UNIVERSITÀ DEGLI STUDI DI ROMA TRE

FACOLTÀ DI GIURISPRUDENZA

SCUOLA DOTTORALE INTERNAZIONALE
"TULLIO ASCARELLI"

Sezione "Sistemi punitivi e garanzie costituzionali"

– XXVII° ciclo –

TESI DI DOTTORATO

LE INDAGINI INFORMATICHE NEL PROCESSO PENALE

TUTOR
CHIAR.MO PROF. LUCA MARAFIOTI

COORDINATORE
CHIAR.MO PROF. MARIO TRAPANI

DOTTORANDO
DOTT. MARCO PITTIRUTI

INDICE

CAPITOLO I
I SOGGETTI DELL'INDAGINE PRELIMINARE INFORMATICA

1. Nuove tipologie probatorie e processo scientifico……**5**
2. Le attribuzioni del pubblico ministero e la competenza del giudice in tema di indagini digitali……**12**
3. Il ruolo della polizia giudiziaria: presupposti e limiti dell'attività *undercover* in ambiente digitale……...**19**
4. Poteri dell'accusa e facoltà della difesa nelle indagini informatiche a confronto. Il ruolo del consulente tecnico……....**30**

CAPITOLO II
I MEZZI DI RICERCA DELLA PROVA DIGITALE

1. I principi-guida nella ricerca della *digital evidence*: genuinità e non alterazione del dato informatico……...**37**
2. Perquisizioni ed ispezioni informatiche tra norme processuali "in bianco" e prassi……**40**
3. Forme e modalità del sequestro di dati digitali: il vincolo pertinenziale....**47**
4. L'apprensione di dati in tempo reale: intercettazioni telematiche e perquisizioni *online* ……..**62**

CAPITOLO III
L'ANALISI TECNICO-SCIENTIFICA DEL DATO INFORMATICO. INTEGRITÀ E CONTINUITÀ PROBATORIA

1. L'indagine informatica urgente: la *live analysis*……...**79**
2. *Computer forensics* e ripetibilità delle operazioni acquisitive: una questione aperta……**86**

3. Esibizione, custodia e conservazione dei dati digitali: un riconoscimento legislativo della funzione di *hash*?.....**94**

CAPITOLO IV

LE INDAGINI INFORMATICHE TRA ESIGENZE DI ACCERTAMENTO E DIRITTI FONDAMENTALI

1. La disciplina in tema di conservazione di dati informatici da parte del *service provider*……....**99**

2. Il difficile bilanciamento tra diritto alla riservatezza ed utilità investigativa alla luce della sentenza 8 aprile 2014 della Corte di Giustizia Europea.....**105**

3. La prova digitale "incostituzionale"……...**109**

4. Violazione degli *standard* metodologici propri della *computer forensics* ed invalidità…….**112**

BIBLIOGRAFIA……...…**119**

Capitolo I – I soggetti dell'indagine preliminare informatica

1. Nuove tipologie probatorie e progresso scientifico

La scienza trova, da sempre, applicazione nel processo penale in funzione di ausilio per l'accertamento di fatti di reato. Basti pensare al rilievo assunto nell'attuale sistema processuale dallo sviluppo delle biotecnologie e della medicina legale.

Da tali ambiti scientifici si attinge per creare nuovi strumenti investigativi e nuove tipologie di prova[1]. Ma nessun settore appare in grado di fornire tanti elementi utili al processo penale quanto quello informatico e telematico.

Ed invero, il crescente utilizzo, nell'era moderna, di strumentazione informatica e telematica per la trasmissione, ricezione ed elaborazione delle informazioni ha comportato che, mediante tali apparati, si veicoli quotidianamente una mole enorme di dati, molti dei quali di sicuro interesse ai fini processuali. È sorta, dunque, l'esigenza, per gli organi investigativi, di ricercare elementi di prova tra i dati contenuti in sistemi informatici o telematici[2].

Non solo. Di pari passo con l'evoluzione della scienza, anche le investigazioni informatiche hanno subìto una trasformazione costante. Alle prime, pionieristiche indagini aventi ad oggetto *floppy disk* si sono, in seguito, sostituite attività sempre più complesse, che reclamano competenze tecniche specifiche e

---

[1] Cfr., in proposito, *ex multis*, O. DOMINIONI, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Giuffrè, Milano, 2005, *passim* e, in particolare, pp. 11-14 e 37-42; P. TONINI, *La prova scientifica: considerazioni introduttive*, in *Dir. pen. proc.*, 2008, *Dossier prova scientifica*, p. 7 ss.; P. FERRUA, *Metodo scientifico e processo penale*, *ibidem*, p. 12 ss.; S. LORUSSO, *Investigazioni scientifiche, verità processuale ed etica degli esperti*, in *Dir. pen. proc.*, 2010, p. 1345 ss. Più in generale, sull'ingresso della scienza nelle attività investigative, cfr. A. CHELO, *Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria*, CEDAM, Padova, 2014, p. 9.

[2] Una panoramica della tematica è offerta da L. LUPARIA, *La disciplina processuale e le garanzie difensive*, in L. LUPARIA-G. ZICCARDI, *Investigazione penale e tecnologia informatica*, Giuffrè, Milano, 2007, p. 127 ss.

sofisticate, fino alle recentissime ipotesi di analisi dei dati contenuti in un sistema di *cloud computing*[3].

Simili mutamenti nelle tecniche d'indagine sono, in parte, frutto dell'utilizzo della tecnologia informatica a scopi criminali. In altre parole, le indagini informatiche hanno rappresentato la risposta dello Stato alle difficoltà di accertamento sorte in relazione a reati perpetrati mediante l'utilizzo di sistemi informatici o telematici.

Sarebbe, però, del tutto miope circoscrivere l'ambito delle indagini informatiche[4] al solo accertamento dei *computer crimes*[5]. A ben vedere, l'espansione incontrollata della *Information and Comunication Technology*[6] – si pensi all'impiego diffuso di *social network* e *smartphone* – impone, oramai, l'acquisizione, l'analisi e la gestione di dati informatici nella stragrande maggioranza delle indagini in ambito penale. Elementi utili alle indagini per qualsiasi tipo di reato, conservati in formato digitale, si ritrovano in numerosi strumenti di utilizzo quotidiano, dal *personal computer* al *server* aziendale, dalla memoria di un lettore di *file* musicali ad una *pen-drive*. Tutti strumenti notevolmente diversi l'uno dall'altro, quanto a modalità di accesso e di recupero del loro contenuto.

In quest'ottica, è bene segnalare fin d'ora l'impossibilità di individuare un preciso *iter* delle indagini informatiche. La scansione e la fisionomia dell'attività

---

[3] Per un'analisi dei profili giuridici della "nuvola informatica" v. G.M. RUOTOLO, Hey! You! Get Off My Cloud! *Accesso autoritativo alle nuvole informatiche e diritto internazionale*, in *Arch. pen.*, 2013, p. 853; D. LA MUSCATELLA, *La ricerca delle fonti di prova sulle reti di* cloud computing*: le nuove frontiere delle investigazioni digitali tra profili giuridici e questioni operative*, in *Cib. dir.*, 2013, p. 477 ss.; nonché R.B. WELLS, *The Fog of Cloud Computing: Fourth Amendment Issues Raised by the Blurring of Online and Offline Content*, in *12 U. Pa. J. Const. L.*, 2014, p. 223 ss.

[4] Una definizione di indagine informatica è offerta da P. GUALTIERI, *Prova informatica e diritto di difesa*, in *Dir. pen. proc.*, 2008, *Dossier prova scientifica*, p. 70: «l'indagine può definirsi informatica, sia quando è diretta all'identificazione dell'autore di crimini informatici (cioè principalmente quelli previsti dalla l. 23 dicembre 1993, n. 547), sia se si utilizzano tecnologie informatiche e telematiche nello svolgimento delle investigazioni sui reati comuni».

[5] V., sul punto, F. RUGGIERI, *Profili processuali nelle investigazioni informatiche*, in L. PICOTTI, *Il diritto penale dell'informatica nell'epoca di* Internet, Cedam, Padova, 2004, p. 155, nota 3. Secondo l'Autrice, l'erroneità della ritenuta equivalenza tra indagini informatiche ed accertamento dei *computer crimes* trova conferma nel dato letterale dell'art. 266-*bis* c.p.p., relativo alle intercettazioni di comunicazioni informatiche e telematiche. Invero, tale disposizione estende l'impiego dell'istituto in parola a tutti i «reati commessi con l'impiego di tecnologie informatiche o telematiche» e, dunque, ben oltre l'accertamento dei soli "reati informatici". Al riguardo, cfr. anche R. ORLANDI, *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc.*, 2009, p. 129.

[6] Cfr., in proposito, D. CURTOTTI, *Le ragioni di un confronto di idee*, in *Arch. pen.*, 2013, p. 765.

investigativa risulta, piuttosto, improntata ad un criterio di utilità: gli strumenti in mano agli inquirenti sono calibrati in base al reato da accertare e a seconda dell'elemento di prova (digitale[7]) da reperire.

Seppure le indagini informatiche presentino carattere multiforme, può, nondimeno, identificarsi un'attività che contraddistingue la pressoché totalità degli accertamenti in materia di *computer crimes*: vale a dire, l'acquisizione con decreto motivato del pubblico ministero, ai sensi dell'art. 132, comma 3, D. Lgs. 196/2003, presso l'*Internet Service Provider*, dati relativi al traffico telematico necessari ad una possibile identificazione dell'autore delle condotte per cui si procede[8]. L'importanza di simile collaborazione appare lampante non appena si consideri che, seppure l'identificazione attraverso indirizzo *Internet Protocol*[9] non possa essere elevata a dato certo, una inottemperanza da parte del *provider* di servizi all'ordine del pubblico ministero potrebbe – in determinati casi *sine die* – paralizzare l'attività di quest'ultimo.

Com'è agevole avvertire, la collaborazione[10] di un soggetto terzo rispetto al procedimento penale, e precisamente il gestore dei servizi telematici, per

---

[7] Sottolinea la natura "digitale" di tali prove, giacché «originate da una manipolazione elettronica di numeri» M. DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, p. 283, mentre G. COSTABILE, Scena criminis*, documento informatico e formazione della prova penale*, in *Dir. inf.*, 2005, p. 531 ss., le colloca «in una sorta di "metaterritorio", dove sembrerebbe perdere consistenza la naturale propensione dell'uomo di rapportarsi al mondo "reale" con l'uso dei cinque sensi». Una definizione compiuta di *digital evidence* è offerta da L. MARAFIOTI, *Digital evidence* e processo penale, in *Cass. pen.*, 2011, p. 4509, il quale vi include «ogni informazione probatoria la cui rilevanza processuale dipende dal contenuto del dato o dalla particolare allocazione su di una determinata periferica, oppure dal fatto di essere stata trasmessa secondo modalità informatiche o telematiche».

[8] V. *infra*, cap. 4, par. 1.

[9] Si tratta di una stringa numerica che identifica un dispositivo collegato alla rete *internet* in un determinato momento. La Corte di Cassazione ha, di recente, avallato l'impostazione della giurisprudenza di merito secondo cui l'*Internet Protocol Address* corrisponderebbe ad «una impronta digitale informatica» (Cass., Sez. III, 23 gennaio 2014, n. 3110, *inedita*). Non di rado si rinvengono, nei *dictum* dei giudici di merito, affermazioni del tipo: «la riferibilità delle condotte all'A. non è […] discutibile. L'imputato era identificato attraverso l'indirizzo *IP* rivelato e registrato al momento delle connessioni» (così Uff. indagini preliminari Napoli, sent. 24 luglio 2014, A.C., *inedita*).

[10] Sul peculiare ruolo assunto dal fornitore di connettività nel procedimento penale, «"custode" di elementi probatori utili, talvolta essenziali, all'accertamento; […] ausiliario degli organi inquirenti, delegato al compimento di ruoli *lato sensu* investigativi», v. L. LUPARIA, *Il sistema penale ai tempi dell'*internet. *La figura del* provider *tra diritto e processo*, in ID. (a cura di), Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Giuffrè, Milano, 2012, p. 1 ss., ed in particolare pp. 2-3.

l'identificazione del soggetto autore di una condotta criminosa *online* rappresenta un carattere innovativo della tematica in parola[11].

Un'altra caratteristica comune delle indagini informatiche concerne la natura immateriale del dato trattato dagli inquirenti. Gli elementi ricercati dagli organi investigativi consistono in «*zeroes and ones of electricity*»[12]. L'impalpabilità del dato conferisce i caratteri di volatilità, immaterialità e fragilità alla fonte digitale[13]. Ad esempio, un *file* comune, quale una immagine in formato *jpg*, comprende circa un milione di *bit*[14]; la modifica di uno solo di essi può comportare una modifica irreversibile, tanto che il *file* potrà apparire illeggibile o corrotto. Perché il dato sia alterato, è sufficiente che venga aperto una sola volta: quantomeno, infatti, sarà stato modificato il metadato relativo alla data di ultimo accesso, con il rischio che ne venga annullata ogni rilevanza probatoria.

Com'è agevole intuire, dunque, l'esigenza di tutelare la genuinità della prova – ineludibile per l'intero sistema processuale – si ripropone, nella fattispecie, con rinnovato vigore.

---

[11] È opportuno segnalare che recentissimi interventi legislativi hanno assegnato ulteriori, particolari compiti ausiliari al pubblico ministero agli *Internet service provider*. Il riferimento è al D.L. 18 febbraio 2015, n. 7, *Misure urgenti per il contrasto al terrorismo, anche di matrice internazionale, nonché proroga delle missioni internazionali delle Forze armate e di Polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e stabilizzazione*, pubblicato in *G.U.*, 19 febbraio 2015, n. 41. In particolare, ai sensi dell'art. 3, «i fornitori di connettività, su richiesta dell'autorità giudiziaria procedente, inibiscono l'accesso ai siti [utilizzati per le attività e le condotte di cui agli articoli 270-*bis* e 270-*sexies* del codice penale], secondo le modalità, i tempi e le soluzioni tecniche individuate e definite con il decreto previsto dall'articolo 14-*quater*, comma 1, della legge 3 agosto 1998, n. 269». Ai sensi dell'art. 4, poi, «quando si procede per i delitti di cui agli articoli 270-*bis*, 270-*ter*, 270-*quater* e 270-*quinquies* del codice penale commessi con le finalità di terrorismo di cui all'articolo 270-*sexies* del codice penale, e sussistono concreti elementi che consentano di ritenere che alcuno compia dette attività per via telematica, il pubblico ministero ordina, con decreto motivato, ai fornitori di servizi di cui all'articolo 16 del decreto legislativo 9 aprile 2003, n. 70, ovvero ai soggetti che comunque forniscono servizi di immissione e gestione, attraverso i quali il contenuto relativo alle medesime attività è reso accessibile al pubblico, di provvedere alla rimozione dello stesso. I destinatari adempiono all'ordine immediatamente e comunque non oltre quarantotto ore dal ricevimento della notifica. In caso di mancato adempimento, si dispone l'interdizione dell'accesso al dominio *internet* nelle forme e con le modalità di cui all'articolo 321 del codice di procedura penale».

[12] L'espressione è di O. KERR, *Digital Evidence and the New Criminal Procedure*, in *105 Colum. L. Rev.*, 2005, p. 291.

[13] Cfr. E. CASEY, *Error, Uncertainty, and Loss in Digital Evidence*, in *Int. J. Dig. Evidence*, 2002, p. 1 ss.

[14] V. S. ATERNO, *Acqusizione e analisi della prova informatica*, in *Dir. pen. proc.*, 2008, *Dossier prova scientifica*, p. 62. Un *bit* corrisponde alla quantità di informazione che otteniamo ricevendo la risposta ad una domanda binaria (ossia che ammette solo le due risposte "sì" o "no"). Con un *bit*, quindi, possiamo rappresentare solo uno tra due possibili valori (ad es. vero/falso); con *n* bit possiamo rappresentare 2n valori differenti. Una sequenza di 8 *bit* corrisponde a un *byte*. Cfr. anche G. PIERRO, *Introduzione allo studio dei mezzi di ricerca della prova informatica*, in *Dir. pen. proc.*, 2011, p. 1516.

Il quadro sin qui messo a punto basta a chiarire che la *digital evidence* può essere danneggiata – sia pure inconsapevolmente – da personale non in possesso delle conoscenze tecniche adeguate.

È possibile tracciare, sul punto, un parallelo con la *scientific evidence*, di cui la prova informatica rappresenta appunto «un sottotipo di recente emersione, a causa dell'alto grado di tecnicismo richiesto per trasformare le informazioni originariamente contenute in macchinari alquanto complessi in dati intellegibili da un giudice»[15]. In quest'ottica, è agevole notare come anche con riferimento alla prova informatica si ripropongano questioni già affrontate in relazione al rapporto tra processo e *novel science*, con particolare riguardo alla capacità dimostrativa della prova scientifica, all'attendibilità dell'esperto e al rischio di una sopravvalutazione del contributo cognitivo offerto da quest'ultimo[16], nonché alla collocazione della prova nell'ambito del sistema codicistico.

Con riguardo a quest'ultimo aspetto, non sono mancate, anche in tempi recenti, decisioni orientate a ricondurre qualsiasi documento informatico all'istituto di cui all'art. 234 c.p.p.[17]. Ciò, nonostante tale ultima disposizione sia stata «pensat[a] per strumenti analogici, la cui peculiarità è data da grandezze fisiche che assumono valori continui»[18].

Una definizione specifica del documento informatico era presente, fino alla sua eliminazione ad opera della L. 48/2008[19], in attuazione della Convenzione di Budapest sulla Criminalità informatica, nell'art. 491-*bis* c.p., ove lo si identificava in «qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli». Tale enunciazione, però, come avvertito dai più attenti commentatori, confondeva contenitore (in ipotesi, un *personal computer*) e contenuto (il *file* oggetto di attenzione

---

[15] Così L. MARAFIOTI, Digital evidence *e processo penale*, cit., p. 4510.

[16] Cfr. A.E. RICCI, Digital evidence*, sapere tecnico-scientifico e verità giudiziale*, in C. CONTI (a cura di), *Scienza e processo penale. Nuove frontiere e vecchi pregiudizi*, Giuffrè, Milano, 2011, p. 342.

[17] Si veda, per tutte, Cass., Sez. III, 27 settembre 2012, n. 37419, in *C.E.D. Cass.*, rv. 253573, secondo cui «i dati contenuti nel *computer* […] costituiscono prova documentale ai sensi dell'art. 234 c.p.p., comma 1, trattandosi della rappresentazione di cose, termine cui deve attribuirsi la più ampia estensione, effettuata mediante mezzi diversi da quelli tradizionali […]».

[18] In questi termini F. ZACCHÈ, *La prova documentale*, Giuffrè, Milano, 2012, p. 26.

[19] Legge 18 marzo 2008, n. 48, *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*, pubblicata in *G.U.*, 4 aprile 2008, n. 80.

investigativa), finendo, così, per pretermettere qualsiasi tutela proprio relativamente al dato evidentemente più a rischio di contaminazione[20].

Più preciso, al riguardo, è l'art. 1 della Convenzione di Budapest, cui l'art. 2 della L. 48/2008 ha dato piena ed intera esecuzione[21], che identifica il dato informatico in «qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione»[22].

Eppure, ulteriore incertezza deriva dalla circostanza che una diversa formula, dai confini più ampi, è rinvenibile nell'art. 1, lett. *p*), del codice dell'amministrazione digitale, ai sensi del quale costituisce un documento informatico ogni «rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti»[23].

Il discorso può muovere dalle conclusioni cui è giunta una parte della dottrina[24], secondo cui occorre distinguere tra il tradizionale metodo di incorporamento analogico, in cui non esiste rappresentazione senza il documento, ed incorporamento digitale, la cui precipua caratteristica è rappresentata dall'immaterialità e, quindi, dall'indipendenza dal supporto. Corollario del ragionamento è la necessità di una maggior tutela, in caso di incorporamento digitale, da eventuali possibilità di falsificazione e/o distruzione del documento.

Tali rilievi sono confermati da molteplici indici di diritto positivo, giacché la L. 48/2008, inserendo nell'apparato regole codicistiche *ad hoc* per l'indagine

---

[20] Cfr. P. TONINI, *Documento informatico e giusto processo*, in *Dir. pen. proc.*, 2009, p. 401 ss., nonché M. DANIELE, *La prova digitale nel processo penale*, cit., p. 284, secondo cui la confusione legislativa si deve all'immaterialità del dato digitale.

[21] La definizione dell'art. 1 deve, dunque, ritenersi vigente anche nel nostro ordinamento, nonostante non sia stata esplicitamente recepita.

[22] Il testo riportato – qui e nel prosieguo dell'opera – è quello presentato all'interno del Disegno di legge del Governo (Atto Camera 2807), in *Guida dir.*, 2008, n. 16, p. 34.

[23] È opportuno segnalare che l'art. 20, comma 1-*bis*, codice dell'amministrazione digitale affronta il problema del valore probatorio del documento informatico. Quest'ultimo è liberamente valutabile in giudizio, «tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità». Stante il riferimento all'idoneità del documento informatico a soddisfare il requisito della prova scritta contenuto nella medesima disposizione, è legittimo il dubbio che la norma si presti ad un utilizzo esclusivo nell'ambito del processo civile ed amministrativo, e non in quello penale.

[24] V., per tutti, P. TONINI, *Documento informatico e giusto processo*, cit., p. 403 ss.

informatica, ha concentrato l'attenzione proprio sulla necessità di «assicurare la conservazione dei dati originali e ad impedirne l'alterazione»[25].

Se così è, deve recisamente escludersi che qualsiasi dato digitale, una volta incorporato in un supporto cartaceo, costituisca prova documentale ai sensi dell'art. 234 c.p.p. Difatti, simile espediente si risolve in una mera scorciatoia probatoria volta ad elidere il doveroso controllo sull'autenticità delle informazioni contenute nel documento stesso[26].

In alternativa all'inquadramento della prova informatica nell'istituto di cui all'art. 234 c.p.p., si era sostenuta la riconducibilità *tout court* della *digital evidence* alla disciplina di cui all'art. 189 c.p.p.

Tuttavia, invocare il contenitore della prova atipica quale *sedes materiae* della prova informatica appare anacronistico a seguito delle modifiche operate dalla L. 48/2008, giacché numerosi istituti, già presenti nel codice di rito, sono stati rimodellati al fine di essere adattati alle problematiche attinenti la fonte di prova informatica.

A dire il vero, già anteriormente alla riforma si era dubitato che il contenitore della prova atipica fosse idoneo a ricomprendere ogni ipotesi di *scientific evidence*[27], sul presupposto che quest'ultima spesso non integra tanto una prova non

---

[25] Così gli artt. 244, comma 2, 247, comma 1-*bis*, 352, comma 1-*bis*, 354, comma 2, c.p.p., nonché, con formule analoghe, gli artt. 254, comma 2, 254-*bis*, 259, comma 2, 260, comma 2, c.p.p. Sulla «nuova sensibilità» del legislatore circa le attività investigative da compiere sul dato informatico, cfr. A. CHELO, *Le prime indagini sulla scena del crimine*, cit., p. 63. Per un'analisi approfondita delle nuove disposizioni, v. *infra*, cap. 2.

[26] In tema, la sentenza del Tribunale di Pescara, 6 ottobre 2006, in *Dir. internet*, 2007, p. 271 ss., presenta profili di interesse. In tale procedimento, in fase di indagine, la polizia giudiziaria aveva stampato alcuni documenti informatici (pagine *web*), senza, tuttavia, adottare alcuna precauzione idonea a garantirne autenticità e provenienza. Il tribunale censurò, all'esito del dibattimento, l'operato della polizia giudiziaria e, in particolare, la circostanza che i documenti informatici non fossero stati acquisiti in copia certificata con sottoscrizione mediante firma digitale. Seppure la sentenza sia apprezzabile per l'attenzione rivolta alla tematica della genuinità del dato digitale, non pare convincente il rimando a regole tecniche adottate da organismi amministrativi, vale a dire la normativa tecnica relativa alla sottoscrizione con firma digitale emanata, già all'epoca, dall'Authority per l'informatica nella P.A. In effetti, il precedente è rimasto isolato e non si registrano decisioni in senso analogo. Cfr. E. APRILE, *Sull'utilizzabilità processuale della riproduzione a stampa di documenti informatici effettuata nel corso di una operazione di polizia giudiziaria*, in *Dir. internet*, 2007, p. 272 ss.

[27] Cfr., sia pure in più ampia prospettiva, F. CAPRIOLI, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cass. pen.*, 2008, p. 3520 ss.

disciplinata dalla legge, quanto, piuttosto, una diversa forma di manifestazione di istituti codicistici già a lungo sperimentati[28].

Così stando le cose, si tratta allora di verificare se – ed entro quali limiti – i tradizionali istituti in tema di prova, anche a seguito delle recenti modifiche, siano effettivamente compatibili con le nuove tipologie probatorie frutto del progresso scientifico; ciò, in particolare, in quella delicata fase in cui, nella maggior parte dei casi, la prova informatica viene a formarsi, vale a dire le indagini preliminari.

