattimento.

Con riguardo al dato informatico, a differenza della dottrina e del parere degli esperti del settore, la Cassazione è, secondo un consolidato orientamento, dell'opinione che la sua acquisizione sia priva di rischi di alterazione, perciò sia «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» (**Cass. Sez. I Penale, sent. n. 14511 del 2009**).

Sempre per la Suprema Corte «non dà luogo ad accertamento tecnico irripetibile la lettura dell'hard disk di un computer», pertanto «l'estrazione dei dati contenuti in un supporto informatico, se eseguita da personale esperto in grado di evitare la perdita dei medesimi dati, costituisce un accertamento tecnico ripetibile» (**Cass. Sez. I Penale, n. 11863 del 2009**).

Nella recente **sentenza n. 29061 del 2015**, poi, la II Sez. Penale statuisce «non dà luogo ad accertamento tecnico irripetibile l'estrazione dei dati archiviati in un computer, trattandosi di operazione meramente meccanica, riproducibile per un numero indefinito di volte». Per la Suprema Corte, perciò, atti come la duplicazione di un hard disk non costituiscono accertamento irripetibile, in quanto è escluso che il personale possa provocare la perdita o l'alterazione dei dati.

CamminoDiritto.it
ISSN 2532-9871

Tesi, invero, confutata da innumerevoli giudici di merito di primo e secondo grado. Nel noto processo contro Alberto Stasi (c.d. omicidio di Garlasco) il G.U.P. ha affermato, con riguardo al rilievo ed acquisizione dei dati informatici dal sistema, che «il collegio peritale evidenziava che le condotte scorrette di accesso da parte dei Carabinieri hanno determinato la sottrazione di contenuto informativo con riferimento al personal computer di Alberto Stasi pari al 73,8% dei files visibili (oltre 156 mila)», e che «queste alterazioni indotte da una situazione di radicale confusione nella gestione e conservazione di una così rilevante quanto fragile fonte di prova da parte degli inquirenti nella prima fase delle indagini ha comportato, in primo luogo, il più che grave rischio che ulteriori stati di alterazioni rimuovessero definitivamente le risultanze conservate ancora nella memoria complessiva del computer [...] non è più possibile esprimere delle valutazioni certe né in un senso né nell'altro: in questo ambito, il danno irreparabile prodotto dagli inquirenti attiene proprio all'accertamento della verità processuale».

Conclude il giudice con un'affermazione che lascia poco spazio a interpretazioni o a opinioni contrastanti: «interventi che hanno prodotto effetti devastanti in rapporto all'integrità complessiva dei supporti informatici». Ciò non fa altro che avvalorare la tesi della consapevolezza da parte di giudici e consulenti esperti informatici, di possibili errori compiuti dagli inquirenti nello svolgimento di indagini sui crimini informatici, e della conseguente necessità di creare regolamenti tecnici ufficiali di buone pratiche e protocolli di computer forensics ministeriali, emanati da una commissione composta da esperti, ma soprattutto che l'acquisizione di dati di tale fragilità ed evanescenza, non possa non essere considerata un atto irripetibile. Necessiterebbe, pertanto, delle tutele difensive previste dalla legge per tale tipologia di atti.

A differenza di quelli ripetibili, gli accertamenti disciplinati dall'art. 360 c.p.p., proprio per la loro irripetibilità, richiedono una procedura che preveda idonee garanzie difensive. Il pubblico ministero deve infatti avvisare senza ritardo la persona sottoposta alle indagini e l'offeso dal reato e i loro difensori, del conferimento dell'incarico e della facoltà di nominare consulenti tecnici. Difensori e consulenti tecnici eventualmente nominati hanno diritto di assistere al conferimento dell'incarico, di partecipare agli accertamenti e di formulare osservazioni e riserve. Sono però escluse da tali garanzie quelle attività di polizia giudiziaria previste dall'art. 354 c.p.p., ossia accertamenti urgenti sui luoghi, sulle cose e sulle persone, e il loro sequestro. A mente dell'art. 354 c.p.p. «Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero. Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. Se del caso, sequestrano il corpo del reato e le cose a questo

CamminoDiritto.it
ISSN 2532-9871

pertinenti. Se ricorrono i presupposti previsti dal comma 2, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi alle persone diversi dalla ispezione personale».

La legge 48 del 2008, in tema di reati informatici, ha aggiunto al comma 2 dell'art. 354 c.p.p. il seguente periodo: «In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità».