2. Le attribuzioni del pubblico ministero e la competenza del giudice in tema di indagini digitali

Dalla analisi d'insieme che precede del complesso *genus* delle indagini informatiche è emerso un carattere tipico di queste ultime: vale a dire, il concreto rimodularsi delle tecniche investigative a seconda delle modalità di offesa del bene tutelato dalla fattispecie criminosa. Proprio tale connotato, unitamente alla fragilità dei dati informatici trattati, implica che gli organi inquirenti interessati all'apprensione di tali elementi debbano possedere una elevata preparazione tecnico-specialistica al fine di scegliere correttamente la tecnica investigativa più idonea al caso di specie, affinché le indagini risultino efficaci[29].

Per perseguire l'obiettivo dell'efficienza investigativa, il legislatore[30], relativamente a reati di pedopornografia *online*[31], ha accentrato le funzioni di

---

[28] In questo senso v. L. MARAFIOTI, Digital evidence *e processo penale*, in *Cass. pen.*, 2011, p. 4511. Deve, comunque, precisarsi che l'istituto di cui all'art. 189 c.p.p. conserva, quantomeno nella prassi, un ambito applicativo con riguardo al dato digitale, come avviene con riguardo a quelle ipotesi di indagini parametriche informatiche considerate mezzo di ricerca della prova atipico dalla Corte di Cassazione.

[29] Secondo la Relazione di accompagnamento al Disegno di legge C 2807, reperibile in *www.camera.it*, poi approvato con la L. 48/2008, la modifica all'art. 51 c.p.p. si giustifica «al fine di facilitare il coordinamento delle indagini e la formazione di gruppi di lavoro specializzati in materia».

[30] D. MANZIONE, *L. 18.3.2008 N. 48 (Criminalità informatica) – Art. 11 – Competenza*, in *Legisl. pen.*, 2008, p. 314, sottolinea che la concentrazione in parola è un'idea del legislatore italiano non imposta dalle regole pattizie. A ben vedere, infatti, l'art. 22 della Convenzione di Budapest, rubricato "Competenza", attiene al diverso problema della giurisdizione.

[31] Segnatamente, l'attribuzione delle indagini alla procura distrettuale avviene nelle ipotesi di cui agli artt. 414-*bis*, 600-*bis*, 600-*ter*, 600-*quater*, 600-*quater*.1, 600-*quinquies*, 609-*undecies*, 615-*ter*, 615-*quater*, 615-*quinquies*, 617-*bis*, 617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 635-*bis*, 635-*ter*, 635-*quater*, 640-*ter*, 640-*quinquies* c.p. Segnala l'esclusione delle fattispecie di cui agli artt. 495-*bis* e 635-*quinquies*, nonché dei falsi informatici, M. GUERNELLI, *La legge di ratifica dela Convenzione sul* Cybercrime*: considerazioni sostanziali e processuali*, in *Riv. trim. dir. pen. ec.*, 2008, p. 768. Per D. MANZIONE, *op. cit.*, pp. 315-316, la

pubblico ministero presso il Tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente (art. 51, comma 3-*quinquies*, c.p.p.)[32].

Tale criterio attributivo[33], che assegna una peculiare categoria di indagini informatiche alla procura distrettuale, riecheggia l'accentramento delle funzioni della pubblica accusa già previsto per reati di particolare allarme sociale come quelli associativi. Tuttavia, la normativa non si giustifica già in virtù di una pretesa unitarietà del fenomeno criminoso da contrastare, come accade per i reati associativi, quanto, appunto, per la necessità di formare gruppi di lavoro specializzati[34].

Già tale ultima annotazione offre motivo di riflessione. Difatti, anche gli appartenenti alle procure non distrettuali sembrerebbero meritevoli di analogo "aggiornamento" tecnico in vista del compimento di indagini in ambito informatico[35].

La norma in parola ha suscitato, però, ben più numerose e penetranti critiche. In primo luogo, si rimproverava la scelta legislativa di concentrare l'attenzione unicamente sui *computer crimes*, a fronte di un fenomeno – l'attività investigativa in ambiente digitale – ormai di necessaria applicazione per l'accertamento di ogni genere di reati[36].

---

disciplina presenta profili di irragionevolezza, stante la diversità di disciplina non giustificata da un comune denominatore fra le fattispecie contemplate.

[32] Un esaustivo commento della normativa è offerto da F. CASSIBBA, *L'ampliamento delle attribuzioni del pubblico ministero distrettuale*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, Giuffrè, Milano, 2009, p. 113 ss.

[33] Sottolinea la terminologia erronea ("Competenza") della rubrica dell'art. 11 della L. 48/08, modificativo dell'art. 51 c.p.p., M.L. DI BITONTO, *La ratifica della Convenzione del Consiglio d'Europa sul* cybercrime*: profili processuali*, in *Dir. internet*, 2008, p. 505.

[34] Cfr. M.L. DI BITONTO, *op. cit.*, p. 508, nonché, in ottica critica, L. LUPARIA, *I correttivi alle distorsioni sistematiche contenute nella recente legge di ratifica della Convenzione sul* Cybercrime, in S. LORUSSO (a cura di), *Le nuove norme sulla sicurezza pubblica*, Cedam, Padova, 2008, pp. 66-67. H. BELLUTA, Cybercrime *e responsabilità degli enti*, in in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, p. 99, sostiene che «all'aterritorialità della maggior parte dei reati informatici si sia voluto far fronte attraverso la predisposizione di una risposta investigativa altrettanto sganciata dal territorio in senso fisico: quel che più conta […] è da un lato il possedere le competenze tecniche idonee a fronteggiare una "realtà virtuale" in costante e assai celere evoluzione […], dall'altro l'aver modo di attuare le dovute indagini grazie alla disponibilità di adeguate apparecchiature tecniche».

[35] F. CASSIBBA, *L'ampliamento delle attribuzioni del pubblico ministero distrettuale*, cit., p. 126, ritiene «indimostrato che le indagini preliminari concernenti ipotesi di sfruttamento sessuale dei minori richiedano un tasso di specializzazione informatica tale da imporre, addirittura, la centralizzazione delle investigazioni». In quest'ottica, a spingere il legislatore, più che un'effettiva esigenza investigativa, sarebbe stata «la spinta "emozionale" impressa dai *mass media*».

[36] V. L. LUPARIA, *I correttivi alle distorsioni sistematiche contenute nella recente legge di ratifica della Convenzione sul* Cybercrime, cit., p. 66.

In secondo luogo, si lamentava l'illogicità del sistema, poiché mancava un corrispondente accentramento della competenza per le indagini sui *computer crimes* in capo al giudice per le indagini preliminari e al giudice dell'udienza preliminare[37].

Infine, si evidenziavano le ripercussioni negative della disciplina sul corretto funzionamento delle procure distrettuali. Inevitabile conseguenza di qualsiasi forma di accentramento investigativo è, infatti, l'esponenziale aumento del numero di notizie di reato veicolate presso di esse[38]. La conseguente impossibilità di occuparsi compiutamente della totalità di queste ultime e, dunque, la necessaria formulazione di criteri di trattazione prioritaria delle *notitiae criminis* all'interno dei singoli uffici pareva ulteriormente scalfire l'obbligatorietà dell'azione penale[39].

Nel tentativo di rimediare alle accennate «dissimmetrie sistematiche»[40], il D.L. 92/2008[41], convertito con la L. 125/2008[42], da un lato, consente che le funzioni di pubblico ministero nel dibattimento siano esercitate, anche nei casi previsti dall'art. 51, comma 3-*quinquies*, c.p.p., da un magistrato designato dal procuratore della Repubblica presso il giudice competente. Dall'altro lato, viene modificato l'art. 328 c.p.p., affinché, con riferimento ai reati di cui all'art. 51, comma 3-*quinquies* c.p.p., le funzioni di giudice per le indagini preliminari e dell'udienza preliminare siano esercitate da un magistrato del tribunale del capoluogo del distretto nel cui ambito ha sede il giudice compente (art. 328, comma 1-*quater* c.p.p.)[43].

Nonostante il sicuro impatto positivo delle modifiche richiamate sulla coerenza interna del sistema, traspare dalle norme in questione una complessa realtà ove, in nome di una pretesa efficienza investigativa, si trascura un principio

---

[37] Cfr. L. LUPARIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa (L. 18 Marzo 2008 n. 48). I profili processuali*, in *Dir. pen. proc.*, 2008, p. 723.

[38] Sui problemi organizzativi sorti nelle procure distrettuali a seguito della modifica, v. F. CAJANI, *La Convenzione di Budapest nell'insostenibile salto all'indietro del Legislatore italiano, ovvero: quello che le norme non dicono…*, in *Cib. dir.*, 2010, p. 185 ss.

[39] In questo senso L. LUPARIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa (L. 18 Marzo 2008 n. 48). I profili processuali*, loc. ult. cit.

[40] Così L. LUPARIA, *I correttivi alle distorsioni sistematiche contenute nella recente legge di ratifica della Convenzione sul* Cybercrime, cit., p. 65.

[41] Decreto Legge 23 maggio 2008, n. 92, *Misure urgenti in materia di sicurezza pubblica*, pubblicato in *G.U.*, 26 maggio 2008, n. 122.

[42] Legge 24 luglio 2008, n. 125, *Conversione in legge, con modificazioni, del decreto-legge 23 maggio 2008, n. 92, recante misure urgenti in materia di sicurezza pubblica*, pubblicata in *G.U.*, 25 luglio 2008, n. 173.

[43] Cfr. D. MANZIONE, *op. cit.*, p. 317, il quale evidenzia l'avvicinamento, quanto alla disciplina, frutto delle interpolazioni in parola, tra indagini sui *cybercrime* e indagini in materia di terrorismo.

fondamentale quale la naturalità del giudice. È fin troppo chiaro, infatti, che, in tali ipotesi, il giudice competente per territorio non sarà più quello del *locus commissi delicti*, ma quello distrettuale designato dalla legge.

Un simile spostamento funzionale della competenza, che "segue" l'attribuzione distrettuale del pubblico ministero, genera qualche perplessità: dalla riforma pare potersi inferire che il legislatore abbia ritenuto l'utilità delle indagini bene da tutelare maggiormente rispetto al principio di naturalità del giudice, vale a dire l'unico criterio dotato di copertura costituzionale (art. 25 Cost.).

È, peraltro, dubbio che l'obiettivo dell'efficacia possa dirsi effettivamente raggiunto, considerata la mancanza di organismi di coordinamento fra procure[44], tanto più necessari in un ambito quale le indagini informatiche in materia di *computer crimes*. Queste ultime, infatti, a causa delle difficoltà relative all'individuazione del *locus commissi delicti*[45], frutto della già evidenziata natura immateriale dei dati informatici, si prestano ad una duplicazione di procedimenti[46].

Di quest'ultimo problema si occupa compiutamente, ma in una prospettiva internazionale, la Convenzione di Budapest sul *Cybercrime*. Quanto alla giurisdizione in tema di criminalità informatica, il testo pattizio si limita, in dettaglio, ad imporre ad ogni Paese l'adozione le misure legislative necessarie a radicare la propria «competenza» – termine utilizzato, all'evidenza, in senso atecnico – in relazione ai reati contemplati dalla Convenzione stessa. Qualora più Stati rivendichino la giurisdizione su un determinato fatto, il conflitto va risolto mediante una consultazione fra i medesimi (art. 22)[47].

---

[44] In ottica critica, relativamente all'esclusione, in capo al procuratore nazionale antimafia, della possibilità di coordinare le operazioni in materia di *Cybercrime*, nonché sul mancato coordinamento tra le procure infradistrettuali, v. D. MANZIONE, *op. cit.*, p. 315.

[45] Cfr. H. BELLUTA, Cybercrime *e responsabilità degli enti*, cit., p. 98. Per L. LUPARIA, *La disciplina processuale e le garanzie difensive*, cit., p. 155, evidenzia come la difficoltà di individuazione del luogo di commissione del reato ha «consegnato una eccessiva discrezionalità al pubblico ministero circa la scelta della sede giudiziaria ove incardinare inizialmente il procedimento».

[46] Di tal ché, ogni speranza di coordinamento resta affidata al coordinamento spontaneo di cui all'art. 371 c.p.p. e, dunque, in ultima analisi, alla buona volontà dei procuratori distrettuali. Cfr. M. DANIELE, *La prova digitale nel processo penale*, cit., pp. 286-287, nonché R. ORLANDI, *op. cit.*, p. 133.

[47] La dottrina statunitense ha criticato la disposizione in parola, poiché non risolverebbe il "dilemma" fondamentale relativo alla giurisdizione, limitandosi ad un mero rimando a possibili accordi fra gli Stati coinvolti. Cfr. M.F. MIQUELON-WEISMANN, *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*, in 23 *J. Marshall J. Computer & Info. L.*, 2005, p. 347, nonché A.M. WEBER, *The Council of Europe's Convention on Cybercrime*, in *18*

Più numerose le disposizioni relative al coordinamento investigativo[48]. L'art. 23, invero, impone alle parti contraenti un obbligo di cooperazione nelle indagini riguardanti i «reati collegati a sistemi e dati informatici, o per raccogliere le prove, in forma elettronica, di un reato»; l'art. 25 impone «la più ampia mutua assistenza» tra le parti in ambito investigativo e, in particolare, nella ricerca della prova informatica[49]. Le richieste di mutua assistenza devono essere rivolte ad un'autorità centrale designata da ciascuno Stato e le autorità centrali devono comunicare in via diretta tra loro (art. 27); per lo Stato italiano, tale autorità è stata individuata nel Ministero di Giustizia (art. 13 L. 48/2008). Ogni Stato può, comunque, trasmettere, anche senza preventiva richiesta, ad altra parte informazioni che ritenga utili al fine di avviare o svolgere indagini relative ai *computer crimes* (art. 26)[50].

Le norme in parola si giustificano non appena si considera il carattere transnazionale della criminalità informatica e l'universalità della rete *internet*[51], i quali impongono strumenti di cooperazione fra Stati ulteriori e di più semplice utilizzo rispetto a quelli tradizionali. Non solo: tali strumenti devono essere attivati in tempi brevissimi, affinché non si produca un definitivo smarrimento del dato. Nella medesima ottica, sono stati attivati, prima e dopo l'attivazione della Convenzione di Budapest, numerosi *working group* per l'ideazione e lo sviluppo di regole comuni e per collaborare nello svolgimento delle indagini informatiche[52].

Berkeley Tech. L.J., 2003, p. 437. Sul punto, v. anche G.M. RUOTOLO, *op. cit.*, pp. 861-862, il quale sottolinea come la disposizione non preveda nemmeno un obbligo *de negoziando*.

[48] È opportuno precisare che gli strumenti forniti dalla Convenzione si aggiungono – e non sostituiscono – a quelli già previsti dai singoli sistemi o da altra fonte pattizia. Cfr. E. SELVAGGI, *Cooperazione giudiziaria veloce ed efficace*, in *Guida dir.*, 2008, n. 16, p. 73.

[49] Le richieste potranno essere inoltrate adottando strumenti che consentono un'immediata ricezione quali *fax* o *posta elettronica*. Ciò, in ragione dell'essenzialità del fattore-tempo in una indagine che mira alla ricerca di dati a forte rischio di dispersione. Cfr. P. PERRI, voce Computer forensics *(indagini informatiche)*, in *Dig. pen.*, VI ed., Agg., Utet, Torino, 2011, p. 108.

[50] Una panoramica delle disposizioni in tema di cooperazione internazionale per l'accertamento dei *cybercrime*, incluse le regole dettate in tema di estradizione, è offerta da C. SARZANA DI SANT'IPPOLITO, *La Convenzione europea sulla cibercriminalità*, in *Dir. pen. proc.*, 2002, p. 510 ss.

[51] Cfr. L. LUPARIA, *La disciplina processuale e le garanzie difensive*, cit., p. 211 ss.

[52] L. LUPARIA, *La disciplina processuale e le garanzie difensive*, cit., pp. 211-212, richiama i gruppi di lavoro nati all'interno dell'Ocse e, nel quadro del G-8, dell'*High Tech Sub-group*. L'Autore ricorda che proprio da una proposta di quest'ultimo è scaturito l'art. 35 della Convenzione, il quale prevede una Rete di assistenza immediata sempre attiva (Rete 24/7) per assicurare assistenza immediata in fase investigativa e per la raccolta di prove. Questa collaborazione può assumere la forma dell'apporto di consigli tecnici (lett. a), nella conservazione di dati (lett. b), e finanche nella raccolta di prove, nella trasmissione di informazioni e nella localizzazione dei sospetti (lett. c). Le comunicazioni tra *task-force* avvengono per mezzo di "punti di contatto" forniti di personale formato ed equipaggiato. Per l'Italia, tale punto è individuato, ai sensi dell'art. 13, comma 2, L. 48/2008 dal Ministero dell'Interno di concerto con il Ministero di Giustizia; E. SELVAGGI,

Restano, però, nella nuova disciplina, alcune zone d'ombra relativamente ai rapporti fra Stati. L'art. 32 della Convenzione permette ad uno Stato, pur senza l'autorizzazione dell'altra parte, di accedere a dati informatici immagazzinati disponibili al pubblico, ovunque essi si trovino, nonché di accedere o ricevere, mediante un sistema informatico posto nel proprio territorio, dati situati in altro Stato, qualora la parte *accipiens* abbia ottenuto il previo consenso della persona «legalmente autorizzata a divulgare i dati»[53].

Chiara la *ratio* della norma: poiché l'attivazione dei tradizionali strumenti di coordinamento investigativo – prima fra tutti la rogatoria – richiede un *iter* lungo e complesso, si consente allo Stato di "fare da sé", sempre che vi sia il consenso di colui che può disporre del dato.

Meno chiara la soluzione al problema circa l'individuazione del titolare del consenso. I dubbi al riguardo nascono dal fatto che, qualora il soggetto in grado di divulgare legittimamente i dati fosse identificato nell'*Internet service provider*[54], un semplice nulla osta da parte di un soggetto privato consentirebbe ad un'autorità di altra nazione una ricerca diretta di elementi di prova localizzati in territorio

---

Task force operativa 24 ore al giorno, in *Guida dir.*, 2008, n. 16, p. 74, riferisce che, per l'Italia, tale Rete di assistenza è stata individuata in una struttura operativa presso il Servizio di polizia postale e delle comunicazioni della Polizia di Stato. In precedenza, anteriormente all'entrata in vigore della L. 48/2008, si era evidenziata l'opportunità di indicare, quale punto di contatto, il procuratore nazionale antimafia, qualora – come poi non è stato – gli fossero stati attribuiti compiti di coordinamento tra procure nel contrasto alla criminalità informatica. V. R. ORLANDI, *op. cit.*, p. 133.

[53] In alcuni casi, la polizia giudiziaria potrebbe apprendere il dato ritenuto di interesse investigativo anche senza coinvolgere l'autorità estera. Questo il caso: la polizia giudiziaria potrebbe trovarsi ad operare su un *client* (vale a dire, un terminale che consente di accedere ad altra risorsa – *server* – che contiene il dato) materialmente presente sul luogo della perquisizione in territorio italiano, il cui effettivo contenuto è, però, interamente ubicato in *server* situati all'estero. In simili ipotesi, l'eventuale acquisizione dei dati sfruttando il *client* avverrebbe a totale insaputa dell'autorità giudiziaria dello Stato ove i *server* sono localizzati. Di qui, l'interrogativo se l'acquisizione dei dati mediante l'attrezzatura (*client*) posta all'interno del territorio nazionale sia consentita o meno. I primi commentatori hanno ritenuto di poter superare il problema, fondando la legittimità dell'attività investigativa sul rilievo che, comunque, il *server* localizzato all'estero «non viene "fisicamente toccato", dal momento che la polizia giudiziaria – operando dal *client* – si limita a richiamare su di esso le informazioni utili alle indagini, al fine di farne una copia; la polizia giudiziaria, in questo modo non forza alcuna misura di protezione, dal momento che la preesistente interconnessione tra le diverse postazioni informatiche è tale da poter affermare che il server è stato appositamente configurato per fornire le risposte alle richieste provenienti da tutti i *client* all'interno di una determinata rete ed, in particolare, a quello oggetto di ispezione». Cfr., al riguardo, S. ATERNO-M. MATTIUCCI, Cloud forensics *e nuove frontiere delle indagini informatiche nel processo penale*, in Arch. pen., 2013, pp. 876-877. Gli Autori reputano, comunque, necessario operare mediante rogatoria oppure mediante richiesta alla società che gestisce il *cloud* laddove i dati contenuti all'interno della "nuvola" costituiscano il corpo del reato (ad esempio, qualora il *cloud* contenga immagini pedopornografiche). Ciò, poiché in tale caso l'autorità giudiziaria è tenuta alla distruzione del materiale

[54] Se, al contrario, si ritenesse che il soggetto che può disporre del dato sia unicamente colui che lo ha formato o a cui il dato afferisce – vale a dire colui sul quale si sta indagando –, la disposizione sarebbe assolutamente inutile.

straniero. Conseguenza inaccettabile, giacché sarebbe evidente la violazione di sovranità da parte dello Stato agente, nonché il contrasto con i principi generali in tema di assistenza giudiziaria internazionale.

Né varrebbe obiettare che la disposizione in parola costituisce una «contraria disposizione espressamente prevista» in grado, quale regola eccezionale, di derogare alle condizioni stabilite dalla legislazione dello Stato a cui l'assistenza è richiesta (art. 25, comma 4, Convenzione di Budapest)[55]. Pare difettare, al riguardo, proprio il requisito dell'indicazione espressa della natura eccezionale della disposizione, poiché all'opinione criticata si perviene unicamente in virtù di una peculiare interpretazione del termine "autorizzazione", intesa quale rimozione, da parte di un soggetto privato, di un ostacolo legislativamente imposto[56].

È opportuno, allora, ritenere comunque doveroso il ricorso ai tradizionali strumenti di cooperazione internazionale ed *in primis* alla rogatoria. Ecco, tuttavia, profilarsi una possibile obiezione: l'impiego dei mezzi di acquisizione della prova già noti potrebbe mettere a rischio l'efficacia dell'accertamento, tenendo a mente le caratteristiche mutabili del dato informatico. In realtà, viene in soccorso, a tal proposito, l'art. 29 della Convenzione, il quale prevede che una parte possa richiedere ad un'altra la conservazione rapida dei dati immagazzinati in un sistema informatico situato nel territorio di quest'ultima, qualora lo Stato richiedente intenda avanzare una richiesta di mutua assistenza per la perquisizione, sequestro o altro strumento simile, o per la divulgazione dei dati. Il congelamento del dato potrebbe, dunque, rivelarsi idoneo alla tutela dell'integrità del dato informatico.

In conclusione, se a livello comunitario il problema dell'immaterialità delle fonti di prova informatiche è stato affrontato e parzialmente risolto attraverso la previsione di strumenti di cooperazione internazionale, a livello interno la disciplina è foriera di contraddizioni, laddove, nel perseguire la chimera dell'efficienza investigativa, finisce per creare un *vulnus* alla naturalità del giudice senza risolvere il vero nodo critico legato alla possibile duplicazione di procedimenti.

---

[55] V. M. GUERNELLI, *op. cit.*, p. 770.
[56] V. M. GUERNELLI, *op. cit.*, p. 770, nota 55.

3. Il ruolo della polizia giudiziaria: presupposti e limiti dell'attività *undercover* in ambiente digitale

Le caratteristiche peculiari della fonte di prova digitale e, segnatamente, la sua immaterialità e deperibilità impongono che il dato sia trattato unicamente da soggetti con conoscenze tecniche specifiche[57].

È, dunque, necessario che gli operanti di polizia giudiziaria, chiamati spesso ad un primo contatto con il dato digitale già nell'immediatezza del fatto, possiedano tali nozioni[58].

Un esempio concreto della delicatezza delle operazioni di gestione del dato informatico è stato recentemente fornito dalle indagini relative ad un recente caso di cronaca[59], ove proprio condotte scorrette di accesso a sistemi informatici da parte degli operanti hanno determinato «la sottrazione di contenuto informativo con riferimento al *personal computer* [dell'indagato] pari al 73,8% dei *files* visibili, con riscontrati accessi su oltre 39.000 *files*, interventi di accesso su oltre 1.500 *files* e creazione di altri 500 *files*», con «effetti devastanti» in ordine all'integrità del dato digitale[60].

Ma i riflessi del fenomeno non si arrestano qui. Ancor prima della gestione del dato informatico, la fase relativa all'individuazione di quest'ultimo presenta caratteri peculiari, dovuti alla difficile convivenza fra regole del mondo digitale e strumenti giuridici in mano agli inquirenti.

---

[57] Di qui le numerose iniziative di formazione del personale di polizia giudiziaria ad opera degli Uffici distrettuali per l'informatica. Cfr. M. CARDUCCI, *La cooperazione giudiziaria e di polizia nelle indagini sul* cybercrime*: l'esperienza del* pool *reati informatici presso la procura di Milano*, in F. CAJANI-G. COSTABILE (a cura di), *Gli accertamenti informatici nelle investigazioni penali: una prospettiva europea*, Experta, Forlì, 2011, p. 17.

[58] Per un richiamo alla necessità, in capo alla polizia giudiziaria, di una «rigorosa applicazione di conoscenze e metodologie scientifiche nell'acquisizione degli elementi materiali» rinvenuti sulla scena del crimine, v. A. CHELO, *Le prime indagini sulla scena del crimine*, cit., p. 8.

[59] A Garlasco (PV), il 22 agosto 2007, Chiara Poggi venne uccisa nella propria abitazione. Fin dal principio delle indagini, le attenzioni della polizia giudiziaria si concentrarono sul fidanzato della giovane, Alberto Stasi. Egli sostenne che, la mattina del delitto, aveva lavorato con il proprio *personal computer* alla tesi di laurea. Il *computer* venne, dunque, posto sotto sequestro ed analizzato dagli operanti.

[60] Le citazioni provengono dalla sentenza del Tribunale Vigevano, 17 dicembre 2009, Stasi, richiamata da L. MARAFIOTI, Digital evidence *e processo penale*, cit., p. 4522. In proposito, v. anche la puntuale ricostruzione dei fatti di G. VACIAGO, Digital Evidence, Giappichelli, Torino, 2012, p. 18 ss. Più in generale, sugli errori tecnici degli operanti nelle indagini scientifiche, cfr. D. CURTOTTI NAPPI-L. SARAVO, *L'errore tecnico-scientifico sulla scena del crimine. L'errore inevitabile e le colpe dello scienziato, del giurista e del legislatore*, in *Arch. pen.*, 2011, p. 1 ss.

Il riferimento è, anzitutto, alle innumerevoli possibilità di anonimato che offre la rete *internet*[61], nonché alle difficoltà legate all'assegnazione di un medesimo indirizzo *Internet Protocol* a più soggetti. Invero, il recente esaurimento degli indirizzi *IP*[62] ha portato alcuni *provider* all'assegnazione di un identico indirizzo a più soggetti nel medesimo arco temporale, con le intuibili conseguenze in ordine all'impossibilità di identificare l'effettiva postazione da cui è stata posta in essere la condotta criminosa.

A ben vedere, il tema in discussione affonda le sue radici nel «peccato originale»[63] dell'accertamento informatico. Anche qualora sia stato possibile identificare compiutamente il macchinario dal quale proviene una determinata attività, è assai improbabile che quest'ultimo fornisca indicazioni sull'effettivo utilizzatore. Ipotesi tipica – si pensi alle indagini relative all'accertamento del reato di detenzione di materiale pedopornografico di cui all'art. 600-*quater* c.p. – è quella in cui viene identificata una determinata abitazione quale fonte della connessione incriminata; al *computer* ivi presente, però, hanno accesso più componenti del nucleo familiare.

Due i corollari che paiono scaturire dalle precedenti riflessioni. Il primo attiene ai poteri del pubblico ministero: egli ha inevitabilmente amplissimi margini di manovra in relazione al momento dell'iscrizione del nominativo dell'indagato nel registro delle notizie di reato di cui all'art. 335 c.p.p., con le intuibili conseguenze in ordine ad una durata arbitraria delle indagini. Nell'ipotesi accennata, l'alternativa sarebbe tra l'immediata iscrizione nel registro di cui all'art. 335 c.p.p. della totalità degli utilizzatori della strumentazione informatica non appena fosse identificata la fonte della connessione utilizzata per attività illecite, e la ritardata iscrizione di un solo nominativo a seguito di più stringenti accertamenti posti in essere dalle forze di polizia all'interno dell'abitazione.

---

[61] Si pensi all'utilizzo di *server proxy*, strumenti che si interpongono tra il *client* e l'utente, mascherando il vero indirizzo *IP* di quest'ultimo. Il riferimento, ancora, è all'utilizzo di macchinari, all'insaputa del proprietario, infettati da *virus* informatici del tipo *trojan*. Con particolare riferimento ai *computer crimes*, dunque, nell'ambiente telematico il numero di sospetti è pressoché infinito.

[62] A seguito dell'esaurimento degli indirizzi *IP* del tipo IPv4, *internet* sta vivendo una fase di transizione dal vecchio protocollo al nuovo IPv6; fase che, tuttavia, presenta notevoli difficoltà per l'incompatibilità tra le due tipologie di *Internet Protocol address*.

[63] L'espressione è di L. LUPARIA, *La disciplina processuale e le garanzie difensive*, cit., p. 144.

Si perviene, così, al secondo corollario: l'indagine informatica non può prescindere dalle ordinarie attività di polizia giudiziaria. Segnatamente, nell'esempio in parola, ispezioni, perquisizioni e sommarie informazioni potrebbero, perlomeno, consentire di identificare in quale stanza sia collocata la strumentazione informatica; chi si trovi solitamente nell'abitazione nell'orario in cui è avvenuta la connessione; nonché, le ulteriori attività poste in essere con l'attrezzatura informatica nella medesima finestra temporale in cui è stato commesso il delitto che si vuole accertare (pagine *web* visitate, scrittura di documenti e quant'altro possa risultare utile)[64].

Alla stregua di questi rilievi, non vi è dubbio circa le ineludibili operazioni preliminari da realizzare ad opera della polizia giudiziaria quando quest'ultima debba interagire con una *scena criminis* digitale, vale a dire una corretta descrizione dell'ambiente e l'individuazione dei soggetti utilizzatori dei supporti informatici.

Vi sono, però, altri ostacoli in grado di frapporsi all'accertamento dell'autore della condotta criminosa; segnatamente, barriere frutto di scelte – del tutto legittime – dell'utilizzatore della strumentazione informatica. Il richiamo è all'utilizzo di misure di protezione dei dati quali la crittografazione[65] o la richiesta di *password* per accedere al sistema o a determinate cartelle[66].

---

[64] Cfr. Cass., Sez. III, 28 novembre 2011, n. 44065, in *C.E.D. Cass.*, rv. 251401. In tale occasione, tra gli elementi che militavano in favore dell'ascrivibilità del *download* e della detenzione di alcuni *file* raffiguranti immagini di carattere pedopornografico all'imputato, vi erano lo *username* e il *nickname* utilizzati sul sito di *file-sharing* ove la polizia giudiziaria aveva individuato tali *files*, i quali erano formati con il nome dell'imputato, nonché la presenza del *computer* nella camera dello stesso all'atto della perquisizione in fase d'indagini. Ancora, in Cass., Sez. V, 16 giugno 2014, n. 25774, *inedita*, si rinviene l'affermazione per cui l'attività investigativa della polizia postale ha consentito «di associare al profilo del sito *Badoo* la famiglia dell'imputato, attraverso l'individuazione dell'indirizzo *IP* del *computer* che aveva creato l'*account* e, nell'ambito del nucleo familiare corrispondente all'utenza telefonica, di risalire all'odierno imputato grazie all'analisi dell'*hard disk* del suo *computer* portatile». Da ultimo, Trib. Aosta, sent. 28 gennaio 2014, C.M.G., *inedita*, illustra le circostanze che hanno portato il collegio ad identificare l'imputato quale effettivo utilizzatore di una postazione informatica all'interno di una abitazione: «non vi è dubbio alcuno sulla riconducibilità del materiale pedo-pornografico sequestrato all'odierno imputato, atteso che il *personal computer* ed il restante materiale informatico venivano rinvenuti nella stanza da letto occupata in via esclusiva da C.M.G.; l'accensione dell'apparecchio era protetto da una *password* associata ad una *user-id* denominata "Marco", chiaramente riconducibile soltanto all'imputato, non essendo emersi nella vicenda altri soggetti aventi tale nome proprio; le altre persone conviventi nell'abitazione - segnatamente C.M.S. - non avevano alcuna pratica di informatica».

[65] In tema, v. N. SOARES, *The Right to Remain Encrypted: the Self-Incrimination Doctrine in the Digital Age*, in *49 Am. Crim. L. Rev.*, 2012, p. 2001 ss.

[66] Cfr., a tal proposito, A.M. GERSHOWITZ, *Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest?*, in *96 Iowa L. Rev.*, 2011, p. 1125 ss.;ID., *The iPhone Meets the Fourth Amendment*, in *56 UCLA L. Rev.*, 2008, p. 27 ss., nonché O.S. KERR, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy"?*, in *33 Conn. L. Rev.*, 2001, p. 33 ss., e S.J.

Se, in determinati casi, un metodo di decrittazione *bruteforce*[67] può condurre alla rimozione di tali ostacoli, soprattutto in caso di *password* brevi, in altre ipotesi potrebbe essere impossibile per gli investigatori superare le misure di protezione[68]. Di tal ché, per proseguire nelle indagini, gli operanti sarebbero "costretti" a dover chiedere al soggetto in possesso della *password* o della chiave di crittografazione di rivelare quest'ultima.

Sicché, in tale eventualità, la prosecuzione stessa delle indagini viene a dipendere da una scelta difensiva dell'indagato: rivelare o meno la propria *password*. Di qui, il correlativo dubbio se quest'ultimo sia costretto o meno a fornire tali informazioni alla polizia giudiziaria, considerando, altresì, che, in caso di assenso, egli fornirebbe un aiuto probabilmente decisivo alle indagini.

Deve, infatti, evidenziarsi che il "contatto" tra polizia giudiziaria e persona indagata avviene, nel corso delle indagini informatiche, in un momento iniziale del procedimento: l'apprensione dell'attrezzatura è, di regola, tra gli atti iniziali di una indagine informatica. In tale fase, è ben possibile che, a fronte dell'impossibilità di accedere al contenuto dell'elaboratore, l'indagine si debba fermare.

Il punto di partenza per la soluzione del quesito pare offerto dai fondamentali canoni del processo penale e, in particolare, dal principio *nemo tenetur se detegere*[69], il quale impone l'esclusione di qualsivoglia onere collaborativo dell'indagato in sede di indagini. Se così è, una siffatta richiesta da parte degli inquirenti dovrà essere preceduta dall'avviso di cui all'art. 64, comma 3, lett. *b*), c.p.p., in virtù del richiamo operato dall'art. 350, comma 1, c.p.p.[70]. In assenza dell'avviso relativo alla facoltà di non rispondere, saranno inutilizzabili sia il dato

---

EDGETT, *Double-Clicking on Fourth Amendment Protection: Encryption Creates a Reasonable Expectation of Privacy*, in *30 Pepp. L. Rev.*, 2003, p. 340 ss.

[67] Il metodo consiste nell'inserimento di tutte le possibili *password* e, dunque, alla lunga, consente con certezza di pervenire al superamento della barriera posta dall'utente; tuttavia, com'è facile intuire, si tratta di un procedimento dalle tempistiche tendenzialmente incompatibili con la celerità necessaria in fase investigativa.

[68] V., in proposito, D. LA MUSCATELLA, *La ricerca delle fonti di prova sulle reti di* cloud computing, cit., pp. 483-484.

[69] Per un'approfondita analisi sul diritto al silenzio nel sistema processual-penale, v. L. MARAFIOTI, *Scelte autodifensive dell'indagato e alternative al silenzio*, Giappichelli, Torino, 2000, *passim*; con precipuo riferimento al tema della prova informatica cfr. ID., Digital evidence *e processo penale*, cit., p. 4516.

[70] *Contra* P. FELICIONI, *Le ispezioni e le perquisizioni*, Giuffrè, Milano, 2012, pp. 247-248. Invero, secondo l'Autrice, «l'avvertimento del diritto al silenzio è garanzia delineata con riferimento agli atti di indagine in cui l'indagato interviene, non per propria scelta, come dichiarante».

raccolto sia i successivi accertamenti operati sul sistema informatico[71] (art. 64, comma 3-*bis* c.p.p.).

La soluzione non pare mutare nemmeno considerando l'art. 19, comma 4, della Convenzione sul *Cybercrime*, in base al quale ogni Stato aderente «deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle proprie competenti autorità di ordinare ad ogni soggetto che abbia conoscenza […] delle misure utilizzate per proteggere i dati informatici in esso contenuti, di mettere a disposizione tutte le informazioni necessarie» per la perquisizione e il sequestro dei sistemi contenenti i dati.

È sufficiente, per il momento, ricordare che, in ordine al problema della crittografazione dei dati, la L. 48/2008 attuativa della Convenzione si limita ad interpolare negli artt. 247 e 352 c.p.p. un comma 1-*bis*. In particolare, si prevede, in capo alla polizia giudiziaria, nell'ambito delle perquisizioni informatiche, nonché delle perquisizioni in flagranza di reato o qualora si debba procedere all'esecuzione di un'ordinanza che dispone la custodia cautelare o un ordine di carcerazione relativo ad uno dei reati di cui all'art. 380 c.p.p., oppure qualora si debba procedere al fermo di una persona indiziata di delitto, il potere di perquisire sistemi informatici o telematici «ancorché protetti da misure di sicurezza». Gli operanti, insomma, possono superare eventuali misure di sicurezza con metodi di decrittazione. Si tratta, all'evidenza, di facoltà ben diversa rispetto alla richiesta all'indagato di fornire accesso al dato mediante l'inserimento della propria *password*[72].

Nella prassi, il problema non sembra essere stato affrontato nel dettaglio. È, comunque, lecito aspettarsi un diverso orientamento della giurisprudenza in ordine all'utilizzabilità delle risultanze, almeno nel caso la *password* sia stata fornita spontaneamente dall'indagato; ciò, considerando il ricorrente «"incubo di impunità" dei soggetti esaminabili nel corso delle indagini»[73] che ha portato i giudici di

---

[71] In questo senso, correttamente, L. LUPARIA, Computer crimes *e procedimento penale*, in AA.VV., *Trattato di procedura penale*, diretto da G. Spangher, vol. VII, Tomo I, Utet, Torino, 2011, pp. 387-388.

[72] La mancata adozione, da parte del legislatore, delle misure richiamate dall'art. 19, comma 4, della Convenzione pare, ad ogni modo, condivisibile, in quanto tali norme avrebbero comportato un insanabile contrasto con l'art. 64 c.p.p.

[73] Così L. MARAFIOTI, *Scelte autodifensive dell'indagato e alternative al silenzio*, cit., p. 226.

legittimità ad affermare che «riconoscere la tutela dell'inutilizzabilità delle dichiarazioni spontaneamente rese equivarrebbe ad ipotizzare [...] una sorta di incapacità penale dell'indagato stesso»[74].

Depone in tal senso anche un'indagine di quanto accade, in tema, in altri ordinamenti. In Gran Bretagna, la questione è stata risolta a livello legislativo; invero, ai sensi della *section* 49 del *Regulation of Investigatory Powers Act*, le forze di polizia possono, in presenza di determinati presupposti[75], imporre un *disclosure requirement* per prevenire o per accertare l'avvenuta commissione di un crimine (*section* 49, comma 3, *R.i.p.a.*)[76].

Negli Stati Uniti, le Corti hanno in più occasioni affrontato il quesito se la richiesta, da parte delle forze di polizia, di fornire la *password* necessaria per accedere ad un *computer* ricada o meno nella tutela del *right against self-incrimination* offerta dal quinto emendamento della Costituzione. Se, inizialmente, si è fornita risposta affermativa[77], in seguito si è, tuttavia, precisato che l'inserimento della *password* all'interno del sistema non costituisce una *compelled testimonial communication* protetta dal quinto emendamento qualora gli inquirenti siano già a conoscenza della presenza dei *files* incriminanti sul *hard disk*[78].

La portata del fenomeno si comprende appieno non appena lo si inquadri in una prospettiva più ampia. Il problema dell'utilizzo della crittografia da parte del

---

[74] Cass., Sez. VI, 8 ottobre 1992, Lo Bello, in *Mass. pen. cass.*, 1993, n. 8, 4 ss.

[75] In particolare, gli inquirenti devono ritenere, «*on reasonable grounds*», che la chiave di crittografazione sia in possesso della determinata persona a cui rivolgere l'ordine di esibizione, che l'imposizione dell'ordine sia «*necessary for the purpose of securing [...] any statutory power or statutory duty*», nel rispetto del principio di proporzionalità con ciò che si ritiene possibile ottenere, e che non vi sia altro modo per ottenere accesso all'informazione che si intende ricercare.

[76] Cfr. B.M. PALFREYMAN, *Lessons from the British and American Approaches to Compelled Decryption*, in *75 Brook. L. Rev.*, 2009, p. 345 ss.

[77] V. *In re* Boucher (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473, (D. Vt. Nov. 29, 2007). Richiama la vicenda J. DUONG, *The Intersection of Fourth and Fifth Amendments in the Context of Encrypted Personal Data at the Border*, in *2 Drexel L. Rev.*, 2009, p. 313 ss.

[78] Ad esempio, qualora l'indagato abbia mostrato di sua spontanea volontà i *file* incriminanti agli operanti durante la *live search* del sistema, prima dello spegnimento del *computer*, come avvenuto nel caso *In re* Boucher (*Boucher II*), No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009). Una ricostruzione della vicenda è offerta da G. VACIAGO, Digital evidence, cit., pp. 124-125. Per un'analisi dei rapporti tra crittografia e quinto emendamento, nella copiosa letteratura statunitense, v. A.J. UNGBERG, *Protecting Privacy Through a Responsible Decryption Policy*, in *22 Harv. J. Law. Tech.*, 2009, p. 537 ss., nonché D. COLARUSSO, *Heads in the Cloud, a Coming Storm. The Interplay of Cloud Computing, Encryption, and the Fifth Amendment's Protection Against Self-Incrimination*, in *17 B.U. J. Sci. & Tech.*, 2011, p. 69 ss.; J.E.D. LARKIN, *Compelled Production of Encrypted Data*, in *14 Vand. J. Ent. & Tech. L.*, 2012, p. 264 ss.; N.K. MCGREGOR, *The Weak Protection of Strong Encryption: Passwords, Privacy, and Fifth Amendment Privilege*, in *12 Vand. J. Ent. & Tech. L.*, 2010, p. 581 ss.

soggetto indagato assume particolare rilevanza con riferimento alle ipotesi di pedopornografia *online*, con particolare riguardo alle ipotesi di cui agli artt. 600-*ter* e 600-*quater* c.p.; di regola, infatti, in tali casi, soltanto un'analisi compiuta dei dati contenuti nello strumento informatico può consentire di reperire decisivi elementi di prova a carico.

Proprio le indagini informatiche in tema di pornografia minorile meritano qualche considerazione a sé, poiché, per il contrasto di alcuni delitti contro la persona ritenuti particolarmente insidiosi[79], il legislatore ha previsto una disciplina *ad hoc*. Ai sensi dell'art. 14, comma 2, L. 269/98[80], su autorizzazione motivata a pena di nullità dell'autorità giudiziaria, il personale addetto dell'organo del Ministero dell'Interno per la sicurezza e la regolarità dei servizi di telecomunicazione può, nell'ambito dei compiti di polizia delle telecomunicazioni, «anche per via telematica», utilizzare indicazioni di copertura, «anche per attivare siti nelle reti, realizzare o gestire aree di comunicazione o scambio su reti o sistemi telematici, ovvero per partecipare ad esse».

Va rilevato, anzitutto, che le attività in questione consentono alla polizia giudiziaria, in ragione della particolare gravità di determinati reati, di agire quale agente provocatore. Si tratta, dunque, di norme che si collocano al di fuori degli ordinari principi vigenti in tema di acquisizione probatoria nell'attuale sistema processuale[81]. Di qui, l'impossibilità di applicare la disciplina in parola al di fuori dei confini tracciati dal legislatore.

Ciononostante, si sono registrati numerosi casi di utilizzo anomalo di tali strumenti di contrasto[82]. Un impiego eccessivamente disinvolto dell'attività *undercover* traspare, segnatamente, dalla diffusione sulla rete *web* di "messaggi

---

[79] Per quanto qui interessa, sono i delitti contro la persona di cui agli artt. 600-*bis*, comma 1, 600-*ter*, commi primo, secondo e terzo, e 600-*quinquies* c.p.

[80] Legge 3 agosto 1998, n. 269, *Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù*, pubblicata in *G.U.*, 10 agosto 1998, n. 185.

[81] Cfr. Cass., Sez. III, 21 ottobre 2003, n. 39706, in *Dir. giust.*, 2003, p. 20 ss., nonché Cass., Sez. III, 17 gennaio 2008, n. 8380, in *C.E.D. Cass.*, rv. 239407.

[82] Per di più, come evidenzia L. LUPARIA, *Le investigazioni informatiche in materia di pornografia minorile tra nuovi e vecchi abusi degli strumenti processuali*, in *Dir. internet*, 2005, p. 485, numerose «illecite strategie investigative […] non transitano sotto il vaglio giurisdizionale a cagione della scelta del prevenuto di accedere al rito negoziale del patteggiamento, opzione prescelta assai di frequente dagli imputati dei delitti a matrice pedopornografica al fine di evitare gli effetti stigmatizzanti della pubblicità dibattimentale».

pubblicitari civetta" del tutto generici[83], così come dalla predisposizione di "siti trappola" da parte di società private incaricate dagli inquirenti. Ciò, benché la lettera dell'art. 14 sia chiara nel consentire l'attività *undercover* ai soli agenti di polizia giudiziaria.

Ancora, si è legittimato, in via di prassi, l'utilizzo del congegno di cui all'art. 14, comma 2, L. 269/98, anche per l'accertamento dei reati di cui agli artt. 600-*quater* e 600-*ter*, comma 4, c.p.

Quest'ultimo punto è estremamente delicato e merita qualche osservazione. Il quesito concerne la sorte processuale del materiale acquisito a seguito delle speciali tecniche investigative previste dalla L. 269/98, qualora gli elementi di prova raccolti non riguardino le fattispecie richiamate, ma altri reati non inclusi nell'elenco tassativo di cui all'art. 14 L. 269/98.

In assenza di qualsivoglia *fumus* relativo ai reati contemplati da quest'ultima disposizione, i giudici di legittimità hanno, inizialmente, ritenuto inutilizzabili in ogni stato e grado – con conseguente preclusione di qualsivoglia impiego del dato anche meramente investigativo – gli elementi di prova a carico dell'indagato desumibili da materiale pedopornografico sottoposto a sequestro a seguito dello svolgimento di indagini sotto copertura[84].

A tale soluzione si è pervenuti, da un lato, ritenendo gli elementi acquisiti frutto di un'attività illecita, e, dunque, inutilizzabile, sulla scia di quell'orientamento che ritiene applicabile la sanzione di cui all'art. 191 c.p.p. anche per violazioni della legge penale sostanziale[85]. Dall'altro lato, si afferma che, in applicazione del

---

[83] V, al riguardo, D. DELL'ORTO, *Pedopornografia* on line *e indagini informatiche – complessità e peculiarità tecnico-giuridiche della materia*, in *Cass. pen.*, 2007, p. 3042 ss. Cfr. anche Cass., Sez. III, 21 ottobre 2003, n. 39706, cit., p. 22. Nel caso di specie, la difesa dell'indagato, nell'ambito del procedimento incidentale di impugnazione di un sequestro probatorio di materiale informatico, lamentava la diffusione nella rete un messaggio pubblicitario in inglese, senza alcun riferimento a *file* pedopornografici; i *file* stessi avevano nomi del tutto generici. Nonostante il Tribunale del riesame non avesse affrontato la vicenda sotto questo profilo, giacché altro è stato ritenuto assorbente, la Cassazione, sollecitata dall'impugnazione del pubblico ministero, afferma, proprio con riferimento a questo profilo, che si è trattato «di una operazione investigativa poco rispettosa delle norme di legge e dei diritti fondamentali del cittadino».

[84] V., per tale ipotesi di inutilizzabilità "derivata", Cass., Sez. III, 22 settembre 2004, Gullello, in *Cass. pen.*, 2005, p. 2679 ss., con nota di C. Marinelli, nonché in *Dir. internet*, 2005, p. 39 ss., con nota critica di E. Aprile. Cfr. anche A. NATALINI, *Pedopornografia e diritti della difesa. Per le attività di contrasto niente* analogia iuris, in *Dir. giust.*, 2003, n. 41, p. 16 ss.

[85] Pare profilare una prova illecita Cass., Sez. III, 21 ottobre 2003, n. 39706, cit., p. 23, secondo cui «l'illegittimità (anzi: illiceità) di tutta la […] attività [investigativa] nel suo complesso [comporta] la totale

principio generale sancito dall'art. 191 c.p.p., le prove acquisite in violazione dei divieti stabiliti dall'art. 14 L. 269/1998 – pur in assenza di una esplicita sanzione – non possono essere utilizzati[86].