Pertanto le garanzie difensive ex art. 360 c.p.p. non sono concesse qualora sia necessario compiere accertamenti urgenti, ove vi sia pericolo che tracce o luoghi siano soggetti ad alterazione. La polizia giudiziaria può, pertanto, svolgere operazioni senza l'obbligo di disporre il sequestro.[8] Tali operazioni vanno comunque documentate con verbale. Nessun parametro fornisce la legge circa l'urgenza e il rischio di alterazioni, lasciando agli investigatori ampia discrezionalità di compiere gli accertamenti ex art. 354 c.p.p. Superflua, a parere dello scrivente, è la novella all'art. 354 c.p.p. apportata con legge n. 48/2008 con riguardo ai dati informatici: essa, in realtà, ribadisce quanto già stabilito al primo comma circa la conservazione delle cose pertinenti al reato, limitandosi a chiarire che in relazione ai dati informatici la polizia giudiziaria debba adottare le misure tecniche necessarie alla loro conservazione, senza peraltro fornire alcuna indicazione relativa alla loro inalterabilità. Appare evidente che, unico interesse del legislatore, riguardi la conservazione del dato informatico, senza alcun minimo accenno a fonti normative, o quanto meno di soft law, che possano fissare delle tecniche di acquisizione dei dati che assicurino «la conformità della copia all'originale e la sua immodificabilità».

L'art. 356 c.p.p. afferma, poi, che «il difensore della persona nei cui confronti vengono svolte le indagini ha facoltà di assistere, senza diritto di essere preventivamente avvisato, agli atti previsti dagli artt. 352 e 354». A ben vedere, l'art. 356 c.p.p., se da un lato prevede un'importante garanzia per l'indagato nel momento in cui consente al suo difensore di assistere anche ad accertamenti urgenti ex articoli 352 e 354 c.p.p., dall'altro, in concreto, ne mina la rilevanza nel momento in cui esclude il diritto di preventivo avviso. Del resto, la giurisprudenza di legittimità ha in più occasioni confermato l'orientamento per cui in caso di atti urgenti, la polizia giudiziaria che non attenda l'arrivo del difensore, nonostante questi abbia esternato la volontà di parteciparvi, non violi i diritti di difesa dell'indagato[9].

4. Data retention.

CamminoDiritto.it
ISSN 2532-9871

Innumerevoli sono state le critiche mosse da parte della dottrina più garantista[10] alla novella, con legge n. 48/2008, dell'art. 254 bis c.p.p., che prevede il sequestro di dati presso il fornitore di servizi informatici, telematici e di telecomunicazioni.

La principale incongruenza consiste nel conferimento di poteri investigativi e di conservazione dei dati in capo a soggetti privati che, peraltro, potrebbero essere interessati direttamente o indirettamente dall'inchiesta. Oltre a non avere le capacità tecniche e alcun obbligo di verbalizzazione delle procedure di conservazione, potrebbero, pertanto, avere addirittura interesse all'alterazione del dato, con grave nocumento di altri soggetti coinvolti.

Ulteriori critiche vanno mosse alla nuova normativa del nostro Paese in materia di data retention (Legge Europea 2017 n. 167/2017 art. 24) che prevede l'obbligo per gli operatori telefonici di conservare il traffico telefonico e telematico per un termine minimo di 72 mesi. Tali tempistiche di conservazione dei dati di traffico telematico e telefonico, risultano palesemente eccessive, sollevando dubbi sulla proporzionalità e adeguatezza della norma, poiché la violazione dei diritti sulla privacy non si limita ai soli indagati o agli imputati, ma interessa tutti gli utenti. Essa va a confliggere con la Data Retention Directive (Direttiva 2006/24/CE) e soprattutto con la disciplina dell'art. 132 del "Codice della privacy".

Una sentenza della Corte di Giustizia del 2014, aveva persino annullato la Data Retention Directive nella parte in cui stabiliva un termine di conservazione dei dati compreso tra 6 mesi e 24 mesi,[11] considerandolo eccessivo, schierandosi apertamente contro la c.d. sorveglianza digitale di massa. Secondo la Corte, tale direttiva determinava una grave ingerenza nei confronti di diritti fondamentali quali il rispetto della vita privata e protezione dei dati personali, ponendosi in contrasto con il principio di proporzionalità in quanto limitava i suddetti diritti ben oltre il minimo necessario.

L'attuale legge è pertanto in palese contrapposizione con le prescrizioni dell'Europa, giacché prevede un termine minimo pari a 12 volte quello minimo e al triplo del massimo previsto dalla direttiva, a sua volta annullato dalla Corte di Giustizia in quanto ritenuto eccessivo, ed in evidente violazione del diritto di privacy.

Pertanto, in tema di data retention le garanzie difensive risultano quanto mai sacrificate: se suscitano perplessità le acquisizioni di dati informatici e la loro conservazione da parte degli inquirenti in assenza di precise regole di computer forensics e di relative sanzioni, ancor più inquietante risulta l'acquisizione e conservazione di dati e materiale probatorio da parte di privati, peraltro non formati in materia di freezing e senza alcun obbligo di

CamminoDiritto.it
ISSN 2532-9871

verbalizzazione.

Oltre alla previsione di un periodo eccessivo di data retention dei dati telefonici e informatici, l'attuale normativa del nostro Paese non fissa, peraltro, alcun criterio oggettivo di conservazione degli stessi. Risulta, così, realmente difficile il rispetto dell'art. 16 della Convenzione di Budapest (supra, nota n. 2).

5. Mezzi di ricerca della prova.

La legge del 2008 ha novellato il comma 2 dell'art. 244 c.p.p., aggiungendo la possibilità per l'autorità giudiziaria di disporre l'ispezione, ossia rilievi segnaletici, 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 la loro inalterabilità.