Tuttavia, successivamente, la Corte non è stata altrettanto rigorosa. In primo luogo, ferma l'inutilizzabilità delle prove acquisite con riferimento a reati non inclusi nel catalogo tassativamente indicato dal legislatore, poiché il materiale raccolto costituisce corpo del reato, il sequestro del medesimo rappresenta comunque, secondo i giudici, un atto dovuto e legittimo ai sensi dell'art. 253 c.p.p.[87].

A sostegno di quest'assunto, si afferma, inoltre, che, qualora nell'ambito di una attività di contrasto *undercover* la polizia giudiziaria si imbatta in altri meno gravi reati, essa non potrebbe non adempiere al proprio «compito istituzionale di svolgere indagini e di assicurare le fonti di prova» anche in relazione a questi ultimi, «in ossequio all'art. 55 c.p.p. e allo stesso principio dell'obbligatorietà dell'azione penale di cui all'art. 112 Cost.»[88].

Non è difficile scorgere in tali argomentazioni l'eco del principio *male captum bene retentum*[89]: poiché il materiale raccolto costituisce corpo del reato, eventuali illegittimità delle operazioni che hanno portato alla scoperta degli elementi a carico non importano l'inutilizzabilità del medesimo o, quantomeno, consentono un utilizzo dello stesso come *notitia criminis* in base alla quale svolgere ulteriori indagini, nonché acquisire elementi probatori e disporre misure cautelari.

In secondo luogo, si è precisato che il *fumus delicti* in ordine ad uno dei reati contemplati dall'art. 14, comma 2, L. 269/98 deve essere valutato *ex ante*; vale a dire, nel momento in cui l'attività è stata disposta dall'autorità giudiziaria, e non con

---

inutilizzabilità, in ogni stato e grado del giudizio, di qualsiasi elemento di prova acquisito per mezzo della stessa».

[86] In quest'ottica, Cass., 13 aprile 2005, P.M. in proc. Spora, in *Riv. pen.*, 2006, p. 762 ss., secondo cui si tratterebbe di un «caso scolastico» di applicazione dell'art. 191 c.p.p.

[87] V. Cass., Sez. V, 30 maggio 2003, n. 23894, in *C.E.D. Cass.*, rv. 225946, nonché, da ultimo, Cass., Sez III, 24 novembre 2010, n. 45571, in *C.E.D. Cass.*, 248767.

[88] Così Cass., Sez. III, 11 maggio 2005, A., cit., pp. 482-483.

[89] Cfr. Cass., Sez. III, 7 luglio 2004, n. 29496, in *C.E.D. Cass.*, rv. 229804. V. anche C. MARINELLI, *L'attività dell'agente provocatore per il contrasto alla pedopornografia: "straripamenti" investigativi e relative implicazioni processuali*, in *Cass. pen.*, 2005, p. 2683 ss.

riguardo all'esito investigativo[90]. Dunque, anche se gli elementi raccolti dalla polizia giudiziaria si riferiscono ad illeciti diversi e meno gravi di quelli ipotizzati in fase investigativa, essi saranno comunque utilizzabili se, al momento in cui l'attività è stata disposta, essa appariva legittima[91].

Tali affermazioni non paiono condivisibili. Invero, come si è esattamente osservato, appare fin troppo concreto il rischio di «manovre di aggiramento [dei limiti stabiliti dall'art. 14, comma 2, L. 269/1998] mediante l'arbitraria elevazione della gravità dell'addebito provvisorio al fine di integrare i parametri richiesti dal legislatore per l'attivazione dei […] poteri speciali di indagine»[92].

Prima di concludere sul punto, appare opportuna qualche considerazione su un ulteriore aspetto problematico della disciplina di cui all'art. 14, comma 2, L. 269/98. Nell'ambito delle indagini informatiche, è spesso arduo tracciare una precisa linea di demarcazione fra le "ordinarie" attività di polizia giudiziaria ai sensi dell'art. 55 c.p.p. e le speciali attività sotto copertura previste dalla legislazione speciale.

Se in alcune ipotesi la scelta dei giudici di legittimità di ricondurre determinate operazioni all'art. 55 c.p.p. appare condivisibile, laddove gli agenti si siano limitati ad un'attività di tracciamento informatico del luogo di provenienza della connessione[93], in altri casi sorge qualche perplessità. Si pensi al caso in cui un agente di polizia giudiziaria crei un falso profilo su un programma per la *chat* tra utenti, al fine di identificare uno dei partecipi alla conversazione; ebbene, la Corte di Cassazione ha ritenuto che simile operazione non rientri tra quelle previste dalla

---

[90] V. Cass., Sez. III, 11 maggio 2005, A., in *Dir. internet*, p. 481 ss., con nota di L. Luparia; v. anche Cass., Sez. III, 25 settembre 2008, n. 40036, in *C.E.D. Cass.*, rv. 241297, e Cass., Sez. III, 3 luglio 2008, n. 26763, in *C.E.D. Cass.*, rv. 240270. V. G. AMATO, *L'attivazione regolare dell'operazione salva i risultati di molte azioni simulate*, in *Guida dir.*, 2005, n. 25, p. 67 ss.

[91] La tesi riecheggia quel costante orientamento giurisprudenziale per cui i risultati delle intercettazioni sono comunque utilizzabili anche quando dalle conversazioni risultino reati di diverso titolo rispetto a quello ipotizzato del decreto autorizzativo. Cfr. Cass., Sez. I, 20 febbraio 2009, G.V.V., in *C.E.D. Cass.*, rv. 243780; Cass., Sez. VI, 24 giugno 2005, Bellato, in *C.E.D. Cass.*, rv. 232046; nonché, con precipuo riguardo alle attività *undercover* di cui all'art. 14, comma 1, L. 269/98, Cass., Sez. III, 6 dicembre 2007, G.F., in *C.E.D. Cass.*, rv. 239912.

[92] Così L. LUPARIA, *Le investigazioni informatiche in materia di pornografia minorile tra nuovi e vecchi abusi degli strumenti processuali*, cit., p. 485.

[93] V., in proposito, Cass., Sez. III, 8 luglio 2010, n. 29616, in *Dir. pen. proc.*, 2010, p. 1166.

L. 269/98, giacché si tratterebbe di attività «consentita a chiunque», e dunque non ad esclusivo appannaggio dell'*insider*[94].

Similmente, un orientamento ormai granitico considera attività d'indagine non sottoposta ai limiti e ai presupposti di cui all'art. 14 L. 269/98 il monitoraggio della rete *internet*, qualora lo stesso sia avvenuto senza alcun contatto con gli utenti e senza attività di intermediazione o acquisto simulato di materiale pornografico[95].

Ma vi è di più. Persino condotte penalmente rilevanti poste in essere dalla polizia giudiziaria senza la necessaria autorizzazione, quali l'accesso, visione e scaricamento[96] di *file* pedopornografici, sono state ritenute ordinarie attività di contrasto dei reati, estranee alla previsione di cui all'art. 14 della L. 269/98[97].

Una disamina delle più recenti sentenze che si sono occupate dell'argomento rivela, insomma, il tentativo di ridurre i confini delle particolari tecniche investigative informatiche di cui all'art. 14 L. 269/98, facendo rientrare tutte le attività "al limite" nei tradizionali compiti di polizia giudiziaria ai sensi dell'art 55 c.p.p.

La scelta giurisprudenziale appare, a ben vedere, finalizzata a consentire un più ampio margine operativo alla polizia giudiziaria. Ne esce rafforzato il potere dell'accusa; potere, questo, dai confini assai ampi già a causa dell'evidenziato carattere multiforme tipico delle indagini informatiche, cui corrisponde un elevato grado di scelta dei mezzi di ricerca della prova da utilizzare.

A fronte dell'elevata ingerenza sulla vita privata dei mezzi di ricerca della prova informatica – si pensi, per tutti, alle accennate attività di contrasto alla pedopornografia *online* – appare doverosa, a questo punto, un'indagine circa i poteri della difesa, onde verificare se possa dirsi sussistente un'effettiva parità delle armi.

---

[94] Nonostante la lettera dell'art. 14, comma 2, L. 269/98 faccia riferimento anche alla mera possibilità di «partecipare» ad «aree di comunicazione o scambio su reti o sistemi telematici», la Corte di cassazione è già da tempo orientata nel senso che l'attività *undercover*, per essere considerata tale, debba necessariamente integrare un ipotesi criminosa. Cfr. Cass., Sez. III, 8 luglio 2010, n. 29616, cit., nonché, da ultimo, Cass., 30 luglio 2013, n. 32926, in *C.E.D. Cass.*, rv. 257274. Sul punto, v. anche E. APRILE, *Limiti alla utilizzabilità processuale del sequestro di materiale informatico acquisito mediante siti* web *"civetta"*, in *Dir. internet*, 2005, p. 43 ss.

[95] V., *ex multis*, Cass., Sez. III, 30 marzo 2009, n. 13729, in *C.E.D. Cass.*, rv. 243389.

[96] Condotta, questa, chiaramente riconducibile alla fattispecie di cui all'art. 600-*quater* c.p.

[97] Cfr. Cass., Sez. III, 6 ottobre 2009, n. 41743, in *C.E.D. Cass.*, rv. 245262; cfr. anche Uff. indagini preliminari Firenze, sent. 28 ottobre 2014, G.A., *inedita*.

4. Poteri dell'accusa e facoltà della difesa nelle indagini informatiche a confronto. Il ruolo del consulente tecnico

La L. 397/2000, conferendo effettività al diritto di prova dell'indagato anche nella fase delle indagini, ha introdotto nel codice di procedura penale la facoltà per il difensore di svolgere una serie di attività in funzione della raccolta di emergenze in grado di supportare le proprie argomentazioni.

Con particolare riferimento alla possibilità di esperire indagini difensive informatiche, viene in considerazione l'art. 391-*sexies* c.p.p., il quale consente al difensore di effettuare un accesso per «prendere visione dello stato dei luoghi e delle cose ovvero per procedere alla loro descrizione o per eseguire rilievi tecnici […]»; in tal caso, il pubblico ministero avrà facoltà di assistervi[98]. A specificare in cosa possano estrinsecarsi i "rilievi" in parola soccorre l'art. 391-*decies* c.p.p., e, segnatamente, il comma 3, il quale chiarisce che il difensore può compiere anche accertamenti tecnici non ripetibili[99]; tuttavia, in simile ipotesi dovrà essere dato avviso al pubblico ministero per l'esercizio delle facoltà previste dall'art. 360 c.p.p. Qualora per gli accertamenti in parola occorrano conoscenze tecniche, i medesimi possono essere svolti da consulenti tecnici all'uopo nominati (art. 327-*bis* c.p.p.).

La disciplina succintamente esposta parrebbe, a prima vista, assicurare un paritario accesso tra accusa e difesa alla fonte di prova digitale in fase di indagine.

Un assunto di questo tipo sembra, però, difficilmente sostenibile, per un duplice ordine di ragioni.

In primo luogo, come si è correttamente notato[100], la L. 48/2008, se pure ha preveduto la possibilità per la polizia giudiziaria di svolgere rilievi aventi per oggetto il dato informatico, specificando le regole generali alle quali deve improntarsi l'azione degli inquirenti (art 354, comma 2, c.p.p.), nulla ha stabilito

[98] Qualora sia necessario accedere a luoghi privati o non aperti al pubblico, se manca il consenso di chi ne ha la disponibilità serve l'autorizzazione del giudice, con decreto che ne specifica le modalità (art. 391-*septies* c.p.p.). L'assenza di uno strumento di impugnazione dell'eventuale diniego ha portato una parte della dottrina a profilare dubbi di incostituzionalità della disposizione per contrasto con l'art. 111, comma 3, Cost., poiché non garantirebbe un effettivo diritto di difesa in parità con l'accusa. Cfr E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, cit., p. 160.

[99] Cfr. L. LUPARIA, *La disciplina processuale e le garanzie difensive*, cit., p. 182 ss.

[100] V. A.E. RICCI, Digital evidence*, sapere tecnico-scientifico e verità giudiziale*, cit., p. 359.

con riguardo alle indagini difensive. Naturalmente, ciò non può essere interpretato nel senso di una estromissione *tout court* della difesa da qualsiasi contatto con il dato informatico; però, pare cogliere nel segno chi teorizza, per il difensore, la possibilità di esperire «autonomi accertamenti solo negli spazi operativi che gli organi pubblici riterranno di riconoscergli in base al caso concreto»[101].

Le perplessità si acuiscono notevolmente se si considera che il difensore soltanto di rado ha accesso al luogo ove, di regola, si svolge l'attività di duplicazione del dato digitale ad opera della polizia giudiziaria, sia esso la scena del crimine o l'abitazione dell'indagato in sede di perquisizione e sequestro.

Inoltre, qualora il consulente tecnico della difesa intenda esaminare l'attrezzatura informatica, oppure partecipare ad una ispezione informatica ai sensi dell'art. 244, comma 2, c.p.p., o ancora esaminare strumentazione già oggetto di ispezione, qualora non sia intervenuto alla stessa, dovrà attendere l'autorizzazione del pubblico ministero (art. 233, comma 1-*bis*, c.p.p.). Facile prevedere che quest'ultimo spesso rifiuterà; e in attesa della decisione del giudice sollecitato con opposizione, o addirittura della Corte di cassazione qualora anche il giudice per le indagini preliminari abbia respinto la richiesta (art. 127, comma 7, c.p.p.), i tempi si allungheranno ancora. E si è avuto modo di chiarire come il fattore-tempo rappresenti una variabile decisiva rispetto al volatile dato digitale.

In secondo luogo, tra accusa e difesa permane una irrimediabile disparità: mentre gli inquirenti hanno la possibilità di disporre innumerevoli accertamenti, avendo alle spalle la macchina statale e le sue disponibilità finanziarie, la difesa dovrà, inevitabilmente, fare i conti con fondi limitati. Deve, infatti, tenersi a mente che, a causa della loro particolare difficoltà e all'impegno richiesto, le attività informatiche compiute dal consulente comportano un esborso economico notevole per l'indagato[102].

---

[101] Cfr. A.E. RICCI, Digital evidence*, sapere tecnico-scientifico e verità giudiziale*, cit., p. 360, la quale adombra il timore, in capo agli inquirenti, che le attività espletate dalla difesa «si traducano in un'improvvida modifica del dato digitale e si verifichino così alterazioni dello stato dei luoghi o delle cose».

[102] Cfr. P. GUALTIERI, *Prova informatica e diritto di difesa*, cit., p. 72. Sottolinea come il pubblico ministero si avvalga di «strutture investigative e strumentazioni tra le più sofisticate e all'avanguardia e del personale più qualificato, mentre [al difensore] è preclusa la possibilità di disporre di risorse analoghe» A.E. RICCI, Digital evidence*, sapere tecnico-scientifico e verità giudiziale*, cit., p. 359.

A dispetto dell'importanza di un diretto rapporto fra difesa e attrezzatura informatica già nella fase investigativa, deve rilevarsi, dunque, come quanto finora osservato porti ad escludere che il difensore riesca ad assumere un ruolo attivo, quantomeno nella prima fase del procedimento. Più probabile, invece, che egli debba «limitarsi ad una azione di critica e contrasto alle iniziative degli organi pubblici di investigazione»[103].

L'unica arma a disposizione della difesa resta, insomma, la nomina di un proprio esperto in contrapposizione al consulente tecnico nominato dal pubblico ministero ai sensi dell'art. 359 c.p.p.[104].

L'attività dell'esperto nominato dalla difesa potrà, invero, condurre all'emersione di una prova d'alibi idonea a minare l'intero impianto accusatorio; e ciò, anche in ipotesi criminose estranee ai *computer crimes*. La mente corre al recente caso di cronaca giudiziaria ove proprio l'analisi forense di un *computer* ha dimostrato che, nell'arco temporale nel quale si era svolto un omicidio[105], l'indagato si trovava nella propria abitazione a lavorare alla tesi di laurea[106].

Non solo. In alcuni casi, una analisi dell'attrezzatura informatica in fase d'indagine è essenziale al fine di sostenere, fin dall'inizio del procedimento, che la macchina identificata quale sorgente dell'azione criminosa fosse infettata da *virus*, *trojan* o altro *malware* tali da creare una *backdoor*[107]. In tal modo, sarebbe difficile

---

[103] Così P. GUALTIERI, *Prova informatica e diritto di difesa*, cit., p. 72.

[104] In alternativa, resterebbe unicamente la possibilità di una mera sollecitazione al pubblico ministero a svolgere ulteriori accertamenti sul dato, anche per mezzo dei suoi consulenti, ai sensi dell'art. 415-*bis*, comma 3, c.p.p. È lecito, tuttavia, dubitare dell'efficacia, nell'ambito di una indagine su materiale informatico, di tale strumento, giacché il materiale probatorio rischia di essersi già formato all'inizio delle indagini – di pari passo con il convincimento del magistrato – e, per di più, non vi è sanzione alcuna in capo alla parte pubblica qualora la richiesta venga ignorata. Cfr., a tal proposito, G. PIERRO, *op. cit.*, p. 1518, nonché S. ATERNO, *In materia di sequestro di hd e acquisizione della prova informatica: un caso eclatante*, in *Dir. internet*, 2007, p. 368.

[105] L'importanza della *timeline* è evidenziata da G. NICOSIA-D.E. CACCAVELLA, *Indagini della difesa e alibi informatico: utilizzo di nuove metodiche investigative, problemi applicativi ed introduzione nel giudizio*, in *Dir. internet*, 2007, p. 520 ss.

[106] Il riferimento è alla già citata vicenda di Garlasco, conclusasi in primo grado con la sentenza del Tribunale Vigevano, 17 dicembre 2009, Stasi. Con particolare riferimento all'alibi informatico di Alberto Stasi, v. G. VACIAGO, *op. cit.*, pp. 21-22.

[107] Si tratta di una "porta di servizio" che permette l'ingresso nel sistema ad un soggetto terzo, che può utilizzare l'attrezzatura "bucata" in numerosi modi. La tesi difensiva che mira ad attribuire l'azione criminosa ad un programma nocivo al sistema informatico viene definita *malware defense*. In proposito, v. Cass., Sez. III, 8 marzo 2012, n. 9210, *inedita*. In tale ipotesi, la Corte ha rigettato la tesi difensiva che attribuiva lo scaricamento di immagini proibite all'azione di un *virus*, poiché di quest'ultimo non erano stati indicati «nome, tipologia, modalità di funzionamento o altri dati idonei a consentire una qualsiasi valutazione». Cfr., altresì, Cass., Sez. V, 23 ottobre 2013, n. 43351, *inedita*. G. VACIAGO, *op. cit.*, p. 14, riferisce del "caso

superare il ragionevole dubbio che le azioni criminose siano state compiute da un terzo ignoto che ha utilizzato in maniera occulta il *computer* dell'indagato.

Dai rilievi che precedono emerge con chiarezza l'importanza assunta dal consulente tecnico della difesa nell'ambito delle indagini informatiche. Ruolo altrettanto centrale viene assunto dal consulente tecnico del pubblico ministero.

Come noto, in generale, la pubblica accusa, qualora debba procedere ad un'operazione tecnica per cui siano necessarie specifiche competenze, può avvalersi di consulenti, i quali possono essere, altresì, autorizzati ad assistere a singoli atti di indagine (art. 359 c.p.p.).

Ebbene, con specifico riguardo alle indagini in ambiente digitale, il consulente tecnico orienta in maniera decisiva l'attività del pubblico ministero. Quest'ultimo, infatti, non ha alcun contatto diretto con l'attrezzatura informatica da analizzare; l'intera opera di reperimento del dato digitale viene svolta dall'esperto, il quale gode di significativi margini di operatività quanto alla scelta dell'attrezzatura da utilizzare per le operazioni tecniche da realizzare nonché, in taluni casi, persino rispetto al materiale da rinvenire.

Si pensi, a titolo d'esempio, a quelle ipotesi in cui al consulente tecnico viene chiesto di individuare immagini pedopornografiche contenute in un *personal computer*. Egli, dapprima, sceglierà le partizioni del sistema da sottoporre ad analisi; successivamente isolerà alcuni *file* a suo parere sospetti, in base al nome[108] e alla tipologia. Qualora siano presenti, all'interno dell'*hard-disk*, immagini a contenuto pornografico, egli selezionerà, tra di esse, quelle raffiguranti – in ipotesi e secondo la sua valutazione – soggetti di minore età[109].

Amero", giovane insegnante finita sotto processo, negli Stati Uniti, per aver mostrato agli alunni immagini pornografiche. Una consulenza tecnica disposta dalla difesa aveva verificato che il *computer* utilizzato in classe dalla donna era stato infettato da programmi *adaware* che provocavano l'apparizione, ad intervalli regolari, a mezzo *pop-up*, di pubblicità a sfondo pornografico, naturalmente all'insaputa dell'utilizzatrice.

[108] In determinati casi, il pubblico ministero potrebbe indicare al consulente alcune parole-chiave da cercare all'interno della strumentazione informatica; ciò, soprattutto, in ipotesi di accertamento di reati associativi, laddove l'attività investigativa abbia fatto emergere l'utilizzo di nomignoli o di peculiari espressioni in codice tra gli associati.

[109] Interessante, sul punto, Cass., Sez. III, 13 luglio 2009, n. 28524, in *C.E.D. Cass.,* rv. 244594. Il Procuratore generale presso la Corte d'appello di Trento aveva impugnato una sentenza di condanna per il reato di cui all'art. 600-*ter*, comma 3, c.p., sostenendo, tra l'altro, che il consulente tecnico informatico che aveva analizzato i supporti non avesse le conoscenze per stabilire che le immagini raffigurate nei *file* rinvenuti nell'*hard disk* dell'indagato riguardassero effettivamente soggetti di minore età. Il motivo di

Già queste poche considerazioni delineano con chiarezza il rischio di una «deriva tecnicista»[110] delle indagini preliminari. Se i più attenti commentatori avevano evidenziato il pericolo che il «servitore apparente» del processo, ne divenisse «segreto padrone»[111], adombrando «supini appiattimenti sull'*ipse dixit* dell'esperto»[112] con riferimento alla valutazione della prova ad opera del giudice, tale rischio pare ora presentarsi con rinnovato vigore in riferimento alla fase delle indagini ed al rapporto tra consulente tecnico di parte e pubblica accusa.

Non solo. Un'ulteriore osservazione fa emergere ancor di più la delicatezza del ruolo dell'esperto. Qualora il dato digitale venga inquinato in fase d'indagine, sarà impossibile per il consulente tecnico nominato dalla difesa ai sensi dell'art. 233 c.p.p., una volta arrivati nella fase dibattimentale, reperire il dato originario. Di tal ché, il contraddittorio sulla prova si ridurrà ad un «mero esercizio di dialettica su materiali […] già "preconfezionati" in sede di indagini preliminari»[113], avente ad oggetto, precipuamente, il metodo utilizzato dall'esperto per l'estrazione o per l'analisi del dato.

Ad amplificare il problema, l'orientamento costante dei giudici di legittimità secondo cui la perizia è mezzo di prova neutro e sottratto alla disponibilità delle parti[114]. Il giudice, dunque, ben può ritenere sufficiente il contributo informativo offerto dal consulente tecnico dell'accusa, non essendo obbligato a nominare un proprio esperto; la difesa non potrà lamentare la mancata assunzione di una prova decisiva in sede di impugnazione, poiché il carattere di decisività si scontra con la rilevata discrezionalità del mezzo di prova in parola[115].

---

gravame è stato disatteso dai giudici di legittimità, poiché «le incertezze potevano sorgere per soggetti non ancora maggiorenni ma prossimi al compimento della maggiore età, ma non per soggetti impuberi».

[110] L'espressione, riferita dall'Autore più in generale al processo penale, è di L. LUPARIA, *La disciplina processuale e le garanzie difensive*, cit., p. 134 ss. Negli stessi termini, ma con riferimento alla prova scientifica, cfr. P. TONINI, *L'influenza della sentenza Franzese sul volto attuale del processo penale*, in *Dir. pen. proc.*, 2012, p. 1225 ss.

[111] Così M. R. DAMAŠKA, *Il diritto delle prove alla deriva*, trad. it., Il Mulino, Bologna, 2003, p. 208.

[112] M. R. DAMAŠKA, *op. loc. ult. cit.*

[113] Così L. LUPARIA, *La disciplina processuale e le garanzie difensive*, cit., p. 128.

[114] V., a tale proposito, C. CONTI, Iudex peritus peritorum *e ruolo degli esperti nel processo penale*, in *Dir. pen. proc.*, 2008, *Dossier prova scientifica*, p. 29 ss.

[115] Cfr., da ultimo, proprio con riferimento ad una ipotesi di perizia informatica rigettata in sede di richiesta di rinnovazione dell'istruzione dibattimentale in appello, Cass., Sez. V, 23 ottobre 2013, n. 43351, *inedita*. Nella prassi, il mezzo di prova della perizia è stato impiegato quale strumento di risoluzione di conflitti insorti tra ricostruzioni inconciliabili ad opera dei consulenti tecnici delle parti. Costituisce un esempio di ciò quanto avvenuto in relazione al già citato processo per i fatti di Garlasco, ove il Giudice dell'udienza

La scienza impiegata dal consulente tecnico informatico prende il nome di *computer forensics*, vale a dire quel settore di ricerca che studia «le problematiche tecniche e giuridiche correlate alle investigazioni sui dati digitali»[116].

Si tornerà in dettaglio sulla qualificazione giuridica dell'attività del consulente e, in particolare, sull'annosa questione circa la riconducibilità delle operazioni poste in essere dal tecnico agli accertamenti tecnici ripetibili di cui all'art. 359 c.p.p. o tra le attività irripetibili ai sensi dell'art. 360 c.p.p.[117]. Per il momento, pare sufficiente limitarsi a qualche annotazione generale sull'attività del *forenser*, con particolare riguardo al punto più delicato della stessa, vale a dire la scelta del *software* da utilizzare per le ricerche.

L'alternativa è tra *software* di tipo commerciale e programmi *open source*. Non è una decisione di poco conto: nonostante il funzionamento sia pressoché analogo, solo per i programmi *open source* è possibile risalire al codice sorgente, sicché solo il quest'ultimo caso il funzionamento del *software* è assoggettabile a controllo. Depone, altresì, a favore dell'utilizzo di *software open source* la possibilità di esaminare il formato dei *file* utilizzati, la facoltà per il *forenser* di accludere l'intero programma ai risultati della propria attività, nonché la disponibilità del programma per lunghi periodi di tempo[118].

---

preliminare, in sede di giudizio abbreviato, forniva incarico ad un apposito collegio peritale al fine di verificare le metodologie di accesso utilizzate dagli operanti nel corso del primo contatto con il "dato informatico". Un accertamento, questo, logicamente antecedente alla valutazione delle conclusioni delle parti ed avente a riguardo l'effettiva integrità del dato. Cfr. Tribunale di Vigevano, sent. 17 dicembre 2009, Stasi, cit.

[116] La definizione è di A. GRILLO-U.E. MOSCATO, *Riflessioni sulla prova informatica*, in *Cass. pen.*, 2011, p. 371. V. anche M. MEYERS-M. ROGERS, *Computer Forensics: The Need for Standardization and Certification*, in *2 Int. J. Dig. Evidence*, 2004, p. 4 ss.

[117] V. *infra*, cap. 3, par. 2.

[118] Cfr. A. GRILLO-U.E. MOSCATO, *op. cit.*, p. 372 ss. Gli Autori sottolineano come solo il *software Open source* risponda ai tradizionali criteri seguiti dalla giurisprudenza statunitense per l'ammissione della prova scientifica nel processo penale. Il richiamo è alla nota sentenza emessa dalla Corte Suprema degli Stati Uniti il 28 giugno 1993 all'esito del procedimento *Daubert vs Merrell Dow Pharmaceuticals* (509 US 579, 589, 1993), nella quale vennero teorizzati cinque principi come sbarramento all'ingresso della "scienza-spazzatura" all'interno del processo, da verificare ad opera del giudice, il quale assume, così, la funzione di *gatekeeper*: l'*empirical testing*, vale a dire se la teoria sia falsificabile, confutabile o testabile; se la procedura è stata sottoposta ad una *peer review*; il tasso di errore reale o potenziale; l'esistenza di *standards* o *controls* relativamente alle operazioni; il tasso di accettazione nella comunità scientifica. A seguito della sentenza, tali criteri vennero recepiti espressamente nella *Rule* 702 delle *Federal Rules of Evidence*. L'eco di tali principi è arrivato fino in Italia, ove in più occasioni sotto stati adoperati dalla giurisprudenza; per un'ipotesi recente relativa alla prova del *DNA*, v. Cass., 31 ottobre 2013, n. 44324, in *C.E.D. Cass.*, rv. 258321. In dottrina, per un'analisi sul rapporto tra *junk science* e processo, v. F. CENTONZE, *Scienza spazzatura e scienza corrotta nelle attestazioni e valutazioni dei consulenti tecnici nel processo penale*, in *Riv. dir. proc. pen.*, 2001, p. 1241 ss.

Eppure, finora, la giurisprudenza non ha prestato la dovuta attenzione alla tematica; addirittura, la Corte di Cassazione ha conferito patente di legittimità ad un'acquisizione dei dati informatici effettuata con *software* senza regolare licenza. Si è affermato, in particolare, che «l'utilizzo di un programma non licenziato per effettuare la copia dei dati informatici non [può] avere alcun riflesso sotto il profilo dell'illegittimità della prova stessa, rappresentata per l'appunto dall'*hard disk* e dal suo contenuto»[119]. Detto altrimenti, condotte scorrette – persino illecite – del consulente tecnico dell'accusa, per i giudici di legittimità, non possono trovare sanzione sul terreno dell'invalidità della prova.

[119] La curiosa affermazione si rinviene in Cass., Sez. fer., 16 novembre 2012, n. 44851, *inedita*.

Capitolo II – I mezzi di ricerca della prova digitale

1. I principi-guida nella ricerca della *digital evidence*: genuinità e non alterazione del dato informatico

Già tre anni prima della legge italiana di ratifica della Convenzione di Budapest, la dottrina statunitense si domandava se non fosse il caso di affrontare gli sconvolgimenti provocati nel sistema processuale dall'avvento della *digital evidence* con una riforma delle *rules of criminal procedure*[120]. «*New facts will demand new law*», questo l'assunto. In tale ottica, la crescita esponenziale dei *computer-related crimes* avrebbe richiesto non tanto e non solo una nuova interpretazione della normativa esistente, quanto, piuttosto, la nascita di nuovi istituti e l'introduzione di modifiche significative all'apparato esistente. Si riteneva, insomma, che una *evidence* volatile ed immateriale fosse incompatibile con le *rules* sviluppate per le *old investigations*. In particolare, si dubitava che tali disposizioni potessero ancora svolgere correttamente il fondamentale ruolo di bilanciamento tra *privacy* e *public safety*.

In ambito europeo, la Convenzione di Budapest, aperta alla firma il 23 Novembre 2001, è stato il primo accordo internazionale ad occuparsi dei crimini commessi attraverso Internet o altre reti informatiche[121]. Essa nasce, come esplicitamente affermato dal Preambolo, dalla preoccupazione che «le reti informatiche e le informazioni in formato elettronico possano anche essere utilizzate per commettere reati e che le prove connesse a tali reati possano essere conservate e trasferite tramite queste reti». Affinché gli Stati siano in grado di «combattere realmente tali reati», vengono, dunque, predisposte una serie di regole che facilitino «la loro individuazione, investigazione e l'esercizio dell'azione penale a livello sia nazionale che internazionale».

---

[120] Cfr. O.S. KERR, *Digital Evidence and the New Criminal Procedure*, cit., p. 290 ss.

[121] La struttura della Convenzione ricalca la Raccomandazione del 1995 del Consiglio dei Ministri agli Stati membri relativa ai problemi legati alla tecnologia delll'informazione. È il traguardo di un percorso lungo, le cui basi possono essere collocate nel primo studio realizzato dall'Organizzazione per la Cooperazione e lo Sviluppo economico nel 1983, passando successivamente per i principi operativi comuni stabiliti nel 1997, in sede G8, dall'H*igh Tech Subgroup of the G-8's Senior Experts on Transnational Organized Crime*.

Nell'ordinamento italiano, alla Convenzione è stata data esecuzione con ben sette anni di ritardo[122], mediante la L. 48/2008. Come la dottrina occupatasi dell'argomento ha avuto modo di chiarire, il legislatore, recependo la normativa europea, non si è limitato ad una pedissequa ripetizione delle norme ivi previste; piuttosto, «l'obbligo pattizio […] ha fornito lo spunto per mettere mano in maniera più celere ad una azione già meditata *motu proprio* da tempo»[123].

Concentrando l'attenzione sui riflessi processual-penalisitici della nuova disciplina e, precipuamente, sulle ricadute in materia di *evidence*, il legislatore ha ritoccato il lessico normativo di numerosi mezzi di ricerca della prova; ha, inoltre, ampliato le attività ad iniziativa della polizia giudiziaria e modificato il codice della *privacy*, prevedendo nuove regole per la *data retention*.

La ricognizione del *corpus* normativo risultante dalla modifica può prendere le mosse da una scelta di fondo operata dal riformatore: si modifica la fisionomia degli istituti già esistenti, affinché gli stessi possano essere utilizzati anche nell'ambito delle indagini informatiche. Basta, invero, uno sguardo d'insieme al libro III, titolo III, nonché al libro IV, titolo V del codice di procedura penale per registrare un arricchimento della disciplina ivi prevista rispetto al passato. Non viene stabilita, invece, una normativa *ad hoc* per la ricerca della *digital evidence* o per le attività urgenti di polizia giudiziaria relative al dato informatico.

Vero è che la prassi aveva già provveduto ad applicare in via analogica i tradizionali mezzi di ricerca della prova e ad estendere l'attività a iniziativa della polizia giudiziaria alla raccolta del materiale contenuto in attrezzatura informatica; sul punto, però, un intervento legislativo era quanto mai opportuno, al fine di precisare i criteri operativi ai quali gli operanti, venuti a contatto col dato informatico, avrebbero dovuto improntarsi[124].

Riallacciandosi a quest'ultimo profilo, il *leitmotiv* della nuova disciplina è così sintetizzabile: piuttosto che enucleare in dettaglio le modalità operative

---

[122] Stigmatizza il ritardo nell'adozione della normativa interna F. CAJANI, *La Convenzione di Budapest nell'insostenibile salto all'indietro del Legislatore italiano, ovvero: quello che le norme non dicono…*, cit., p. 186.

[123] Così L. LUPARIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa (L. 18 marzo 2008 n. 48). I profili processuali*, cit., p. 717.

[124] Il rilievo sistematico della L. 48/2008 è evidenziato da P. TONINI, *Documento informatico e giusto processo*, cit., p. 404 ss.

dell'intervento sul dato informatico, si stabilisce la necessità di adottare «misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione» (artt. 244, comma 2, 247, comma 1-*bis*, 352, comma 1-*bis*, 354, comma 2 c.p.p.); oppure, con maggiore precisione, si prevede che il dato debba essere trattato con una procedura che assicuri «la conformità dei dati acquisiti a quelli originali e la loro immodificabilità» (artt. 254-*bis* e, ancora, 354, comma 2, c.p.p.; nonché, con formula pressoché analoga, l'art. 260, comma 2, c.p.p.).

Vengono, in definitiva, indicati, quali canoni fondamentali per l'attività di ricerca della prova informatica, la tutela della genuinità e la non alterazione del dato. Eppure, in nessun caso si commina una sanzione esplicita per il mancato rispetto dei parametri in questione.

Si tratta, com'è chiaro, di una tecnica legislativa che demanda al singolo operatore la scelta, in concreto, del mezzo con cui realizzare le operazioni tecniche sul dato[125]. Ciò trova giustificazione, senza dubbio, nella obsolescenza degli strumenti della *computer forensics* e si spiega, verosimilmente, con la volontà del legislatore di non porre freno al progresso tecnologico in materia[126]. Eppure, un'alternativa parimenti valida poteva identificarsi nell'utilizzo della fonte regolamentare. Tale ultimo strumento è, infatti, facilmente aggiornabile, ed in più presenta il vantaggio di uniformare i protocolli di gestione del dato informatico su tutto il territorio nazionale[127]. Mentre, allo stato, tutto resta affidato alla volontà e alle conoscenze tecniche degli operanti[128].

Sotto diverso profilo, il riformatore è stato criticato, da un lato, per aver tralasciato di affrontare compiutamente i problemi più delicati delle indagini informatiche[129], dall'altro lato, per aver scelto la via dell'interpolazione, piuttosto che la predisposizione di una nuova disciplina compiutamente modellata sul

---

[125] Cfr. L. LUPARIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa (L. 18 marzo 2008 n. 48). I profili processuali*, cit., p. 719.
[126] V. M. DANIELE, *La prova digitale nel processo penale*, cit., p. 293
[127] Sull'importanza di uno *standard* investigativo comune v. M. MEYERS-M. ROGERS, *Computer forensics: the Need for Standardization and Certification*, cit., p. 1 ss.
[128] Critica sul ricorso a clausole generali è A.E. RICCI, Digital evidence, *sapere tecnico-scientifico e verità giudiziale*, cit., p. 363.
[129] L. LUPARIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa (L. 18 marzo 2008 n. 48). I profili processuali*, cit., p. 718, menziona, tra gli altri, la captazione delle comunicazioni vocali su sistemi *voice-over-IP*, nonché le intercettazioni parametriche e l'apprensione in tempo reale della posta elettronica.

fenomeno delle indagini informatiche[130]. Pare di scorgere, dietro le argomentazioni in questione, una obiezione di fondo, basata sul rilievo in base al quale le peculiari caratteristiche della *digital evidence*, immaterialità e volatilità *in primis*, mal si concilierebbero con i tradizionali strumenti codicistici[131].

A questo punto, per verificare la fondatezza di tale obiezione, s'impone un'analisi che affronti in dettaglio le singole norme modificate dalla L. 48/2008.

2. Perquisizioni ed ispezioni informatiche tra norme processuali "in bianco" e prassi

A seguito delle interpolazioni effettuate dalla L. 48/2008, l'art. 244 c.p.p. consente all'autorità giudiziaria, quando occorre accertare le tracce e gli altri effetti materiali del reato, di disporre «rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici»[132]. L'art. 247, comma 1-*bis*, c.p.p. permette, altresì, di perquisire sistemi informatici e telematici, qualora vi sia fondato motivo di ritenere che essi contengano dati, informazioni, programmi informatici o tracce comunque pertinenti al reato. In entrambi i casi, dovranno essere adottate misure tecniche in grado di assicurare la genuinità e la non alterazione del dato.

Anzitutto, pare opportuno dedicare qualche considerazione alla possibilità stessa di configurare, in astratto, un'ispezione informatica. Invero, l'ispezione è tradizionalmente ricostruita quale analisi esterna, scevra di qualsiasi apporto valutativo, di una *res*[133]. Ebbene, pare arduo configurare una «operazione tecnica»

---

[130] In questi termini ancora L. LUPARIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa (L. 18 marzo 2008 n. 48). I profili processuali*, cit., p. 719, nonché ID., *I correttivi alle distorsioni sistematiche contenute nella recente legge di ratifica della Convenzione sul* Cybercrime, cit., pp. 64-65.

[131] Così, esplicitamente, S. FASOLIN, *La copia di dati informatici nel quadro delle categorie processuali*, in *Dir. pen. proc*, 2012, p. 372.

[132] La collocazione dell'ispezione informatica nel comma 2 dell'art. 244 c.p.p. potrebbe far ritenere che tale mezzo di ricerca della prova sia esperibile soltanto qualora «il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi» (art. 244, comma 2, c.p.p.). In realtà, non pare revocabile in dubbio che, nonostante l'infelice collocazione topografica della nuova disposizione, essa debba ritenersi riferita ad ogni caso in cui occorra «accertare le tracce e gli altri effetti materiali del reato» (art. 244, comma 1, c.p.p.). V., al riguardo, L. CORDÌ, *L. 18.3.2008 n. 48 (Criminalità informatica) – Art. 8*, in *Legisl. pen.*, 2008, pp. 286-287.

[133] È noto l'insegnamento di F. CORDERO, *Procedura penale*, IX ed., Giuffrè, Milano, 2012, p. 827, secondo cui «l'*inspìciens* usa gli occhi; ai perquirenti servono le mani».

su un sistema informatico che si limiti ad una mera verifica esterna dello stesso, senza alcun accesso ai dati all'interno del sistema.

Il primo stadio della ricerca può, dunque, incentrarsi sull'indagine circa l'effettivo spazio operativo dell'art. 244 c.p.p. con riferimento a sistemi informatici e telematici. Secondo una prima esegesi ricostruttiva, che affonda le proprie radici nella prassi, sarebbe possibile, nel corso di un'ispezione, effettuare, dapprima, una copia del sistema informatico o telematico, utilizzando la tecnica della *bit stream image*[134], e, successivamente, l'elaborazione e l'analisi del dato così acquisito[135].

Se, per un verso, è lodevole l'accento posto sulla necessità di operare su un duplicato del dato, al fine di non inquinare l'elemento di prova originario, per altro verso, deve rilevarsi che tale impostazione pare fondarsi su un equivoco: considerare come oggetto dell'attività di ricerca della prova non il dato, bensì il contenitore (ad esempio, il *computer* su cui sono memorizzati i *file* di interesse investigativo). Poiché quest'ultimo non viene acquisito – viene, invero, creata solo una copia-clone del sistema –, si ritiene di operare nell'ambito dell'ispezione e al di fuori del sequestro.

In realtà, l'attività di duplicazione di dati informatici, giacché si traduce nell'ablazione di una *res*, sia pure immateriale, pare rientrare non già tra le ispezioni o le perquisizioni, quanto proprio nell'alveo del sequestro. Volendo ricercare un referente normativo per questa attività tecnica, non sembrano venire in considerazione le «misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione» degli artt. 244 e 247 c.p.p.[136], quanto, piuttosto, gli artt. 254-*bis* e 260, comma 2, c.p.p., i quali – anch'essi introdotti dalla L. 48/2008 – prevedono che il dato informatico sia duplicato «su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua

---

[134] La *bit stream image*, o copia forense, consiste in una perfetta riproduzione, *bit* per *bit*, di un qualsiasi dispositivo di riproduzione. Tale opera di clonazione riguarda tutte le aree del disco, comprese quelle che non contengono alcun *file* visibile all'utente (aree non allocate), il che permette il recupero di *file* (o porzioni di esso) cancellati.

[135] In questo senso G. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, cit., p. 196, L. CORDÌ, *op. cit.*, p. 290 ss., A. CISTERNA, *Perquisizioni in caso di fondato motivo*, in *Guida dir.*, n. 16, 2008, p. 66, nonché, anteriormente alla riforma, ID., *Esplorazioni limitate sul* computer *del cronista anche se c'è rivelazione di segreti professionali*, in *Guida dir.*, 2007, n. 31, p. 64 ss.

[136] *Contra* L. LUPARIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa (L. 18 marzo 2008 n. 48). I profili processuali*, cit., p. 719.

immodificabilità». E l'art. 254-*bis* c.p.p. esplicitamente definisce "sequestro" l'attività in questione.

A tal proposito, basti evidenziare che non sembra priva di solidità concettuale quella ricostruzione dottrinale che, prendendo atto delle modalità concrete con cui viene realizzata una perquisizione, ha evidenziato una mutazione genetica dell'istituto: se, tradizionalmente, la perquisizione costituisce l'antecedente logico e giuridico del sequestro, quella informatica «si presta a essere eseguita non prima ma dopo il sequestro» dell'apparecchiatura o del dato[137]. Invero, dapprima si sequestra, come già chiarito, il dato informatico mediante copia forense dell'intero sistema, o addirittura mediante sequestro "fisico" dell'*hard disk*; in seguito si scruta all'interno del medesimo alla ricerca dei dati utili all'indagine[138].

Viene, a questo punto, in considerazione quella diversa linea interpretativa secondo cui l'attività ispettiva avente ad oggetto un sistema informatico dovrebbe essere limitata ad un'osservazione del medesimo. In particolare, si potrebbe, in tale sede, segnalare «la presenza di periferiche collegate o scollegate, […] [oppure] di particolari sistemi *hardware* o *software* o l'utilizzo e la presenza di sistemi particolari di connessione o di supporti informatici di pertinenza»[139].

Tuttavia, si profila subito un'obiezione: tale ricostruzione mal si accorda con l'imposizione di adottare misure tecniche finalizzate alla conservazione e alla non modificazione del dato. Tale inciso, infatti, sembra adombrare una condotta attiva degli operanti sulla strumentazione.

Il punto di partenza per la risoluzione del problema pare offerto da una lettura combinata degli artt. 244, comma 2, e 247, comma 1-*bis* c.p.p. In particolare, è utile notare che, mentre l'art. 244, comma 2, c.p.p. fa generico riferimento, quale oggetto dell'attività ispettiva, a «sistemi informatici o telematici», con riferimento

---

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

[138] Sulle peculiarità delle perquisizioni informatiche, nella prospettiva nordamericana, v. L.R. ROBINTON, *Courting Chaos: Conflicting Guidance from Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Data*, in *12 Yale J. L.*, 2010, p. 311 ss.; O. KERR, Ex Ante *Regulation of Computer Search and Seizure*, in *96 Va. L. Rev.*, 2010, p. 1241 ss.; ID., *Search Warrants in an Era of Digital Evidence*, in *75 Miss. L. J.*, 2005, 85 ss.; ID., *Searches and Seizures in a Digital World*, in *119 Harv. L. Rev.*, 2005, p. 531 ss.

[139] In questi termini S. ATERNO, *Art. 8. Modifiche al titolo III del libro terzo del codice di procedura penale*, in G. CORASANITI-G. CORRIAS LUCENTE, Cybercrime*, responsabilità degli enti e prova digitale. Commento alla Legge 18 marzo 2008, n. 48*, Cedam, Padova, 2009, p. 206.

alla perquisizione informatica, l'art. 247, comma 1-*bis*, c.p.p. fa espresso riferimento ai «dati, informazioni, programmi informatici o tracce comunque pertinenti al reato» localizzati all'interno dei sistemi in questione[140].

Si può, quindi, in via di prima approssimazione, abbozzare la seguente conclusione: qualora occorra accertare le tracce o gli altri effetti materiali del reato, si può procedere ad un'ispezione – sia dell'esterno (involucro) sia dell'interno (*software* in uso) – di un sistema informatico o telematico, e, in particolare, alla descrizione dello stato dell'apparecchiatura, inclusa l'eventuale presenza di periferiche collegate al sistema, fino alla verifica dei processi in corso; ma oltre tale *step* gli operanti non possono procedere. Naturalmente, tali attività devono essere effettuate mediante l'ausilio di *software write-blocker*, per evitare che il dato venga modificato: si giustifica, così, l'inciso di cui alla parte finale dell'art. 244, comma 2, c.p.p.

L'attività degli inquirenti in sede di perquisizione, invece, può spingersi oltre: essi possono compiere operazioni sui dati contenuti nell'apparecchiatura, quale l'apertura di cartelle e programmi[141]; anche in questo caso, come imposto dall'art. 247, comma 1-*bis*, c.p.p., le operazioni devono essere realizzate mediante l'ausilio di strumentazione utile ad impedire l'alterazione del dato[142]. Inoltre, com'è ovvio, tali operazioni debbono essere ineludibilmente finalizzate alla ricerca del corpo del reato o, comunque, di tracce pertinenti al reato.

Deve, tuttavia, riconoscersi che, così ricostruiti i due istituti, il confine tra loro appare assai labile[143].

---

[140] Cfr. P. PERRI, Computer forensics *(Indagini informatiche)*, cit., p. 104.

[141] Cfr. G. BONO, *Illegittimità dei provvedimenti di perquisizione e sequestro delle credenziali di accesso al sistema di prenotazione di voli aerei* on line, in *Cass. pen.*, 2013, pp. 1529-1530.

[142] *Contra* L. CORDÌ, *op. cit.*, p. 291, per cui il significato degli incisi relativi alla tutela della genuinità del dato muta secondo la natura dell'istituto: nel caso dell'art. 244, comma 2, c.p.p. le misure servono «in ragione della duplicazione ed a presidio dell'autenticità della stessa»; nel caso dell'art. 247, comma 2, c.p.p. le misure conservative sono strumentali al successivo sequestro. Per A. VITALE, *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico*, in *Dir. internet*, 2008, p. 508, l'imposizione, da parte del legislatore, dell'obbligo di adottare misure conservative esplicita «la regola per cui le ispezioni e le perquisizioni (cioè atti, normalmente, irripetibili) concernenti supporti informatici o telematici vanno sempre rese attività ripetibili in futuro; naturalmente, ciò è realizzabile solo se si agisce in una dimensione digitale, giacché, nel mondo reale, l'irripetibile non può artificiosamente essere reso ripetibile».

[143] Il confine tra i due istituti appare ancor meno distinto qualora l'attività investigativa abbia ad oggetto un sistema di *cloud computing*. Come è stato esattamente osservato, infatti, in simile ipotesi, «un'attività invasiva di accesso interno al sistema e di utilizzo degli strumenti informatici potrebbe provocare

A ben vedere, il problema è a monte: vale a dire, nella scelta di fondo operata dalla L. 48/2008. I più attenti commentatori hanno avvertito come l'intervento riformatore abbia «implicitamente ripudiat[o] la visione […] secondo cui perquisizioni e ispezioni non sarebbero istituti idonei allo svolgimento di azioni di *digital investigation* incidenti in via diretta sul contenuto dei sistemi informatici, quanto piuttosto strumenti procedurali da confinare alla sola ricerca dell'involucro "esterno" racchiudente i dati elettronici»[144]. Mentre l'analisi del dato dovrebbe avvenire mediante i tradizionali strumenti degli accertamenti tecnici di cui agli artt. 359-360 c.p.p.