Nonostante l'attività di ispezione prevista dall'art. 244 c.p.p. dovrebbe limitarsi alla semplice osservazione, nella maggioranza dei casi viene a dissolversi il limite fra questa e la perquisizione. L'attività di ispezione durante la fase delle indagini, rischia perciò di alterare i dati digitali, per loro natura evanescenti. A ben vedere lo stesso legislatore del 2008 nella novella dell'art. 244 c.p.p. aveva constatato uno sconfinamento dell'ispezione nell'ambito della perquisizione, altrimenti non avrebbe avuto necessità di rimarcare l'adozione di misure atte alla inalterabilità dei dati.

L'ispezione del dato digitale si trasforma, in tal modo, in un atto irripetibile, nei confronti del quale sarebbe necessaria l'attribuzione di tutte le garanzie difensive previste ex art. 360 c.p.p. Ove le garanzie non fossero rispettate, il giudice dovrebbe dichiarare inammissibili le evidenze informatiche. Tuttavia nella prassi il giudice continua a considerare l'ispezione, anche quando non si limita alla mera osservazione, un atto ripetibile.

Anche riguardo la perquisizione informatica, le novelle poste dalla normativa del 2008, con l'introduzione dell'art. 247 comma 1 bis c.p.p., si sostanziano nell'adozione di misure volte ad assicurare la conservazione dei dati digitali impedendone l'alterazione. Per l'art. 247 comma 1 bis c.p.p. «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».

CamminoDiritto.it
ISSN 2532-9871

Le maggiori problematiche non riguardano l'attività "post mortem", ossia su terminale spento, ma quella c.d. "live", su un computer acceso al momento dell'acquisizione dei dati sulla scena criminis, giacché in tal caso i rischi di perdita e alterazione delle evidenze digitali sono notevoli. Alcune memorie dell'elaboratore (memoria cache e memoria ram) vengono, infatti, automaticamente cancellate al momento dello spegnimento del pc. E' perciò necessaria la presenza di personale esperto per l'acquisizione dei dati di un terminale live (attività definita dump), e di strumentazione specifica che ne permetta il recupero e l'archiviazione senza possibilità di appiglio per la difesa dell'indagato, che potrebbe chiedere l'inammissibilità delle evidenze informatiche perché alterate al momento dell'acquisizione.

Secondo autorevole dottrina,[12] in tali casi le garanzie difensive dovrebbero essere ampliate, traducendosi sostanzialmente in un'attività non ripetibile, che necessita pertanto delle protezioni previste dall'art. 360 c.p.p.

La perquisizione, attività volta all'individuazione e acquisizione del corpo del reato e cose ad esso pertinenti, viene effettuata in sede di indagini preliminari su iniziativa del pubblico ministero, il quale può procedere personalmente o delegare gli ufficiali di polizia giudiziaria (art. 247 c.p.p.). Questi ultimi, ai sensi dell'art. 352 c.p.p., possono compiere di propria iniziativa perquisizioni nella flagranza del reato o nel caso di evasione, se hanno fondato motivo di ritenere che sulla persona o in un determinato luogo si trovino occultate cose o tracce pertinenti al reato che possono essere cancellate o disperse.

L'art. 352 comma 1 bis c.p.p., aggiunto con legge n. 48/2008, afferma che nella flagranza del reato, gli ufficiali di polizia giudiziaria, adottando le misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, se hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce pertinenti al reato, che possono essere alterati o dispersi. Le garanzie dell'indagato sono stabilite dal comma 4 dello stesso articolo che afferma: «La polizia giudiziaria trasmette senza ritardo, e comunque non oltre le quarantotto ore, al pubblico ministero del luogo dove la perquisizione è stata eseguita il verbale delle operazioni compiute. Il pubblico ministero, se ne ricorrono i presupposti, nelle quarantotto ore successive, convalida la perquisizione».

Come si può desumere anche dall'art. 352 c.p.p., la perquisizione, in particolare quella informatica, deve essere giustificata da un "fondato motivo" e non utilizzata come metodo di ricerca di un'eventuale notizia di reato, altrimenti verrebbe a mancare l'esigenza probatoria sottesa al provvedimento. In tali casi, qualora mancasse un fondato motivo, il pubblico ministero non dovrebbe convalidare la perquisizione.

CamminoDiritto.it
ISSN 2532-9871

A tal proposito, la Suprema Corte si è più volte espressa affermando che l'acquisizione indiscriminata di informazioni e dati contenuti all'interno della memoria di un computer non può e non deve risolversi in una distorsione delle attività d'indagine volte alla ricerca della notitia criminis. E' opportuno sottolineare che, ove i terminali sottoposti a perquisizione fossero protetti da password, l'indagato non avrebbe alcun obbligo di rivelarla agli inquirenti. Nel caso in cui fosse richiesta allo stesso, questi dovrebbe essere informato del diritto di rifiutare di riferirla. Non dovrebbe inoltre essere ammesso alcun tipo di pressione da parte degli inquirenti per ottenere la password del cellulare, computer, o altro strumento elettronico, in quanto tale diritto dovrebbe essere equiparato alla facoltà di non rispondere dell'indagato.[13]

Le criticità relative al sequestro sorgono dalla necessità di conciliare l'interesse all'acquisizione di elementi utili per la prosecuzione delle indagini con il rispetto della privacy della persona ad esso sottoposta, in considerazione del fatto che, per le eventualità di inquinamento, il materiale rimasto in possesso del perquisito non possa essere successivamente utilizzabile. A tal fine sarebbe da evitare un'acquisizione indiscriminata sia dell'hardware che dei dati presenti su un computer, ma nello stesso tempo non deve essere tralasciato alcun elemento probatorio, in quanto non più utilizzabile successivamente.

Un sequestro mirato non è, tuttavia, sempre possibile, per la difficoltà di stabilire a priori, sulla scena criminis, le evidenze informatiche necessarie alle indagini e quelle superflue, specialmente in considerazione del fatto che il p.m. deve cercare le prove sia a carico che a discarico dell'indagato. Di questo parere era, in un primo momento, la giurisprudenza dominante, che aveva affermato che non si potevano a priori individuare i supporti informatici necessari alle indagini. Tale orientamento aveva esteso il sequestro a tutte le periferiche, non per esigenze investigative ma per maggior comodità della p.g.

Parte della giurisprudenza aveva cercato di porre riparo al sequestro probatorio indiscriminato, che includeva anche periferiche di input/output quali tastiere, monitor, e stampanti, statuendo che dovesse disporsi il dissequestro e la restituzione «di accessori del computer che non possono ritenersi rientranti nel concetto di corpo del reato, non essendo cose mediante le quali è stato commesso il reato».[14] Stante la possibilità di duplicazione dei dati del PC, sarebbe invece auspicabile un minor ricorso al sequestro dell'elaboratore, o anche solo delle memorie dello stesso, per rendere meno invasivi gli effetti dell'accertamento nella vita e nelle abitudini dei soggetti coinvolti.

Tutto ciò al fine di evitare la lesione di diritti costituzionalmente garantiti, nei casi in cui non vi sia la necessità di un sequestro preventivo, ma solo probatorio. La giurisprudenza di legittimità (Cassazione Pen. Sez. I sent. n. 25766 del 2007) aveva stabilito che

CamminoDiritto.it
ISSN 2532-9871

nell'ambito informatico vi deve essere «proporzione tra il contenuto del provvedimento emesso e le esigenze di accertamento dei fatti che deve avvenire con particolare rigore, evitando quanto più possibile interventi inutilmente invasivi».

La recentissima sentenza n. 31918/2017 della Cassazione, ha tentato di fare chiarezza sull'argomento per superare le discordanze giurisprudenziali, approvando l'estensione delle ipotesi di sequestro a tutto l'hardware, con ampia discrezionalità dell'operatore, anche nei casi in cui la notizia di reato sia soltanto delineata e suscettibile di approfondimenti istruttori.

Anche il sequestro integrale ed indiscriminato di tutti i dati digitali presenti su un apparecchio elettronico (computer, tablet, smartphone, ecc.), compresi perciò quelli non pertinenti al reato, in linea di principio dovrebbe essere evitato, nel rispetto della privacy del soggetto sottoposto alle indagini e del principio di proporzionalità e adeguatezza. Al riguardo la Suprema Corte ha avuto un orientamento non univoco.

Nella sentenza della **Sez. VI Penale n. 24617 del 2015**, ha chiaramente affermato la sua avversità al sequestro generalizzato, statuendo che «non è possibile acquisire in modo indiscriminato un intero archivio elettronico, sol perché è facile l'accesso, l'effettuazione di copia ed il trasferimento fisico rispetto alla massa di documenti cartacei corrispondenti, pur in assenza di qualsiasi correlazione specifica con le indagini». Nelle più recenti sentenze (**Cass. Sez. V Penale, sent. n. 1822 del 2018**) la Cassazione ha però confermato un diverso precedente orientamento, secondo il quale la copia forense integrale è una modalità conforme alla legge, che peraltro mira a proteggere, nell'interesse delle parti, l'integrità ed affidabilità del dato. Inoltre, ove l'attività di analisi per la selezione dei dati sia particolarmente complessa, non può essere condotta nell'arco temporale ridotto delle attività di perquisizione e sequestro. Generalmente, non è ammissibile il sequestro per finalità esplorative, come strumento di ricerca della notitia criminis, in particolare nel caso di sequestro presso terzi, ove avvengono intrusioni illegittime nella sfera personale del soggetto.

Per ciò che riguarda le intercettazioni telefoniche e ambientali, queste devono essere autorizzate dal GIP ove sussistano gravi indizi di reità e l'indispensabilità ai fini della prosecuzione delle indagini, su richiesta del p.m., e dovranno essere prorogate ogni 15 giorni. Le intercettazioni telematiche disciplinate all'art. 266 bis c.p.p., prevedono minori tutele rispetto quelle telefoniche. Tale distinzione crea incertezza con riguardo al campo d'azione delle tutele, ove si utilizzino particolari tecnologie telefoniche che usano canali della rete (ad. es. il noto strumento di comunicazione Skype): data la loro natura ibrida non è chiaro se ricevano le tutele delle intercettazioni telefoniche o di quelle telematiche.