Eppure, sono evidenti i vantaggi di un siffatto impianto: da un lato, si evitano storture quali la figura ibrida dell'inquirente/esperto; dall'altro, limitando l'attività sul dato ad una fase successiva – oppure, ad un intervento diretto dell'esperto per la creazione della copia forense – si aggira il problema dell'inquinamento involontario della prova per mano di operanti non in possesso delle conoscenze tecniche sufficienti.

Al contrario, l'intervento di chirurgia lessicale operato dal riformatore, rimodellando istituti evidentemente commisurati ad una realtà fisica al fine di adattarli ad una realtà digitale, ha inevitabilmente finito per creare discrasie interne al sistema, quale, appunto, la sovrapposizione di istituti come l'ispezione e la perquisizione[145].

---

un'alterazione del sistema stesso o dei dati ed una modifica dei *file* o del loro contenuto (soprattutto se il *file* o la "cartella" vengono aperti). In questo caso, il sistema, se stimolato da una operazione anche semplice come il *click* del *mouse*, autonomamente effettua una serie di operazioni in grado di modificare informazioni interne al sistema stesso. Ciò potrebbe porre in essere un'attività contrastante con il nuovo disposto dell'art. 244 c.p.p. che stabilisce la necessità di adottare misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. L'attività posta in essere in questo caso sembra andare oltre il semplice "sguardo esplorante" tipico dell'ispezione. Tale attività sembra andare oltre il semplice scrutamento del contenuto, delle forme, delle qualità e caratteristiche del mezzo per giungere invece ad una attività più vicina a quella tipica di perquisizione». Così S. ATERNO-M. MATTIUCCI, Cloud forensics *e nuove frontiere delle indagini informatiche nel processo penale*, cit., p. 876.

[144] Così, lucidamente, L. LUPARIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa (L. 18 marzo 2008 n. 48)*, cit., p. 719.

[145] Neppure può ritenersi che il riformatore fosse vincolato, nelle proprie scelte, dalla normativa pattizia. È appena il caso di ricordare, in proposito, che – del tutto comprensibilmente – la Convenzione non prevedeva affatto ipotesi di ispezione informatica, limitandosi, all'art. 19, a teorizzare la necessità di misure legislative per consentire di «perquisire o accedere in modo simile: *a)* ad un sistema informatico o parte di esso e ai dati informatici ivi immagazzinati […]».

Tale sovrapposizione si accentua nella prassi, ove ispezione e perquisizione vengono compiute con le medesime modalità operative[146]. In entrambi i casi, come accennato, si realizza un duplicato del sistema informatico o telematico (copia forense). Creato, quindi, un ulteriore duplicato, su quest'ultimo vengono svolte le opportune operazioni tecniche.

Riallacciandosi a tale ultima osservazione, emerge un altro profilo degno di nota. Gli inquirenti, attraverso la copia forense dell'*hard disk*, reperiscono una quantità enorme di dati. Più in dettaglio, con la duplicazione del dato, gli operanti entrano in possesso della totalità dei dati contenuti all'interno dell'elaboratore, compresi dati cancellati ai quali nemmeno l'utilizzatore potrebbe – senza una strumentazione complessa – risalire. Appare, dunque, assai concreto il rischio che il mezzo di ricerca della prova si trasformi in un indebito strumento di reperimento di diverse notizie di reato[147].

Come antidoto a simili abusi, la giurisprudenza ha da tempo chiarito che il decreto di perquisizione dei dati contenuti in un *personal computer* deve individuare, almeno nelle linee essenziali, gli oggetti da ricercare con riferimento a determinate attività illecite, sì da consentire che il mezzo di ricerca della prova trovi giustificazione in fatti addebitati ad un determinato soggetto e non sia eseguito sulla scorta di semplici congetture[148].

Assunto certamente condivisibile, ma non risolutivo. Solo talvolta il reperimento di notizie di reato è causato da una scorretta attività consapevole degli inquirenti; spesso, invece, ciò è frutto di rinvenimenti casuali in corso d'indagine, eventualità resa ancor più probabile dalla grande quantità di informazioni conservate su apparecchiatura informatica. Sul punto, si registra un vuoto normativo; per limitare la possibilità di abusi, appare condivisibile la proposta di

---

[146] Lo riferisce G. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, cit., p. 196.

[147] Cfr. P.P. PAULESU, *Notizia di reato e scenari investigativi complessi: contrasto alla criminalità organizzata, operazioni «sotto copertura», captazione di dati digitali*, in *Riv. dir. proc.*, 2010, pp. 801-802; nella dottrina nordamericana v., altresì, S. TREPEL, *Digital Searches, General Warrants, and the Case for the Courts*, in *10 Yale J. L. & Tech.*, 2007, p. 120 ss.

[148] In questi termini, proprio con riferimento ad un'ipotesi di indagini "esplorative" su un *personal computer*, Cass., Sez. I, 4 luglio 2007, P.M. in proc. Pomarici, in *Dir. internet*, 2007, p. 585 ss. Cfr. le osservazioni di E. APRILE, *Sequestro del* computer *di un giornalista, clonazione della relativa memoria e tutela del segreto professionale*, in *Dir. internet*, 2007, p. 587 ss.

disciplinare compiutamente in via normativa il sequestro di tali risultanze sulla falsariga di quanto già avvenuto in altri ordinamenti[149].

Onde evitare perquisizioni "esplorative", si è prospettata, altresì, la necessità di un più frequente utilizzo dell'istituto previsto dall'art. 248 c.p.p.[150]. Secondo tale impostazione, la parte pubblica, nel corso di una indagine informatica, dovrebbe rivolgere una richiesta di consegna alla parte privata, e solo in caso di rifiuto ad opera di quest'ultima gli operanti sarebbero giustificati a procedere a perquisizione.

Anche quest'ultima disposizione è stata oggetto di modifica ad opera della L. 48/2008. Segnatamente, il riformatore ha ampliato l'oggetto della richiesta di consegna presso le banche. Per rintracciare le cose da sottoporre a sequestro, o per accertare altre circostanze utili a fini investigativi, gli operanti possono esaminare, oltre a atti, documenti e corrispondenza, anche dati, informazioni e programmi informatici (art. 248, comma 2, c.p.p.).

Deve recisamente escludersi che il riferimento alle "banche" nella suddetta disposizione intenda richiamare le banche dati presso qualsiasi struttura, pubblica o privata. Tale peculiare interpretazione era stata propugnata da una Procura della Repubblica, al fine di giustificare una richiesta di consegna, prima, ed un decreto di perquisizione e sequestro, poi, delle credenziali di accesso ad un sistema informatico di prenotazione di voli *on-line* di una compagnia aerea[151]. Tale decreto, nelle intenzioni della pubblica accusa, avrebbe dovuto portare all'identificazione di passeggeri sospettabili di fungere da corrieri internazionali di stupefacenti.

Com'è agevole avvertire, si tratta di un evidente caso di utilizzo di un mezzo di ricerca della prova come strumento per reperire *notitiae criminis*. Bene ha fatto, dunque, la Corte di Cassazione a censurare simile abuso[152]. Del tutto condivisibile il percorso argomentativo dei giudici di legittimità, i quali hanno rilevato come, in

---

[149] Come accade per i *Zufallsfunden* nella *StPO* tedesca: auspica l'introduzione di una disciplina analoga, per diminuire il rischio di abusi dei mezzi di ricerca della *digital evidence*, R. ORLANDI, *Questioni attuali in tema di processo penale e informatica*, cit., pp. 136-137. Il § 108 della *StPO* prevede, come riferisce l'Autore, che, non appena rinvenuta una *res* pertinente a reato diverso rispetto a quello per cui si procede, la perquisizione deve essere «bloccata dalla polizia o dal pubblico ministero, in attesa che il giudice dell'indagine preliminare (*Ermittlungsrichter*), appurato il corretto operare dell'autorità requirente, emetta più duraturo provvedimento di sequestro».

[150] V., sul punto, A. LOGLI, *Sequestro probatorio di un* personal computer. *Misure* ad explorandum *e tutela della corrispondenza elettronica*, in *Cass. pen.*, 2008, p. 2957 ss..

[151] Ne riferisce Cass., Sez. IV, 24 maggio 2012, n. 19618, in *Cass. pen.*, 2013, p. 1523 ss.

[152] V. Cass., Sez. IV, 24 maggio 2012, n. 19618, cit.

presenza di un mero sospetto di commissione di un crimine non meglio identificato, i dati informatici presenti all'interno di un sistema di prenotazione di voli non possono in alcun modo essere qualificati cose pertinenti al reato, come pure richiesto dall'art. 247, comma 1-*bis*, c.p.p.

Inoltre, la Corte ha rilevato che, nel sistema italiano, ogni qualvolta il legislatore ha inteso far riferimento ad una banca dati, si è utilizzata la dizione di sistema informatico o telematico; di tal ché, non vi sono dubbi che le banche cui si riferisce l'art. 248 c.p.p. siano esclusivamente gli istituti di credito[153].

3. Forme e modalità del sequestro di dati digitali: il vincolo pertinenziale

3.1 L'oggetto del sequestro informatico

La fondamentale problematica inerente al sequestro di materiale informatico attiene all'individuazione della *res* oggetto del provvedimento ablativo. Nel particolare contesto delle indagini digitali, la difficoltà di individuare il bene da sottrarre alla libera disponibilità di chi lo detiene traspare già dall'art. 19 della Convenzione di Budapest, ove si prevede la possibilità, per le «autorità competenti» degli Stati aderenti di «sequestrare o acquisire in modo simile un *sistema informatico* o *parte di esso* o un *supporto per la conservazione di dati informatici*» (lett. *a*), nonché di «fare e trattenere una copia di quei dati informatici» (lett. *b*).

Il nucleo della questione sta nel capire se, nell'operare un sequestro di dati digitali, si debba prelevare l'intero contenitore – e, in via subordinata, se il sequestro riguardi l'intero apparato o soltanto l'*hard disk* o di altro supporto di memorizzazione – o unicamente il dato di interesse investigativo quale un singolo *file*. Com'è agevole avvertire, al fine di fornire risposta al quesito, occorre, preliminarmente, verificare se il *personal computer* – o parte di esso – assuma la qualifica di corpo del reato o, quantomeno, di cosa pertinente al reato.

Il discorso può muovere dalle conclusioni cui è giunta parte della dottrina che si è fatta carico di procedere ad analoga verifica. Può, anzitutto, escludersi che il

[153] Cfr. G. BONO, *op. cit.*, pp. 1530-1531.

computer nella sua totalità, comprensivo dell'intera attrezzatura utilizzata (*monitor*, *mouse*, stampante, videocamera, microfono ecc.) costituisca corpo del reato o cosa pertinente al reato. Deve, infatti, distinguersi fra supporti in grado di contenere dati o programmi (ad esempio *hard disk*, supporti di memorizzazione)[154] potenzialmente rilevanti ai fini del sequestro e meri involucri del tutto inutili per le indagini (quali *tower*, *monitor* e *mouse*)[155].

Eppure, anteriormente alla L. 48/2008, erano proliferate prassi devianti concernenti l'indiscriminata apprensione di materiale informatico[156]. In particolare, quanto al *personal computer*, l'ablazione dell'intero sistema veniva giustificata richiamando, per un verso, la natura di corpo del reato o cosa pertinente al reato di quest'ultimo[157], per altro verso, l'esigenza di tutelare eventuali esigenze probatorie legate alla necessità di ricerche più approfondite sull'attrezzatura[158].

Si tratta di questioni legate a doppio filo alla natura immateriale della fonte di prova in questione; natura che mal si attaglia a disposizioni dettate con precipuo riguardo a beni dotati di una propria materialità. La mente corre all'art. 253 c.p.p., il quale fa riferimento al sequestro del «corpo del reato e delle cose pertinenti al reato necessarie per l'accertamento dei fatti». Poiché tale disposizione non è stata interessata dall'intervento riformatore, qualora si ritenga che i *file*, beni immateriali, non rientrino nella nozione di "cosa" rilevante ai sensi dell'art. 253 c.p.p., dovrebbe

---

[154] Si pensi a chiavi *USB* o cd/dvd-rom.

[155] Per A. CHELO MANCHIA, *Sequestro probatorio di* computers*: un provvedimento superato dalla tecnologia?*, in *Cass. pen.*, 2005, p. 1636, sequestrare tutto un *computer* la cui memoria contiene immagini pedopornografiche equivarrebbe a «sequestrare una cassetta di sicurezza nel momento in cui all'interno della stessa vengano rinvenute immagini dello stesso tipo stampate su carta fotografica».

[156] Ne riferisce, *ex multis*, A. MONTI, *No ai sequestri indiscriminati di* computer, in *Dir. internet*, 2007, p. 268 ss., il quale configura, ironicamente, un «"principio di precauzione": non sapendo bene con cosa si ha a che fare, meglio eccedere e prendere tutto ciò che – genericamente – ricade nella nozione di *hardware*». V. anche G. DA VALLE, *L. 18.3.2008, n. 48 (Criminalità informatica) – Art. 9*, in *Legisl. pen.*, p. 297 ss.

[157] Cfr. Cass., Sez. III, 6 novembre 2002, Maggiore, in *Guida dir.*, 2003, n. 3, p. 79, ove si afferma laconicamente, in una indagine in tema di pedopornografia *online*, che il *computer* dell'indagato, essendo stato usato per la consumazione del reato, costituisce corpo del reato «in quanto contenent[e] le immagini oscene oggetto dell'illecito acquisto o, comunque, ponendosi in plausibile rapporto di pertinenzialità con lo stesso».

[158] V. Cass., Sez. V, 14 aprile 2006, n. 13647, *inedita*. Un interessante *excursus* dei provvedimenti della giurisprudenza di merito *pre*-riforma è offerto da A. MONTI, *No ai sequestri indiscriminati di* computer, in *Dir. internet*, 2007 p. 268.

logicamente concludersi per l'impossibilità di assoggettare a sequestro i medesimi in virtù della disposizione in parola[159].

La soluzione al problema della sequestrabilità dei supporti informatici appare ancor più complessa non appena si consideri che, con riferimento ai reati commessi tramite *computer*, l'*hard disk* e gli eventuali strumenti di memorizzazione utilizzati rilevano unicamente in quanto contengono, al proprio interno, i dati, *file* o programmi utilizzati per compiere l'azione criminosa[160]. Se così è, considerare *tout court* l'intero *hard disk* corpo del reato pare una forzatura. Più appropriato qualificarlo cosa pertinente al reato[161], giacché l'apprensione del disco rigido può rivelarsi funzionale all'identificazione dell'autore di una condotta criminosa[162].

Cionondimeno, ancora oggi, per la Corte di Cassazione, il «*computer*» – si badi: senza alcuna distinzione tra *software* e *hardware* – «può costituire esso stesso il corpo di un determinato reato, allorché», ad esempio, «contiene immagini pedopornografiche, o costituire una cosa pertinente al reato allorché è comunque servito per commettere il reato o i reati ipotizzati»[163].

Pur registrando tale orientamento, sarebbe opportuno che, nel caso di indagini relative a reati comuni, laddove si ritenga che dati utili a fini probatori siano contenuti su strumentazione informatica, se i *file* sono compiutamente identificati[164], il sequestro si limiti a questi ultimi. Sarebbe, invero, ingiustamente

---

[159] Cfr. A. MONTI, *La nuova disciplina del sequestro informatico*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, cit., pp. 201-202.

[160] Se così è, non può tuttavia, potersi presumere la necessità dell'apprensione dell'*hard disk* dal mero titolo di reato. In proposito, si veda Cass., 10 marzo 2014, n. 11393, *inedita*, secondo cui, in presenza di una imputazione per fatture per operazioni inesistenti, ai sensi dell'art. 2, D. Lgs. 74/2000, giacché, di regola, la fatturazione avviene con modalità informatiche, «l'esigenza probatoria della loro apprensione è implicita nella stessa natura dello strumento informatico».

[161] La giurisprudenza ha in più occasioni chiarito come per "cosa pertinente al reato" debbano intendersi, in senso lato, «le cose che servono, anche indirettamente, ad accertare la consumazione dell'illecito, il suo autore e le circostanze del reato, con riferimento a ogni possibile legame, individuabile caso per caso, tra le cose stesse e l'accertamento dell'illecito». Così Cass., Sez. VI, 20 maggio 2007, Iannini, in *C.E.D. Cass.*, rv. 207591.

[162] L. LUPARIA, *La disciplina processuale e le garanzie difensive*, cit., pp. 202-203, ricorda come il disco rigido sia il «luogo che raccoglie le tracce dell'attività svolta attraverso l'elaboratore».

[163] Così, in maniera particolarmente *tranchant*, Cass., Sez. III, 22 febbraio 2012, n. 7025, *inedita*. In dottrina, sia pure anteriormente alla L. 48/2008, cfr. G. COSTABILE, Scena criminis, *documento informatico e formazione della prova penale*, cit., p. 534.

[164] All'identificazione si potrebbe pervenire, ad esempio, mediante perquisizione del sistema.

afflittivo un provvedimento ablativo avente ad oggetto l'intero contenuto dell'*hard disk*[165].

Si è, però, già avuto modo di osservare come, nella prassi, anche la ricerca di singoli *file* avvenga mediante asportazione fisica delle memorie[166] oppure con la realizzazione di copia forense dell'intero sistema. Tale ultimo caso, in determinate ipotesi, trova giustificazione nella circostanza che potrebbe non essere praticabile una selezione dei *file* al momento dell'acquisizione del dato, come avviene qualora gli operanti si trovino in presenza di un gran numero di *file* da esaminare o di partizioni crittografate[167].

Per compiere passi avanti nella ricerca, è opportuno, a questo punto, concentrare l'attenzione sulle operazioni tecniche per l'ablazione del dato.

La L. 48/2008, pur non avendo introdotto modifiche alla disposizione che disciplina oggetto e formalità del sequestro, ha, comunque, precisato le modalità operative del sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni (art. 254-*bis* c.p.p.). Si è, invero, precisato che l'acquisizione di dati può essere realizzata mediante «copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità».

Ora, nella suddetta formula si ravvisa un chiaro riferimento alla modalità di duplicazione *bit-stream image*. Pare, dunque, corretto qualificare quest'ultima attività quale modalità operativa per il sequestro di dati informatici[168].

Anche l'art. 260 c.p.p. prevede, con formula analoga all'art. 254-*bis* c.p.p., che la «copia»[169] avvenga su adeguati supporti mediante procedura che ne assicuri

---

[165] In questo senso P. TROISI, *Sequestro probatorio del* computer *e segreto giornalistico*, in *Dir. pen. proc.*, 2008, p. 770.

[166] Solo in alcuni casi l'ablazione dell'intero *hard disk* potrebbe trovare giustificazione nell'impossibilità di effettuare una copia forense, per l'incompatibilità tra durata delle operazioni tecniche per la creazione di quest'ultima e la necessaria celerità dell'esecuzione del mezzo di ricerca della prova in parola.

[167] Cfr. M. STRAMAGLIA, *Il sequestro di documenti informatici: quale tutela per il segreto professionale forense?*, in *Dir. inf.*, 2008, p. 837.

[168] Secondo M. STRAMAGLIA, *op. cit.*, p. 843, «l'estrazione di copia di dati informatici configura un'ipotesi di sequestro *sui generis*, in quanto consente che i dati digitali, in virtù della loro natura immateriale, permangano nella disponibilità dell'autorità giudiziaria, restando al contempo disponibili anche presso il legittimo titolare».

[169] L'utilizzo del termine «copia» al posto di «duplicato» o, perlomeno, «copia forense» appare, comunque, improprio. Come precisato dall'art. 1, d.lgs. 82/2005, per «copia informatica di documento informatico» deve intendersi «il documento informatico avente contenuto identico a quello del documento da cui è tratto su

la genuinità. La disposizione, però, rischia di ingenerare ulteriore confusione. Ad una veloce lettura, infatti, potrebbe desumersi dalla norma che dapprima gli inquirenti debbano sequestrare fisicamente l'attrezzatura informatica e, segnatamente, l'*hard disk*. Seguendo tale impostazione, si potrebbe essere indotti a concludere che solo a seguito di tale operazione si potrà realizzare una copia del dato attraverso la realizzazione di una *bit-stream image*.

Basta un rilievo, però, a denotare le carenze di simile prospettiva. Questa ricostruzione sconta quella medesima indebita confusione tra contenitore e contenuto che, di tanto in tanto, riaffiora nelle scelte legislative in tema di informatica giuridica[170]. Ciò che è oggetto di sequestro sono, in ultima analisi, i dati, le informazioni o i programmi informatici; l'*hard disk* che li racchiudeva in principio è un mero contenitore, in quanto i medesimi possono essere utilizzati su una diversa apparecchiatura[171].

Certo, i dati – a causa della loro natura immateriale – dovranno essere conservati su idonea attrezzatura; ma tale osservazione non sposta i termini della questione relativamente al vero oggetto del provvedimento ablativo. Dai rilievi sinora svolti, infatti, emerge che, una volta realizzata una copia forense di un *hard disk*, è tale documento informatico a costituire il bene oggetto di sequestro.

Impostato il discorso in questi termini, è possibile giungere a conclusioni diverse rispetto a quanto affermato dalla giurisprudenza di legittimità circa l'ammissibilità di una richiesta di riesame del provvedimento di sequestro probatorio nell'ipotesi in cui, a seguito di estrazione di copia forense dell'*hard disk*, quest'ultimo sia stato restituito al legittimo proprietario.

In particolare, si rinviene spesso, nelle sentenze dei giudici di legittimità, la tesi secondo cui, a seguito dell'estrazione di copia di documenti informatici, la richiesta di riesame avverso il provvedimento di sequestro sarebbe inammissibile

---

supporto informatico con diversa sequenza di valori binari» (lett. *i-quater*); mentre, per la miglior tutela delle esigenze di genuinità del dato informatico imposte dalla L. 48/2008, viene in rilievo il diverso concetto di «duplicato informatico», vale a dire il «documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario».

[170] Si pensi alla vecchia definizione di documento informatico di cui all'art. 491-*bis* c.p.p.

[171] Cfr. T.K. CLANCY, *The Fourth Amendment Aspects of Computer Searches and Seizures: a Perspective and a Primer*, in *Miss. L. J.*, 2005, 193 ss.

per carenza di interesse. Ciò, dal momento che il provvedimento di estrazione di copia sarebbe autonomo rispetto al sequestro, e, dunque, non impugnabile per il principio di tassatività delle impugnazioni[172].

A tale orientamento se ne contrappone un altro, decisamente minoritario, fondato su una peculiare ricostruzione dell'istituto del riesame del sequestro probatorio. Secondo tale diversa impostazione, permarrebbe, anche a seguito della restituzione dei supporti, l'interesse del soggetto che ha subito l'apprensione della *res* alla verifica che il mezzo di ricerca della prova sia stato impiegato nei casi ed entro i limiti previsti dal codice[173]. Ciò, soprattutto, laddove il soggetto cui il bene sia stato sottratto sia terzo rispetto al procedimento penale dal quale la richiesta di sequestro è originata; cosa che ben spesso accade nell'ambito delle indagini informatiche. Invero, in siffatta ipotesi, non residuerebbe al soggetto attinto dal provvedimento alcuna possibilità di sottoporre ad un controllo il provvedimento di sequestro, nonché la successiva duplicazione dei propri documenti informatici[174].

In realtà, per arrivare a sostenere la sussistenza dell'interesse ad impugnare il decreto di sequestro in capo al soggetto cui è stata sottratta e poi restituita l'attrezzatura informatica, non è necessario affrontare un *iter* argomentativo così impervio. Per risolvere la questione, difatti, appare dirimente una diversa considerazione: se l'oggetto del sequestro va correttamente rinvenuto nel documento informatico, diviene irrilevante l'avvenuto dissequestro del supporto originario. Non si tratta, infatti, di verificare *ex post* la legittimità di un sequestro ormai esaurito, quanto di controllare la sussistenza di presupposti e limiti di un provvedimento ablativo i cui effetti sono ancora in atto. Né si deve affrontare la

---

[172] Cfr., da ultima, Cass., Sez. VI, 14 aprile 2012, n. 29846, in *C.E.D. Cass.*, rv. 253251. V. anche Cass., Sez. Un., 24 aprile 2008, Tchmil, in *Cass. pen.*, 2008, p. 4031 ss., con osservazioni di E. Aprile. In dottrina, v. M. STRAMAGLIA, *op. cit.*, p. 844.

[173] In quest'ottica, per tutti, v. Cass., Sez. I, 31 maggio 2007, Sarzanini, in *Dir. inf*, 2008, p. 741. Critica sulla sussistenza di un gravame «astratto» così configurato è S. CARNEVALE, *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare*, in *Dir. pen. proc.*, 2009, p. 475. L'Autrice ricorda che «il diritto vivente ha affermato a più riprese la valenza tutta interna delle conclusioni sul *fumus commissi delicti* raggiunte in sede cautelare, insuscettibili di travalicare i confini del procedimento incidentale. […] Quand'anche la catena dei controlli sul provvedimento apprensivo conducesse ad una pronuncia della Corte di Cassazione, la quale in ipotesi riscontrasse la fragilità dell'impianto accusatorio, il procedimento principale resterebbe impermeabile a simile valutazione».