CamminoDiritto.it
ISSN 2532-9871

Problemi analoghi sussistono anche riguardo le e-mail: la richiesta di accesso alla casella di posta presso il fornitore di servizi dovrebbe essere ricondotta nell'ambito del sequestro e non dell'intercettazione. La possibilità per il p.m. di disporre anche di impianti esterni privati per le intercettazioni, rende più complesso il controllo da parte dell'autorità giudiziaria, privando l'indagato delle garanzie difensive. Riguardo l'intercettazione su chat e piattaforma WhatsApp, il recente intervento della Cassazione (**2017 n. 32146**) stabilisce l'utilizzabilità anche senza rogatoria delle intercettazioni di chat gestite su territorio estero, spostando la competenza in Italia, in quanto i dati sono registrati con impianti nazionali e scambiati su territorio italiano. Ciò permette un esercizio più snello dell'attività investigativa, ma soprattutto una maggiore prevenzione in caso di rischio di attentati di matrice terroristica.

6. Garanzie dell'indagato e recente giurisprudenza in materia di detenzione di materiale pedopornografico.

L'accertamento dei reati di pornografia minorile virtuale richiede particolare attenzione da parte degli investigatori, per evitare il rischio di rendere inutilizzabili dati ed evidenze informatiche necessari all'incriminazione e alla condanna di soggetti che si macchiano di crimini di elevata riprovazione sociale. Sempre più spesso sono state le corti sovranazionali a smentire gli orientamenti giurisprudenziali nazionali, mossi talvolta dalla impazienza di punire crimini così abietti, senza avvedersi che talvolta vengono calpestati diritti costituzionalmente protetti.

Prendendo spunto dalle predette considerazioni, non si può non esaminare una recente sentenza della Corte Europea dei Diritti dell'Uomo, che ha suscitato grande interesse e scalpore a livello internazionale (**Corte Europea dei Diritti dell'Uomo - Sezione Terza, Sentenza 30 maggio 2017, n. 32600/12)**, sottolineando il crescente rilievo che la tutela della sfera privata dell'individuo ha assunto negli ordinamenti sovranazionali, in particolare fra i Paesi dell'Unione europea.

Il caso concreto al vaglio della Corte EDU, vede coinvolto un uomo spagnolo che lascia il computer portatile al tecnico informatico per compiere delle riparazioni. Quest'ultimo si avvede della presenza sul disco fisso di un ampio quantitativo di materiale pedopornografico, denunciando il fatto alle autorità e consegnando loro il computer. Nonostante non vi sia alcun rischio di manomissione, la polizia effettua l'accesso senza attendere l'autorizzazione giudiziaria. Dal conseguente processo il proprietario del PC subisce una condanna per detenzione e diffusione di immagini pedopornografiche.

Ritenendo violati i suoi diritti, questi ricorre in appello, e poi presso la Corte Costituzionale spagnola, ma in entrambi i casi il ricorso viene respinto. La Corte

CamminoDiritto.it
ISSN 2532-9871

Costituzionale ritiene giustificato l'accesso al computer in quanto non era protetto da alcuna password, deducendone che il soggetto non avesse intenzione di stabilire limiti all'accesso. L'uomo si appella alla Corte EDU, la quale accoglie il ricorso rilevando che l'accesso ai file, per le modalità in cui si è verificato, costituisce una violazione al suo diritto alla vita privata e alla corrispondenza, ed è per questo ingiustificabile.

Secondo la Corte di Strasburgo, difatti, non sussisteva una condizione di emergenza che giustificasse l'analisi del computer da parte della polizia senza preventiva autorizzazione del giudice. L'articolo 8 della Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle libertà fondamentali, stabilisce che ogni persona ha diritto al rispetto della propria vita privata e della corrispondenza e che, nell'esercizio di tale diritto, non può esservi ingerenza di una autorità pubblica a meno che sia prevista dalla legge e costituisca una misura necessaria al perseguimento della sicurezza nazionale e pubblica, alla prevenzione dei reati, alla protezione della salute o della morale, o dei diritti e delle libertà altrui.

La Corte EDU ha dovuto valutare se tale diritto dovesse godere della sua massima estensione anche in presenza di condotte integranti il reato di pedopornografia, definito "abominevole" dalla stessa Corte. La pronuncia rafforza l'idea che proprio per la gravità di reati di questo genere, chi ha la responsabilità della raccolta delle prove è tenuto svolgere il compito nel pieno rispetto delle regole, per evitare che diventino inutilizzabili all'interno del processo.

Sempre in tema di detenzione di materiale pedopornografico, notevoli critiche ha suscitato la sentenza della **Corte d'Appello di Roma (Sez. III sent. 17/01/2013)**, che ha assolto da tale reato, previsto e punito dall'art. 600 quater c.p., l'imputato condannato in primo grado. Secondo la Corte infatti, l'intervenuta cancellazione dei file d'immagine di contenuto pedopornografico acquisiti on line, esclude il reato, in quanto costituisce indice della volontà dell'imputato non già di disporre di dette immagini, bensì di disfarsene. Detto materiale, nel caso di specie, era stato cancellato dall'imputato e recuperato dal consulente utilizzando un apposito programma.

La Corte giunge a tale conclusione in quanto: «non appare pertanto possibile escludere, con la necessaria sicurezza, l'eventualità di una acquisizione meramente accidentale. La descritta equivocità delle emergenze probatorie non consente pertanto, ad avviso di questa Corte, di ritenere pacificamente sussistente, al di là di ogni ragionevole dubbio, l'una o l'altra delle due condotte (entrambe penalmente rilevanti) previste dal contestato art. 600 quater c.p., ovvero il "procurarsi" (che implica qualsiasi modalità di procacciamento, compresa la via telematica) e il "disporre" (che implica un concetto più ampio della detenzione) ciò in quanto, in relazione alla prima condotta, sussiste la concreta possibilità

CamminoDiritto.it
ISSN 2532-9871

di una modalità di acquisizione inconsapevole del materiale, via internet, senza alcun criterio selettivo e, in relazione alla seconda condotta, l'intervenuta cancellazione delle (poche) immagini di contenuto pedopornografico acquisite, costituisce indice della volontà dell'imputato non già di disporre di dette immagini bensì di disfarsi di files di contenuto non gradito».

La suesposta sentenza, crea indubbiamente molti interrogativi riguardo l'accertamento e l'acquisizione dei dati informatici nei casi di detenzione di materiale pedopornografico: se infatti rileva la quantità di immagini incriminate a fronte di quelle complessivamente acquisite, sarà necessario sequestrare tutto il materiale scaricato dall'utente, senza possibilità per gli investigatori di omettere l'acquisizione di immagini con contenuti palesemente non incriminanti.

Sempre con riferimento al reato di detenzione di materiale pedopornografico la Suprema Corte (**Cass. Pen. Sez. III 20 gennaio 2016 n. 12458**) affronta una controversa questione, ossia se la presenza in un computer di file temporanei di Internet con immagini pedopornografiche, salvati automaticamente nella cache durante la navigazione nel web, possa integrare il delitto previsto dall'art. 600 quater c.p.

La Suprema Corte accoglie le doglianze del ricorrente, cassando la sentenza impugnata e rinviando ad altra sezione della Corte di Appello per un nuovo giudizio, in quanto tali file non erano detenuti volontariamente, dal momento che essi vengono salvati in automatico dal computer in occasione della navigazione in Internet. Il ricorrente rilevava inoltre una evidente omissione degli inquirenti, i quali non avevano accertato se i file video a sfondo pedofilo scaricati dalla rete, fossero stati mai aperti e visionati Il ragionamento della Corte è palese: la semplice visione di immagini pedopornografiche, contenute in un sito Internet, non è sufficiente ad integrare il reato di cui all'art. 600 quater c.p.

L'orientamento della giurisprudenza di legittimità, non è tuttavia unanime al riguardo. Con s**entenza n. 24345 del 21 aprile 2015**, la Suprema Corte ha respinto il ricorso di un imputato, ritenendo sussistente il reato di cui all'art. 600 quater c.p., in quanto i file incriminati «venendo memorizzati per essere utilizzati in caso di accesso alle stesse pagine in momenti successivi, di fatto potevano essere, in qualsiasi momento, richiamati in visione dall'imputato».

Invero, per rispondere del reato di cui all'art. 600 quater c.p., è necessario agire con la precisa intenzione di procacciarsi il materiale pedopornografico. Presumere tale volontà dalla presenza nel computer di file che siano conseguenza di salvataggi automatici, costituisce indubbiamente una forzatura.

CamminoDiritto.it
ISSN 2532-9871

7. Sviluppi normativi.

Non vi è dubbio alcuno che le maggiori difficoltà dell'accertamento riguardino la natura stessa del dato informatico, non connotato dalla materialità. In materia di reati informatici le indagini non potranno, perciò, essere svolte secondo i tradizionali canoni acquisitivi, in quanto ogni errore o dimenticanza rischierebbe di compromettere la regolare acquisizione del dato, e di conseguenza anche l'esito dell'indagine ovvero l'utilizzo delle risultanze informatiche durante il processo.

A tal fine è necessario il riferimento a protocolli tecnici che prevedano regole base il cui rispetto è garanzia per la genuinità delle operazioni d'indagine, a tutela sia dell'indagato (o imputato) che dell'accusa. Linee guida e protocolli dovranno poi essere emanati con decreto ministeriale, ed aggiornati periodicamente, al fine di evitare un insieme di disposizioni prive di alcuna valenza giuridica, ovvero prive di alcun contatto con le reali necessità. Le evidenze e i dati acquisiti in violazione dei criteri stabiliti nei protocolli, dovranno necessariamente essere ritenuti inutilizzabili in ogni fase del procedimento, comprese le indagini preliminari. Ciò sta a significare che, su richiesta di parte ove il giudice per le indagini preliminari accerti la violazione dei protocolli da parte degli inquirenti, i dati non potranno essere inseriti neanche nel fascicolo del pubblico ministero. Dovrebbe inoltre essere chiarito con una norma di legge che evidenze informatiche acquisite in violazione dei criteri scientifici stabiliti dai protocolli o comunque in violazione delle regole del processo accusatorio, non potranno essere valutate liberamente dal giudice ex art. 192 c.p.p.