[174] V., in proposito, L. BACCHINI, *Il sequestro probatorio nei confronti del giornalista non indagato: il problema del bilanciamento di interessi costituzionalmente garantiti ed il rischio di elusione delle tutele*, in *Dir. inf.*, 2008, pp. 747-748.

vexata quaestio se la restituzione della *res* sequestrata esaurisca oppure no il vincolo di indisponibilità impresso con la misura ablativa: vale a dire, se la liberazione del *corpus mechanicum* comprenda o meno quella del *corpus mysticum*[175].

A sostegno della tesi qui accolta, sotto diverso angolo visuale, si è osservato che il mezzo d'impugnazione dovrebbe comunque ritenersi ammissibile «anche in forza del solo interesse a riottenere l'informazione in quanto tale, a prescindere dal supporto in cui era incardinata ed indipendentemente dall'esigenza di impedirne l'uso probatorio»[176]. Difatti, se, per un verso, il sequestro di dati informatici mediante la creazione di un duplicato riduce la portata afflittiva del provvedimento ablativo con riguardo alla fruizione del bene, per altro verso lede interessi di diversa natura; di tal ché, si impone un controllo finalizzato ad «impedire che i propri dati personali restino a disposizione degli inquirenti al di fuori dei casi consentiti, controllarne gli usi, verificarne la pertinenza rispetto agli scopi perseguiti, sino ad ottenerne la restituzione qualora difettino i presupposti per il loro trattenimento»[177].

Con precipuo riguardo alla restituzione dell'*hard disk*, si è, però, sostenuto che, laddove i dati contenuti all'interno del medesimo consentano all'indagato di aggravare le conseguenze del reato oppure la commissione di nuovi reati, sarebbe opportuno evitarne la riconsegna anche qualora sia stata realizzata una copia forense[178].

Ora, in primo luogo, è doveroso notare come tale *periculum* costituisca il presupposto di altro istituto rispetto al sequestro probatorio e, precisamente, del sequestro preventivo di cui all'art. 321 c.p.p. In assenza di un provvedimento del giudice che dispone la misura cautelare in parola, deve, dunque, evitarsi un'indebita sovrapposizione di due istituti diversi quanto a presupposti e finalità. Ad ogni modo, quanto al rischio di reiterazione del reato, appare sufficientemente

[175] V. Cass., Sez. Un., 24 aprile 2008, Tchmil, cit.
[176] Cfr. S. CARNEVALE, *op. cit.*, p. 480.
[177] Così, ancora, S. CARNEVALE, *op. loc. ult. cit.*, la quale riconduce tali interessi al più generale concetto di «autodeterminazione informativa» di cui all'art. 2, comma 1, del D. Lgs. 196/2003.
[178] Cfr. P. TROISI, *op. cit.*, 2008, p. 767.

rassicurante l'utilizzo di tecniche crittografiche, da parte degli operanti, al fine di impedire l'accesso a determinati *file* o programmi[179].

In secondo luogo, occorre evidenziare che gli strumenti informatici rappresentano sempre più, al giorno d'oggi, un indispensabile strumento di lavoro; senza considerare il valore affettivo dei *file* contenuti nella memoria del dispositivo sottratto. Chiaro, dunque, l'interesse di colui che può legittimamente disporne a vedersi riconsegnato al più presto il materiale sequestrato.

Né varrebbe obiettare, in contrario, che, al fine di recuperare i dati presenti nel *computer*, l'indagato potrebbe utilizzare lo strumento offerto dall'art. 258 c.p.p., il quale prevede la possibilità di estrarre copia dalle *res* oggetto di sequestro[180]. Invero, in tale ipotesi è comunque necessario il nullaosta dell'autorità giudiziaria; un eventuale diniego allungherebbe eccessivamente i tempi della riconsegna. È, dunque, manifesta l'inutilità dell'istituto qualora vi sia urgenza, ad esempio per improrogabili ragioni lavorative, di rientrare in possesso del materiale sottratto.

In realtà, ai sensi dell'art. 262 c.p.p., deve ritenersi che, non appena realizzata la copia forense dei dati di interesse investigativo o dell'intero *hard disk*, l'autorità giudiziaria debba disporre la restituzione della *res* all'avente diritto. Invero, giacché ogni successiva analisi può essere compiuta partendo dal duplicato ottenuto, il mantenimento del vincolo ablativo sul dato originale non adempie ad alcuna necessità probatoria.

Allo stato, tuttavia, è doveroso segnalare che, nella prassi, il sequestro di attrezzatura informatica si protrae, di regola, ben oltre il periodo strettamente necessario per operare l'operazione di clonazione dei dati[181]. Tale ultima operazione – è bene ricordarlo – non è prevista quale obbligatoria da alcuna norma codicistica;

---

[179] La chiave d'accesso dovrebbe, quindi, essere consegnata all'autorità giudiziaria procedente. In questo senso A. CHELO MANCHIA, *op. cit.*, pp. 1637-1638.

[180] Cfr. G. VACIAGO, *Digital evidence*, cit., p. 56. Al contrario, secondo Cass., Sez. VI, 8 agosto 2013, n. 34578, *inedita*, al cospetto di un sequestro "sovrabbondante" quando a modalità di esecuzione, l'interessato dovrebbe «chiedere la eventuale estrazione o la copiatura di *file* utili per gli inquirenti ed ottenere la restituzione dei relativi *hardware*». Com'è evidente, però, non si offrono rimedi in caso di diniego da parte degli inquirenti.

[181] Il discorso vale, com'è ovvio, nei limiti in cui il materiale sequestrato attenga ad *hard disk*, supporti di memorizzazione e altri contenitori di dati in relazione ai quali non è necessario operare diversi accertamenti su altre parti *hardware*. Le conclusioni mutano in presenza, ad esempio, di apparecchi multimediali più complessi quali apparecchi per il gioco d'azzardo modificati, sui quali potrebbe rendersi opportuna una verifica di eventuali elementi meccanici modificati; cfr., in proposito, Cass., Sez. III, 21 gennaio 2013, n. 3087, *inedita*.

di tal ché, ben può il pubblico ministero affidare l'attrezzatura sequestrata ad un consulente senza disporre, inizialmente, alcuna duplicazione del dato. Parimenti, qualora la pubblica accusa o il consulente, su incarico della Procura, scelga di operare secondo il metodo della *bit-stream image*, non vi è alcun termine da rispettare per il completamento della procedura.

Tale prassi, d'altronde, non è stata in alcun modo censurata dalla Corte di Cassazione. Invero, quest'ultima, chiamata ad intervenire in un'ipotesi di sequestro di memorie informatiche protrattosi per oltre un anno, ha ritenuto che l'indebita estensione temporale del sequestro probatorio non dà, comunque, luogo ad una violazione di legge valorizzabile di fronte ai giudici di legittimità[182]. Secondo i giudici, inoltre, la mancata indicazione di un termine di scadenza temporale del vincolo ablativo nell'art. 253 c.p.p. non comporta l'illegittimità costituzionale della disposizione per un eventuale contrasto con gli artt. 2, 3 e 42 Cost., giacché il sequestro probatorio costituisce un «provvedimento che, per la sua finalità esclusivamente probatoria, ha una necessaria ed elastica contenutezza, non aprioristicamente determinabile, pena la perdita dell'utile funzionalità dell'istituto, il quale […] attiene alla fase […] delle indagini preliminari, ed è stato predisposto al fine di dare riscontro alla *notitia criminis* e dell'eventuale raccolta degli elementi di prova»[183].

Similmente, la Corte di Cassazione ha ritenuto non illogico un diniego al dissequestro di materiale informatico, su cui era stata già espletata perizia in sede di incidente probatorio, fondato sul rilievo che avrebbe potuto essere disposta, in sede di giudizio, integrazione o rinnovazione delle operazioni tecniche in parola[184]. Ebbene, davvero non si comprende il fondamento di quanto asserito. Poiché già vi è stata una compiuta analisi del dato informatico, i casi sono due: o è stato già realizzato un perfetto duplicato dell'*hard disk*, identico in tutto e per tutto all'originale, e, dunque, non vi è ragione per mantenere sotto sequestro il contenitore; oppure, vi è stata una analisi con contestuale modifica del dato, in

[182] Cfr. Cass., Sez. VI, 11 marzo 2010, n. 10038, *inedita*. In tale sentenza, si riconosce, comunque, che «l'utilizzo di altre modalità esecutive (ad es. la clonazione, laddove praticabile) avrebbe potuto e potrebbe garantire il medesimo esito [investigativo] con minor disagio per il ricorrente».
[183] Così Cass., Sez. VI, 11 marzo 2010, n. 10038, cit.
[184] Cass., Sez. IV, 20 dicembre 2012, n. 49556, *inedita*.

contraddittorio tra le parti, ai sensi dell'art. 360 c.p.p., a seguito della quale non vi è più nulla di genuino da analizzare[185]. In entrambi i casi, il mantenimento del sequestro sull'intera attrezzatura si palesa come ingiustamente ed inutilmente afflittivo.

A ben vedere, tali decisioni si inseriscono in un più ampio filone giurisprudenziale, caratterizzato da un approccio "prudente" in base al quale è opportuno che i reperti informatici reperiti in fase d'indagine vengano mantenuti in sequestro in attesa di diverse o nuove analisi del dato nelle successive fasi o negli ulteriori gradi di giudizio; e ciò, anche laddove già sia stata realizzata copia forense dell'intero sistema[186].

Una possibile, parziale soluzione ai problemi cui si è cercato finora di dare risposta avrebbe potuto essere rappresentata dalla previsione della copia forense quale modalità *standard* di ablazione del dato, eventualmente facendo salvi casi eccezionali di incompatibilità tra simile modalità acquisitiva e la necessaria celerità dell'esecuzione del sequestro; oppure, la previsione di termini perentori entro i quali realizzare tale operazione, laddove si ritenesse inevitabile il sequestro dell'intero *hard disk*[187].

Invece, con riferimento al sequestro probatorio, il legislatore ha previsto il metodo acquisitivo della copia forense non già con riferimento al sequestro presso privati, bensì, come accennato, unicamente nella disposizione relativa all'acquisizione di dati digitali presso «fornitori di servizi informatici, telematici o

---

[185] È interessante rilevare come la casistica giurisprudenziale testimonia di un uso assai ridotto dell'incidente probatorio per lo svolgimento di una perizia sul dato informatico, fondato sul rischio di una modificazione non evitabile del dato (art. 392, lett. *f*) c.p.p.). Per un caso analogo, relativo al sequestro di un *server* informatico presso uno studio legale, v. Cass., Sez. III, 20 gennaio 2003, Manganello, in *Cass. pen.*, 2004, p. 1339.

[186] Cfr. Cass., Sez. I, 25 gennaio 2012, n. 3126, *inedita*, ove si ritiene che il mantenimento del sequestro di un intero *hard disk*, operato in fase investigativa, sia giustificato «dalla necessità di conservare in originale il supporto informatico contenente *files* ritenuti rilevanti ai fini della prova, per ulteriori eventuali verifiche in altre fasi e gradi del processo». Ancora, secondo i giudici di legittimità, la «disponibilità del computer, sequestrato e poi restituito, consentirebbe indagini e verifiche tecniche ben più affidabili, approfondite e penetranti sull'hard disk di quelle che è possibile effettuare su semplici copie del *software*». Così Cass., Sez. VI, 1 luglio 2009, Genchi, in *Cass. pen.*, 2010, p. 253 ss., con osservazioni di P. Spagnolo. Non si rinvengono, in sentenza, indici per verificare se la copia cui si accenna fosse una *bit-stream image* dell'intero *hard disk* o la copia di alcuni *file* del sistema selezionati dalla pubblica accusa.

[187] Secondo A. MONTI, *La nuova disciplina del sequestro informatico*, cit., pp. 207 ss., il «quadro di garanzia» disegnato dalle norme modificate dalla L. 48/2008 impone, comunque, al pubblico ministero, qualora «non segu[a] la via più comoda – quella della copia sicura dei dati», l'onere di «spiegare […] sia il perché non dispone la duplicazione delle informazioni, sia quali sistemi adotta per far sì che l'esito dell'acquisizione garantisca "immodificabilità", "inalterabilità" e "conformità all'originale"».

di telecomunicazioni»[188]. In tal caso, si impone a questi ultimi un onere di conservazione e di protezione dei dati originali (art. 254-*bis* c.p.p.). Non si prevede alcun termine per realizzare l'acquisizione; stante l'espressa qualificazione di "sequestro", è indubbio che il decreto sia impugnabile mediante richiesta di riesame ai sensi dell'art. 257 c.p.p.

La formulazione dell'art. 254-*bis* c.p.p. ha ingenerato alcuni dubbi interpretativi dei quali occorre farsi carico. La questione principale attiene all'ambito operativo della disposizione.

Il sequestro in parola ha per oggetto dati «di traffico o di ubicazione»[189]. La disciplina dell'acquisizione da parte degli inquirenti dei dati di traffico è, però, già disciplinata da altra disposizione, vale a dire l'art. 132, comma 1, del D. Lgs. n. 196/2003, il quale prevede che i dati relativi al traffico telematico siano conservati dal fornitore di servizi per dodici mesi dalla data della comunicazione. L'autorità giudiziaria acquisisce tali dati, entro il termine indicato, con decreto motivato del pubblico ministero; per il principio di tassatività delle impugnazioni, giacché il Codice della *privacy* tace sul punto, si ritiene che tale provvedimento acquisitivo non sia soggetto a controllo[190].

Con riferimento all'acquisizione dei dati di traffico presso i fornitori di servizi di telecomunicazioni, le due disposizioni rischiano, com'è agevole avvertire, di sovrapporsi. Sennonché, la scelta tra l'una o l'altra disciplina non è indifferente, giacché esse, come accennato, differiscono quanto a termini e controlli.

I più attenti commentatori hanno, allora, proposto una lettura in grado di ritagliare un ambito applicativo ad entrambi gli istituti. Facendo leva sulla

---

[188] A. MONTI, *La nuova disciplina del sequestro informatico*, cit., p. 212 ss., distingue diversi ruoli in capo a tali soggetti nell'ambito delle indagini a seconda delle circostanze: titolari di un mero dovere di collaborazione con l'autorità qualora i fornitori di servizi abbiano locato spazio fisico in cui l'indagato ha posizionato i *server*; destinatari diretti del provvedimento del sequestro qualora siano possessori delle risorse fisiche su cui l'indagato ha memorizzato i propri dati (*hosting*) e qualora detentori di dati rilevanti a fini investigativi.

[189] I dati di traffico sono definiti, dall'art. 4, comma 1, lett. *h*), Codice *privacy* come quei dati «sottopost[i] a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica e della relativa fatturazione, ivi compresi i dati necessari per identificare abbonato e utente»; i dati relativi all'ubicazione (art. 4, comma 1, lett. *i*), Codice *privacy*) sono quei dati trattati in una comunicazione elettronica che «indic[ano] la posizione la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico […]».

[190] *Contra* P. GUALTIERI, *Prova informatica e diritto di difesa*, in *Dir. pen. proc.*, 2008, *Dossier prova scientifica*, p. 73.

collocazione topografica dell'art. 254-*bis* c.p.p. all'interno del titolo III, capo III, del codice di rito, si è sostenuto che quest'ultima disposizione miri unicamente a chiarire le modalità operative con le quali l'ablazione del dato informatico debba essere compiuta qualora il mezzo di ricerca della prova in parola sia esperito presso fornitori di servizi informatici, telematici e di telecomunicazioni; quanto ai limiti e ai presupposti, il sequestro di dati sarebbe comunque ammesso solo nelle tradizionali ipotesi di cui agli artt. 247, comma 1-*bis*, e 253, comma 1, c.p.p.[191]. In altre parole, l'art. 254-*bis* c.p.p. disciplinerebbe il *quomodo* del sequestro di dati informatici presso i soggetti ivi indicati; l'acquisizione dei dati di traffico presso i *provider*, invece, resterebbe disciplinata, quanto a termini e modalità, da quanto previsto nel Codice *privacy*.

La correttezza di tale ricostruzione pare confermata dalla *ratio* dell'art. 254-*bis* c.p.p.: bilanciare le finalità investigative con le esigenze dei fornitori di servizi informatici, telematici e di telecomunicazioni i quali subirebbero un danno ingente sia dalla sottrazione di strumentazione informatica sia dalla perdita di dati essenziali per la fatturazione[192]. Rimangono, tuttavia, oscure le ragioni per cui la modalità di apprensione del dato mediante copia su adeguato supporto sia stata configurata quale mera facoltà per gli inquirenti[193].

Per completare il quadro, restano da identificare i «fornitori di servizi informatici, telematici e di telecomunicazioni» cui fa riferimento l'art. 254-*bis* c.p.p.; formula, questa, che appare più estesa e, dunque, non sovrapponibile a quella di fornitore di servizi di comunicazione elettronica rilevante ai sensi dell'art. 132 D. Lgs. 196/03[194]. Ebbene, la dizione normativa appare sufficientemente estesa da far

---

[191] V., per tutti, A. CISTERNA, *Perquisizioni in caso di fondato motivo*, cit., p. 66 ss.

[192] Cfr. Relazione di accompagnamento al Disegno di legge C 2807, cit. In dottrina, v. A. MACRILLÒ, *Le nuove disposizioni in tema di sequestro probatorio e di custodia ed assicurazione dei dati informatici*, in *Dir. internet*, 2008, p. 514.

[193] La norma prevede, infatti, che l'autorità giudiziaria *può* disporre che i dati informatici vengano acquisiti mediante copia, «per esigenze legate alla regolare fornitura dei medesimi servizi». È opportuno evidenziare che tali esigenze si manifesteranno nella pressoché totalità dei casi. Sarebbe stato più opportuno, dunque, configurare come obbligatorio tale sistema acquisitivo, eventualmente facendo salvi casi eccezionali, nei quali l'autorità giudiziaria avrebbe dovuto motivare il perché della mancata attivazione delle modalità operative in parola.

[194] Per servizi di comunicazione elettronica si intendono «i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei

rientrare, nell'ambito operativo dell'istituto, non soltanto coloro che forniscono quale *core business* servizi consistenti nella trasmissione di segnali su reti elettroniche, ma anche quei soggetti che forniscono tali servizi all'interno di una diversa attività d'impresa[195]. Resta inteso che i dati da sequestrare costituiscano, ai sensi dell'art. 253 c.p.p., corpo del reato o cose pertinenti al reato necessarie per l'accertamento dei fatti.

3.2 Il sequestro di corrispondenza informatica

La L. 48/2008 ha riscritto il primo comma dell'art. 254 c.p.p., estendendo l'ambito del sequestro di corrispondenza, presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni, a «lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, *anche se inoltrati per via telematica*», che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti o che possono avere relazioni con il reato[196]. Il secondo comma della disposizione prevede che, qualora al sequestro provveda un ufficiale di polizia giudiziaria, questi non possa aprire o alterare gli oggetti di corrispondenza, né prendere altrimenti conoscenza del loro contenuto; questi dovrà, invece, consegnare il tutto all'autorità giudiziaria.

La disposizione in questione suscita profondi interrogativi con particolare riguardo al suo effettivo raggio d'azione. Conviene, anzitutto, esaminare più da vicino il contenuto dell'art. 254, comma 1, c.p.p. Non vi è dubbio che la formula «oggetti di corrispondenza, anche se inoltrati per via telematica» ricomprenda i messaggi di posta elettronica[197].

---

limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002» (art. 4, comma 1, lett. *e*), Codice *privacy*).

[195] In quest'ottica, A. MONTI, *La nuova disciplina del sequestro informatico*, cit., p. 210 ss., porta ad esempio le aziende operanti nel settore del commercio elettronico, le compagnie aeree o ferroviarie che consentono prenotazioni e acquisti *online*, nonché gli istituti bancari che offrono l'operatività via *Internet* sui conti correnti. *Contra*, S. ATERNO, *Le investigazioni informatiche e l'acquisizione della prova digitale*, in *Giur. merito*, 2013, p. 966, secondo cui la norma esclude tutti i soggetti che non rientrano tra i fornitori di servizi di comunicazione.

[196] Già da una prima lettura appare evidente una stortura: arduo immaginare l'inoltro di pieghi e pacchi per via telematica. Si tratta, all'evidenza, di una conseguenza della tecnica interpolativa.

[197] Prima della riforma, si era molto discusso circa le forme e le modalità di apprensione della corrispondenza elettronica. Per tutti, v. L. LUPARIA, *La disciplina processuale e le garanzie difensive*, cit., p. 170 ss.

A prima vista, parrebbe doversi escludere che la corrispondenza elettronica già giunta a conoscenza del destinatario rientri nell'istituto. Perché si tratti di "corrispondenza", come noto, è necessario che l'*e-mail*, spedita dall'indagato o a lui diretta, sia in attesa dell'inoltro dal *server* di posta del mittente a quello del destinatario; oppure, deve essere stata da quest'ultimo ricevuta ma non ancora letta[198].

Una interpretazione rigorosa della disposizione in parola, allora, imporrebbe di configurare la possibilità di sequestrare le *e-mail* presso fornitori di servizi postali, telematici o di telecomunicazioni solo in queste due ipotesi. Quanto alla prima – vale a dire, sequestro della corrispondenza telematica localizzata presso il fornitore del servizio, antecedentemente all'invio al destinatario – essa appare ipotesi remota, considerati i termini brevissimi di smistamento[199]. L'attenzione si concentra, dunque, sulla seconda. Vengono, al riguardo, in considerazione due casi: il ricevente utilizza servizi di *web mail*, e dunque il messaggio si trova sui *server* del fornitore di servizi *mail* da lui utilizzato; oppure, adopera *software* quali *Outlook*, i quali provvedono a scaricare il messaggio sul *computer* del destinatario. In quest'ultima ipotesi, di regola, non vi è alcuna *e-mail* da apprendere sul *server*. Di qui, per esclusione, dovrebbe ritenersi che la disposizione si riferisca alle ipotesi di apprensione di messaggi non letti stazionanti sul *server*.

Si delinea, però, subito un problema: non è dato discernere con chiarezza i confini fra il sequestro di corrispondenza elettronica di cui all'art. 254, comma 1, c.p.p., così ricostruito, e l'istituto delle intercettazioni telematiche, di cui all'art. 266-*bis* c.p.p.

Il dubbio sussiste giacché le *e-mail* rientrano senz'altro nel «flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrenti tra più sistemi»[200]. Si è adombrato, allora, il rischio che l'art. 266-*bis* c.p.p. venga, nella

---

[198] Invero, allorquando il destinatario della *e-mail* ha preso conoscenza del contenuto del messaggio, questo non è più corrispondenza, difettando del requisito dell'attualità. Cfr. C. PECORELLA, *Diritto penale dell'informatica*, Cedam, Padova, 2006, p. 294.

[199] In questo senso A. MACRILLÒ, *op. cit.*, pp. 512-513. L'Autore ipotizza, inoltre, che il riformatore, nel modificare l'art. 254 c.p.p., avesse in mente quel determinato servizio, offerto dagli uffici postali, per cui il mittente inoltra la corrispondenza a mezzo *mail* all'ufficio, il quale stampa quando ricevuto in formato cartaceo per poi procedere all'invio.

[200] A conferma di quanto esposto, anteriormente alla L. 48/2008, un'attenta dottrina riconduceva l'acquisizione dei messaggi non letti all'art. 266-*bis* c.p.p. Cfr. R. ORLANDI, *op. cit.*, p. 134.

prassi, soppiantato dall'art. 254 c.p.p., non essendo necessaria, per l'attivazione di quest'ultimo, a differenza di quanto richiesto per le intercettazioni telematiche, la gravità indiziaria, né l'indispensabilità ai fini della prosecuzione delle indagini, né l'autorizzazione del giudice per le indagini preliminari[201].

Se così è, onde evitare perniciose sovrapposizioni tra i due istituti e, soprattutto, indebiti aggiramenti delle garanzie difensive[202], appare necessario intendere in senso lato la nozione di "corrispondenza" accolta dall'art. 254 c.p.p.: vale a dire, includere nell'ambito applicativo della norma l'apprensione di tutte le *e-mail*, lette e non, già pervenute all'indirizzo *e-mail* del ricevente – e, quindi, non facenti parte di un "flusso" telematico rilevante ai sensi dell'art. 266-*bis* c.p.p. – ma ancora presenti, per qualsiasi ragione[203], sul *server* di posta del destinatario.