A tutela dei diritti di difesa di indagato ed imputato, ma anche del corretto esercizio dell'azione penale, è auspicabile una nuova normativa sui reati informatici che riconosca, una volta per tutte, il dato digitale così fragile e alterabile da essere considerata la sua acquisizione, nella totalità dei casi un atto irripetibile, con l'attribuzione di tutte le garanzie previste dall'art. 360 c.p.p. Gli esperti nel settore informatico sono infatti concordi nel ritenere ogni duplicazione del dato digitale, rischiosa per l'integrità dello stesso.

Anche sull'attività di intercettazione dovrebbe essere fatta chiarezza dal legislatore, con particolare riguardo alla non più attuale distinzione tra intercettazioni telefoniche e telematiche. I moderni strumenti di collegamento non consentono, oggi, la benché minima distinzione fra tecnologie telefoniche e telematiche, creando confusione in riferimento alla legislazione da applicare. Sarebbe quindi necessaria una legislazione unitaria per entrambe le tecnologie, che preveda sufficienti garanzie difensive ed escluda un'acquisizione indiscriminata dei dati.

CamminoDiritto.it
ISSN 2532-9871

Per un maggior rispetto della riservatezza, sarebbe inoltre opportuno prevedere "udienze di stralcio" tenute in camera di consiglio, per l'esclusione dagli atti del processo di dati non utili all'esercizio dell'azione penale o alla difesa dell'imputato.

[1] Molto discussa è la novella del 1993 che ha inserito il comma 3 bis all'art. 268 c.p.p., il quale prevede che: «quando si procede a intercettazioni di comunicazioni informatiche o telematiche il pubblico ministero può disporre che le operazioni siano compiute anche mediante impianti appartenenti a privati». L'art. 268 ha subìto ulteriori modifiche, anche a seguito di una sentenza della Corte costituzionale (sent. n. 336 del 10 ottobre 2008), che ne ha dichiarato l'illegittimità nella parte in cui non prevedeva che, dopo la disposizione di una misura cautelare personale, il difensore non potesse ottenere la trasposizione delle registrazioni di conversazioni o comunicazioni intercettate, anche non depositate, utilizzate per l'adozione del provvedimento cautelare. [2] Il c.d. freezing, ossia la conservazione dei dati, prevista dall'art. 16 della Convenzione di Budapest del 2001. Per l'articolo 16 della Convenzione (Conservazione rapida di dati informatici immagazzinati): «1. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle competenti autorità di ordinare o ottenere in altro modo la protezione rapida di specifici dati informatici, inclusi i dati sul traffico, che sono stati conservati attraverso un sistema informatico, in particolare quando vi è motivo di ritenere che i dati informatici siano particolarmente vulnerabili e soggetti a cancellazione o modificazione. 2. Quando una Parte rende effettive le previsioni di cui al precedente paragrafo 1 attraverso l'ordine ad un soggetto di conservare specifici dati informatici immagazzinati che siano in suo possesso o sotto il suo controllo, la Parte deve adottare le misure legislative e di altra natura che siano necessarie per obbligare tale soggetto a proteggere e mantenere l'integrità di quei dati informatici per il periodo di tempo necessario, per un massimo di novanta giorni, per consentire alle autorità competenti di ottenere la loro divulgazione. Una Parte può prevedere che tale ordine possa essere successivamente rinnovato. 3. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per obbligare il custode o la persona incaricata di conservare i dati informatici di mantenere il segreto sulla procedura intrapresa per il periodo di tempo previsto dal proprio diritto interno. 4. I poteri e le procedure di cui al presente articolo devono essere soggetti agli articoli 14 e 15». [3] Di diverso parere autorevole dottrina, fra cui G. Costabile secondo il quale canonizzare all'interno di norme giuridiche, procedure tecniche a livello informatico, più che rappresentare una garanzia avrebbe portato ad effetti distorsivi rappresentati dall'evoluzione costante della disciplina e dalle peculiarità proprie di ciascun caso. L'autore precisa, poi: «consiglierei di evitare troppi tecnicismi e precisazioni di sorta, definendo al massimo alcuni principi cardine sull'integrità dei dati, la ripetibilità degli accertamenti ed altro ancora, lasciando allo stato dell'arte la parte tecnica di esecuzione delle operazioni per raggiungere i citati obiettivi».

CamminoDiritto.it
ISSN 2532-9871

Soltanto parzialmente condivisibili risultano, a parere dello scrivente, le precisazioni dell'autore. Quando si parla di procedimento penale e di diritti dell'indagato o imputato, e nello specifico di accertamenti che potrebbero incidere sulla libertà della persona, non può essere lasciata «allo stato dell'arte la parte tecnica di esecuzione delle operazioni». Essa deve, anzi, essere nei limiti del possibile confinata entro margini precisi, fissati in minima parte dalla legge, ma nella parte più consistente da protocolli standardizzati a livello ministeriale e altri atti di soft law. [4] Caso "Vierika", Trib. di Bologna, sent. di primo grado. Afferma il giudice che: «quando anche il metodo utilizzato dalla p.g. non dovesse ritenersi conforme alla migliore pratica scientifica, in difetto di prova di una alterazione concreta, conduce a risultati che sono, per il principio di cui all'art. 192 c.p.p., liberamente valutabili dal giudice alla luce del contesto probatorio complessivo». [5] Su questa linea di pensiero anche D'Aiuto G., Levita L. su "I reati informatici – Disciplina sostanziale e questioni processuali", Giuffrè Editore. [6] L'art. 111 Cost., nella sua nuova formulazione con legge di revisione costituzionale n. 2 del 1999, stabilisce che: «La giurisdizione si attua mediante il giusto processo regolato dalla legge. Ogni processo si svolge nel contraddittorio tra le parti, in condizioni di parità, davanti a giudice terzo e imparziale. [...] Il processo penale è regolato dal principio del contraddittorio nella formazione della prova. [...] La legge regola i casi in cui la formazione della prova non ha luogo in contraddittorio per consenso dell'imputato o per accertata impossibilità di natura oggettiva o per effetto di provata condotta illecita». [7] La chain of custody del sistema statunitense. Essa si riferisce alla documentazione cronologica delle procedure e delle attività di sequestro, repertamento, custodia, controllo, analisi dei dati. E' determinante per la corretta acquisizione di elementi di prova in dibattimento e per la genuinità delle analisi stesse. [8] Cassazione Penale sez. III, sentenza n. 1935 del 30/07/1994: «Trattasi di attività di accertamento e rilevazione che spetta alla polizia giudiziaria organizzare secondo ragionevoli modalità, considerate le condizioni di tempo e di luogo e la natura delle indagini in corso. Se il Pubblico Ministero non può intervenire tempestivamente, la polizia giudiziaria non è affatto obbligata a disporre subito il sequestro, ma come bene indica l'art. 354, secondo comma c.p.p. può provvedere solo "se del caso" ed intanto rientra nella sua facoltà tenere sul posto le cose oggetto dell'accertamento, informandone il P.M». [9] Cass. Pen. sent. n. 7967, nella quale i giudici stabiliscono che all'atto urgente e indifferibile compiuto dalla polizia giudiziaria «il difensore può assistere senza diritto di essere previamente avvisato, dovendo la polizia giudiziaria unicamente avvertire la persona sottoposta alle indagini della facoltà di farsi assistere da un difensore di fiducia». [10] Fra cui L. Lupària, La ratifica della Convenzione Cybercrime del Consiglio d'Europa, in Diritto Penale e Processo; G. Costabile, Aspetti giuridici comuni delle indagini informatiche. [11] Cause riunite C-293/12 e C-594/12, Digital Rights Ireland. [12] D'Aiuto G., Levita L. - I reati informatici – Disciplina sostanziale e questioni processuali, – Giuffrè Editore, 2012. [13] Molti i casi di denunce in tal senso. Nel caso dei fratelli Occhionero, più volte i difensori hanno denunciato una eccessiva insistenza degli inquirenti nel cercare di convincere gli indagati a fornire loro le credenziali di accesso. Non si può non concordare con l'affermazione del difensore avv. Bottacchiari secondo

CamminoDiritto.it
ISSN 2532-9871

cui: «i computer devono essere analizzati nel rispetto di tutte le regole del contraddittorio, in base alla metodica forense che preserva dal rischio di contaminazione e cancellazione dei dati», e con specifico riferimento a Francesca Occhionero: «in maniera insistente, con fortissima pressione, le chiedevano la password di accesso». [14] Tribunale del Riesame di Venezia, ordinanza 6 ottobre 2000.

Bibliografia - D'Aiuto G., Levita L. – I reati informatici – Disciplina sostanziale e questioni processuali, Giuffrè Editore, 2012. - Garuti G. - Modelli differenziati di accertamento – vol. VII – Trattato di procedura penale – diretto da G. Spangher, UTET Giuridica. - Luparia L., Ziccardi G. - Investigazione penale e tecnologia informatica - L'accertamento del reato tra progresso scientifico e garanzie fondamentali, Giuffrè Editore. - Dalia A. A. – Ferrajoli M. - Manuale di diritto processuale penale – IX edizione - CEDAM, 2016. - AA.VV. – Gli accertamenti informatici nelle investigazioni penali: una prospettiva europea – a cura di F. Cajani e G. Costabile, Experta. - Convention on cybercrime - Budapest, 23/11/2001 - Piccinni M.L., Vaciago G. - Computer Crimes - Casi pratici e metodologie investigative dei reati informatici - Moretti Vitali Editori.