Con riferimento a quest'ultimo profilo, poiché spesso non vi è modo di verificare con certezza se i messaggi siano effettivamente giunti a conoscenza del destinatario, sembra opportuno che tutti i messaggi ivi contenuti siano appresi secondo le regole di cui all'art. 254 c.p.p. La disposizione così, rappresenterebbe un fronte di tutela avanzato per la corrispondenza elettronica rispetto alle ordinarie regole in tema di sequestro, la cui vera parte cogente si ravvisa nella misura in cui essa impedisce alla polizia giudiziaria di prendere cognizione del contenuto dei messaggi. Naturalmente, l'apprensione del dato dovrà essere operata con le modalità delineate dall'art. 254-*bis* c.p.p.[204].

Quanto alla captazione dei flussi informatici, *e-mail* incluse, in transito dal destinatario al mittente, dovrà, invece, applicarsi la più garantita disciplina prevista in tema di intercettazioni telematiche.

---

[201] Cfr. L. CORDÌ, *op. cit.*, p. 293.
[202] Per una indagine su apprensione di *e-mail* a fini investigativi e garanzie individuali nel sistema nordamericano, cfr. P.L. BELLIA-S. FREIWALD, *Fourth Amendment Protection for Stored E-mail*, in *41 U.S.F. L. Rev.*, 2006-2007, p. 559.
[203] Come, appunto, l'utilizzo di un servizio *web mail* cui si accennava poco sopra.
[204] Sottolinea questo aspetto L. MARAFIOTI, Digital evidence *e processo penale*, cit., p. 4515.

4. L'apprensione di dati in tempo reale: intercettazioni telematiche e perquisizioni *online*

4.1 Le intercettazioni telematiche nell'ordinamento italiano

La ricerca della prova digitale in fase investigativa può vertere, oltre che su materiale già formato contenuto all'interno di attrezzatura informatica, anche su flussi di dati in transito tra più sistemi informatici o telematici[205].

Viene in rilievo, a tal proposito, l'art. 266-*bis* c.p.p., introdotto dalla L. 547/1993[206], il quale consente, «nei procedimenti relativi ai reati indicati nell'articolo 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche», l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici, nonché quello intercorrente tra più sistemi[207].

---

[205] Cfr., al riguardo, G. DI PAOLO, voce *Prova informatica*, in *Enciclopedia del diritto. Annali*, VI, Giuffrè, Milano, 2013, p. 743 ss.

[206] Legge 23 dicembre 1993, n. 547, *Modifiche ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*, pubblicata in *G.U.*, 30 dicembre 1993, n. 305.

[207] Le intercettazioni telematiche di cui all'art. 266-*bis* c.p.p. vanno tenute ben distinte dalle intercettazioni preventive per via telematica di cui all'art. 226 disp. att. c.p.p. Tale strumento, introdotto dal D.L. 18 ottobre 2001, n. 374, convertito, con modificazioni, nella L. 15 dicembre 2001, n. 438, attivabile dal Ministero dell'interno, dai responsabili dei servizi centrali della Polizia di Stato, dei Carabinieri e della Guardia di finanza nonché dal questore o dal comandante provinciale dei Carabinieri e della Guardia di finanza, con richiesta da sottoporre al procuratore della Repubblica presso il Tribunale del capoluogo del distretto in cui si trova il soggetto da sottoporre a controllo o in cui sono sorte le esigenze di prevenzione, si sostanzia anch'esso in una captazione di comunicazioni o conversazioni per via telematica (art. 226, comma 1, disp. att. c.p.p.), nonché nel tracciamento delle medesime ovvero nell'acquisizione dei dati esterni relativi alle comunicazioni telematiche e «di ogni altra informazione utile in possesso degli operatori di telecomunicazioni» (art. 226, comma 4, disp. att. c.p.p.). Perché l'autorizzazione possa essere disposta, il controllo preventivo deve essere necessario per l'acquisizione di notizie concernenti la prevenzione di delitti di cui agli artt. 407, comma 2, lett. *a*) n. 4 e 51, comma 3-*bis*, c.p.p. L'attività intercettiva si colloca, in questa peculiare ipotesi, in una fase precedente all'avvio del procedimento penale. Vige il divieto di utilizzo degli elementi acquisiti nel procedimento penale, «fatti salvi i fini investigativi»; dell'attività in parola non può, comunque, farsi menzione in atti di indagine, né essa può costituire oggetto di deposizione o essere altrimenti divulgata (art. 226, comma 5, disp. att. c.p.p.). In dottrina, circa «la singolarità di una captazione di comunicazioni segrete non […] giustificata dalla commissione di un reato, bensì da meri sospetti di polizia circa la potenziale criminosità di certi comportamenti del soggetto», v. L. LUPARIA, *La disciplina processuale e le garanzie difensive*, cit., p. 167 ss. Di intercettazioni telematiche preventive si occupa anche l'art. 25-*ter* della L. 356/1992, come modificato, sul punto, dalla L. 547/1993. Ai sensi di tale ultima disposizione, la captazione di flussi informatici può essere autorizzata dal Procuratore della Repubblica presso il Tribunale del capoluogo del distretto ove le operazioni devono essere eseguite, su richiesta del Ministero dell'interno (o, per sua delega, dal direttore della Direzione investigativa antimafia), dai responsabili a livello centrale dei servizi centrali e interprovinciali della Polizia di Stato, dei Carabinieri e della Guardia di finanza nonché dal questore, qualora le intercettazioni siano necessarie per l'attività di prevenzione e di informazione in ordine ai delitti di cui all'art. 51, comma 3-*bis*, c.p.p. Anche in tale ipotesi gli elementi acquisiti sono privi di qualsiasi valore a fini processuali. Al riguardo, v. C. PARODI, *La disciplina delle intercettazioni telematiche*, in *Dir. pen. proc.*, 2003, p. 892.

Com'è agevole notare, le intercettazioni telematiche hanno un ambito di applicazione più ampio rispetto alle captazioni di conversazioni o comunicazioni telefoniche. Le captazioni telematiche, invero, sono consentite, oltre che nei procedimenti per i reati per cui è previsto l'impiego delle tradizionali forme d'intercettazione, anche per qualsiasi reato posto in essere per il tramite di strumentazione informatica o telematica[208].

Proprio con riferimento ai confini operativi della disposizione sono stati sollevati, in dottrina, alcuni dubbi[209]. Si è, infatti, obiettato che una lettura coordinata degli artt. 266 e 266-*bis* c.p.p. imporrebbe di ritenere che anche le intercettazioni telematiche possano essere disposte unicamente per i reati elencati dall'art. 266 c.p.p. con riferimento alle "tradizionali" forme di captazione. Ciò, onde evitare che il mezzo di ricerca in parola possa essere attivato o meno, per l'accertamento di un medesimo reato, a seconda delle modalità concrete di realizzazione di quest'ultimo[210].

Queste perplessità non paiono, tuttavia, condivisibili. In primo luogo, milita contro l'interpretazione "restrittiva" in questione l'inequivocabile dato letterale e, segnatamente, la formula aperta con cui l'art. 266-*bis* c.p.p. richiama indistintamente i reati «commessi mediante l'impiego di tecnologie informatiche o telematiche».

In secondo luogo, è opportuno ricordare come l'ordinamento già conosca ipotesi in cui, per l'accertamento di alcuni reati, un determinato mezzo di ricerca della prova sia attivabile solo laddove l'offesa sia posta in essere mediante un particolare strumento. Il riferimento è all'art. 266, comma 1, lett. *f*), c.p.p., il quale prevede, proprio in tema di intercettazioni, la possibilità di attivare le operazioni di ascolto per accertare reati di ingiuria, minaccia, usura, abusiva attività finanziaria,

---

[208] L. LUPARIA, *La disciplina processuale e le garanzie difensive*, cit., p. 163, pone in risalto un aspetto problematico. Poiché alcune strumentazioni utilizzate per la captazione di traffico telematico, quali il *telemonitor*, sono in grado di intercettare contemporaneamente traffico telefonico e telematico, si profila il rischio che vengano ascoltate conversazioni telefoniche anche in talune ipotesi ove l'autorizzazione del giudice era circoscritta ai soli flussi telematici. In tale ipotesi, l'Autore ritiene inutilizzabili i risultati acquisiti per violazione dell'art. 15 Cost.

[209] Cfr. C. DI MARTINO, *Le intercettazioni telematiche e l'ordinamento italiano: una convivenza difficile*, in *Ind. pen.*, 2002, pp. 221-222.

[210] Si veda, per tutti, F. FILIPPI, *L'intercettazione di comunicazioni*, Giuffrè, Milano, 1997, p. 82.

abuso di informazioni privilegiate, manipolazione del mercato, molestia o disturbo alle persone commessi «*col mezzo del telefono*».

In altre parole, è ben possibile che ad una specifica modalità di commissione di un reato consegua, quale riflesso processuale, l'ammissibilità di un particolare mezzo di ricerca della prova per il suo accertamento. D'altronde, la *ratio* della disciplina delle intercettazioni telematiche sta proprio nel fornire alla pubblica accusa, per l'accertamento di reati realizzati con attrezzature tecnologicamente avanzate, strumenti tali da «lottare tecnicamente "ad armi pari"» con gli autori delle condotte in questione[211].

Ciò chiarito, conviene analizzare in dettaglio la disciplina *ad hoc* dettata per le intercettazioni telematiche. Ai sensi dell'art. 268, comma 3-*bis*, c.p.p. il pubblico ministero può disporre che le operazioni vengano poste in essere «anche mediante impianti appartenenti a privati»[212]; entro cinque giorni dalla conclusione delle operazioni o il diverso termine previsto ai sensi del comma 5, qualora dal deposito possa derivare grave pregiudizio per le indagini, i difensori hanno facoltà di prendere cognizione dei flussi captati[213]. Scaduto il termine, l'acquisizione dei flussi di comunicazioni informatiche o telematiche è disposta dal giudice su richiesta delle parti, escluse le comunicazioni manifestamente irrilevanti, procedendo, eventualmente, anche d'ufficio, allo stralcio delle registrazioni e dei verbali di cui è vietata l'utilizzazione; all'udienza di stralcio hanno diritto di partecipare sia il pubblico ministero sia i difensori, con un preavviso di almeno ventiquattro ore (art. 268, comma 6, c.p.p.). Il giudice dispone la «stampa in forma intellegibile delle informazioni contenute nei flussi di comunicazione informatiche o telematiche da acquisire» secondo forme, modi e garanzie previste per l'espletamento delle

---

[211] Così, testualmente, C. PARODI, *La disciplina delle intercettazioni telematiche*, cit., p. 890, il quale ritiene la tesi in parola «maggiormente condivisibile su un piano di riconoscimento di "efficace" di tutela».

[212] È bene evidenziare che impianti privati non possono mai essere utilizzati per compiere intercettazioni di conversazioni o comunicazioni telefoniche: l'art. 268, comma 3, c.p.p. prevede unicamente la possibilità di eseguire la captazione mediante impianti installati nella procura della Repubblica; qualora questi ultimi siano insufficienti o inidonei, laddove sussistano eccezionali ragioni di urgenza, il pubblico ministero dispone, con decreto motivato, la realizzazione della captazione attraverso impianti di pubblico servizio o in dotazione della polizia giudiziaria.

[213] C. PARODI, *op. cit.*, p. 894, identifica l'oggetto della presa di cognizione da parte del difensore nel «supporto magnetico nel quale sono memorizzati sia i dati relativi al contenuto della comunicazione che i cd. "*file di log*", ossia le informazioni sugli orari di connessione [e sui dati] identificativi della comunicazione».

perizie[214]; le stampe costituiscono atto irripetibile in grado di transitare nel fascicolo per il dibattimento (art. 268, comma 7, c.p.p.). In ultimo, si prevede che i difensori possano richiedere copia «su idoneo supporto» dei flussi captati, oppure copia della stampa in forma intellegibile delle comunicazioni (art. 268, comma 8, c.p.p.).

Quanto ai profili dell'istituto sprovvisti di apposita disciplina, come la dottrina occupatasi dell'argomento ha chiarito, «la collocazione [dell'art. 266-*bis* c.p.p.] quale sorta di "ramificazione" dell'art. 266 c.p.p. […] impone all'interprete di inquadrare lo strumento investigativo in parola nel contesto delle regole generali in materia di ascolto delle comunicazioni vocali»[215].

È indubbia, quindi, l'applicabilità delle disposizioni dettate con precipuo riferimento alle intercettazioni telefoniche in ordine ai presupposti e alle forme del provvedimento che dispone le intercettazioni (art. 267 c.p.p.)[216], alla conservazione della documentazione (art. 269 c.p.p.) e all'utilizzazione dei risultati delle captazioni in altri procedimenti (art. 270 c.p.p.). Parimenti, le comunicazioni captate non possono essere utilizzate qualora eseguite fuori dei casi consentiti dalla legge (art. 271, comma 1, c.p.p.), oppure laddove relative a conversazioni o comunicazioni dei soggetti tenuti al segreto professionale, qualora concernano fatti conosciuti in ragione del loro ministero, ufficio o professione, a meno che tali soggetti abbiano deposto su quei fatti o li abbiano altrimenti divulgati (art. 271, comma 2, c.p.p.).

Residua, invece, qualche incertezza sull'applicabilità alle captazioni telematiche della disposizione dettata con riferimento all'esecuzione delle intercettazioni telefoniche dall'art. 268, comma 3, c.p.p. Più in particolare, è questione dibattuta se, quando si procede a intercettazioni telematiche, il pubblico

---

[214] Tale operazione è necessaria in quanto i flussi intercettati consistono in segnali digitali non immediatamente comprensibili per gli operanti. Cfr. C. PARODI, *op. cit.*, pp. 891 e 894.

[215] Così L. LUPARIA, *La disciplina processuale e le garanzie difensive*, cit., p. 162.

[216] Deve segnalarsi che, con riferimento alle intercettazioni telematiche, ricorre maggiormente, rispetto alle captazioni telefoniche, l'ipotesi che il mezzo della ricerca della prova sia disposto d'urgenza dal pubblico ministero, stante la natura volatile del dato informatico; in tal caso, sarà necessaria la trasmissione del decreto motivato che dispone le operazioni entro ventiquattro ore al giudice per le indagini preliminari, il quale decide entro quarantotto ore dal provvedimento con decreto motivato (art. 267, comma 2, c.p.p.). Nonostante il grave pregiudizio alle indagini in caso di ritardo sia, con riferimento alle indagini informatiche, quasi *in re ipsa*, (cfr. C. PARODI, *op. cit.*, p. 893), ciò non deve indurre a ritenere insussistente un onere motivazionale al riguardo in capo al pubblico ministero.

ministero sia tenuto a motivare laddove decida di utilizzare impianti appartenenti a privati invece che quelli installati presso la Procura della Repubblica.

La questione ruota intorno alla configurazione dell'art. 268-*bis* c.p.p. – il quale, come accennato, prevede la possibilità di utilizzare, per l'esecuzione delle operazioni di captazione telematica, strumentazione appartenente a privati – quale regola generale tale da esonerare la pubblica accusa da qualsivoglia onere motivazionale laddove opti per l'utilizzazione di impianti privati; oppure, come mera eccezione a quanto previsto in via ordinaria per le intercettazioni dall'art. 268, comma 3, c.p.p., con correlativo alleggerimento – ma non elisione – del dovere di motivare la propria scelta in capo al pubblico ministero.

A sostegno della prima tesi, si è evidenziato che la mancata previsione della sanzione dell'inutilizzabilità in caso di violazione del disposto di cui all'art. 268, comma 3-*bis*, c.p.p. confermerebbe la libertà assoluta del pubblico ministero di far eseguire le operazioni presso gli impianti privati secondo quanto ritenga più opportuno[217].

Si è, però, obiettato che, giacché l'utilizzo di impianti privati lede maggiormente la libertà e la segretezza delle conversazioni, sembra più rispettoso delle garanzie previste dall'art. 15 Cost. ritenere comunque doverosa, laddove possibile, l'esecuzione delle operazioni per mezzo degli impianti installati nella procura della Repubblica, con correlativa necessità di motivare allorché si decida di far eseguire le operazioni con impianti privati. In quest'ottica, la mancata previsione dell'inutilizzabilità rappresenterebbe una «mera svista legislativa risalente alla legge 547 del 1993», a cui rimediare valorizzando il ruolo dell'art. 191 c.p.p. di «"norma valvola" capace di veicolare nel sistema probatorio i diritti inviolabili della persona, traducendo i precetti costituzionali in divieti probatori»[218].

Tale ultima ricostruzione sembra preferibile. Si rinviene un appiglio testuale all'interpretazione qui accolta nell'art. 268, comma 3-*bis*, c.p.p., il quale prevede la possibilità di effettuare le operazioni «*anche*» tramite impianti privati[219]; tale dato

[217] In questo senso G. BRAGHÒ, *Le indagini informatiche fra esigenze di accertamento e garanzie di difesa*, in *Dir. inf.*, 2005, p. 523.
[218] Le citazioni sono di L. LUPARIA, *La disciplina processuale e le garanzie difensive*, cit., pp. 164-165.
[219] Cfr. C. DI MARTINO, *op. cit.*, p. 224.

pare confermare la natura residuale della disposizione, legata alle specifiche caratteristiche tecniche dell'operazione di captazione da porre in essere. Restano valide, insomma, anche per le captazioni informatiche le regole dettate dall'art. 268, comma 3, c.p.p.

Un altro profilo d'interesse attiene alla ricerca dell'oggetto dell'attività intercettiva. L'art. 266-*bis* c.p.p., nell'individuare quale oggetto della captazione il «flusso di comunicazioni relativo a sistemi informatici o telematici ovvero incorrente tra più sistemi», non fornisce alcuna definizione di questi ultimi. Soccorre, a tal riguardo, la giurisprudenza di legittimità, che ha chiarito come un sistema informatico sia costituito da «una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche»[220], mentre un sistema telematico è un insieme di strumenti tecnologici (*hardware*) e programmi (*software*) destinato alla trasmissione a distanza di informazioni[221].

Nella prassi, l'intercettazione di cui all'art. 266-*bis* c.p.p. può riguardare flussi di diverso tipo: la gamma, amplissima, va dal monitoraggio dell'intero traffico telematico generato da una determinata utenza, indipendentemente dal tipo di connessione[222], all'inoltro di tutte le *e-mail* indirizzate ad una specifica casella di posta elettronica verso un diverso indirizzo controllato dagli inquirenti[223].

Più problematica la riconducibilità all'art. 266-*bis* c.p.p. della captazione di conversazioni *Voice-overIP*[224]. In prima battuta, poiché le conversazioni in parola

---

[220] Cass., Sez. VI, 14 dicembre 1999, Piersanti, in *C.E.D. Cass.*, rv. 214945.

[221] V. Cass., Sez. V, 20 maggio 2003, n. 22319, *inedita*. È opportuno notare che la Convenzione di Budapest non distingue tra sistema informatico e telematico, limitandosi a definire il primo, in senso ampio, come «qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati». Cfr., sul punto, C. SARZANA DI S. IPPOLITO, *Informatica,* internet *e diritto penale*, Giuffrè, 2010, p. 217.

[222] Ne riferisce G. BRAGHÒ, *Le indagini informatiche fra esigenze di accertamento e garanzie di difesa*, cit., p. 522.

[223] Simile attività di captazione è possibile con riguardo alle società di telecomunicazioni nazionali. Cfr. F. CAJANI, *La Convenzione di Budapest nell'insostenibile salto all'indietro del legislatore italiano, ovvero: quello che le norme non dicono…*, cit., p. 195 ss., il quale offre, altresì, un panorama delle difficoltà applicative in ordine all'intercettazione delle caselle di posta elettronica *.com*.

[224] Si tratta, in breve, di una tecnologia che consente chiamate vocali sfruttando una rete che utilizzi il protocollo *IP* per la trasmissione dei dati.

costituiscono di certo un flusso informatico, esse parrebbero rientrare nell'ambito applicativo dell'istituto[225]. Eppure, tale rilievo non sembra decisivo.

Negli ultimi anni, invero, lo sviluppo tecnologico ha fatto sì che l'intero sistema di telefonia, mobile e fissa, sia, oramai, un vero e proprio sistema telematico, come espressamente riconosciuto anche dalle Sezioni Unite della Corte di Cassazione[226]. Così, di pari passo con lo sfumare della distinzione tra comunicazioni telefoniche e comunicazioni telematiche, sbiadiscono i confini tra art. 266 c.p.p. e art. 266-*bis* c.p.p. Tanto da far apparire fondata l'opinione di chi, già al tempo dell'introduzione dell'art. 266-*bis* c.p.p., teorizzava l'inutilità del nuovo istituto, giacché anche le intercettazioni informatiche o telematiche ben avrebbero potuto essere ricondotte alle «altre forme di telecomunicazione» già previste dall'art. 266 c.p.p.[227].

Ad ogni modo, corollario delle affermazioni che precedono è l'impossibilità di discernere tra intercettazione di conversazioni o comunicazioni telefoniche ai sensi all'art. 266 c.p.p. e captazione di flussi informatici o telematici *ex* art. 266-*bis* c.p.p. unicamente a seconda dell'impiego o meno di tecnologie informatiche o telematiche. Se così fosse, invero, tutte le captazioni di comunicazioni vocali, anche quelle a mezzo del telefono, dovrebbero ormai ricondursi *tout court* all'art. 266-*bis* c.p.p.; conseguenza, questa, evidentemente inaccettabile.

Il problema appare di più facile soluzione non appena si considera la *ratio* dell'art. 266 c.p.p.: vale a dire, limitare quanto più possibile le violazioni del principio di libertà e segretezza delle comunicazioni di cui all'art. 15 Cost. in presenza di comunicazioni vocali[228]. Più che il mezzo di trasmissione della conversazione, informatico o meno, allora, conta la sostanza: e le conversazioni tramite *VoIP* sembrano condividere tutti i tratti tipici di quelle conversazioni

---

[225] Cfr. C. PARODI, VoIP, Skype *e tecnologie d'intercettazione: quali risposte d'indagine per le nuove frontiere delle comunicazioni?*, in *Dir. pen. proc.*, 2008, p. 1311, ritiene che «il dato strettamente tecnologico, costituito dal transito delle [forme di comunicazione] in forma digitalizzata attraverso *pc* connessi tra loro o alla rete *Internet*» imponga l'inquadramento delle intercettazioni di comunicazioni *VoIP* nell'art. 266-*bis* c.p.p.

[226] Cass., Sez. Un., 8 maggio 2000, D'Amuri, in *Cass. pen.*, 2000, p. 1419.

[227] In quest'ottica, v. G. FUMU, sub *art. 266*-bis, in AA.VV., *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, III agg., Utet, Torino, 1998, p. 132.

[228] In questo senso L. LUPARIA, *La disciplina processuale e le garanzie difensive*, cit., p. 166.

telefoniche che il legislatore aveva in mente allorquando tracciò i limiti di ammissibilità delle intercettazioni di comunicazioni di cui all'art. 266 c.p.p.[229].

Il discorso approda, allora, in ultima analisi, ad un solo risultato: le intercettazioni di conversazioni *VoIP* devono essere autorizzate solo nell'ambito di quei procedimenti in cui occorra accertare uno dei reati elencati dall'art. 266 c.p.p.[230].

Merita, da ultimo, alcune considerazioni il quesito circa la possibilità di disporre le intercettazioni telematiche in presenza di «sufficienti indizi», anziché gravi, laddove la captazione sia «necessaria» – e non indispensabile – per lo svolgimento di indagini in relazione a delitti di criminalità organizzata o di minaccia col mezzo del telefono. Come noto, simile deroga all'art. 267 c.p.p. è prevista dall'art. 13, L. 203/1991. Tale ultima, disposizione, tuttavia, richiama unicamente l'art. 266 c.p.p. e non l'art. 266-*bis* c.p.p. Com'è stato evidenziato in dottrina, il dato letterale potrebbe essere superato ritenendo che il richiamo all'art. 266 c.p.p. debba, in realtà, riferirsi più in generale a tutte le attività di captazione consentite all'interno del sistema[231].

---

[229] *Contra* F. CAJANI, *La Convenzione di Budapest nell'insostenibile salto all'indietro del legislatore italiano, ovvero: quello che le norme non dicono…*, cit., pp. 193-194, nt. 15, il quale, tra le diverse argomentazioni, fa leva sul «dato sistematico» in base al quale il legislatore, introducendo un apposito art. 266-*bis* c.p.p. per disciplinare le intercettazioni di comunicazioni informatiche o telematiche, avrebbe confermato, *a contrario*, che tra le «altre forme di comunicazione» di cui all'art. 266 c.p.p. non possano rientrarvi quelle informatiche.
Per lungo tempo il tema non è stato affrontato compiutamente dalla giurisprudenza, poiché *Skype* si era a lungo rifiutato di fornire i codici necessari all'Autorità giudiziaria.

[230] Per lungo tempo il tema non è stato affrontato compiutamente dalla giurisprudenza, poiché i creatori del più noto servizio *VoIP*, *Skype*, si erano a lungo rifiutati di fornire i codici necessari all'Autorità giudiziaria per esperire utilmente la captazione. Cfr., in proposito, F. CAJANI. *La Convenzione di Budapest nell'insostenibile salto all'indietro del legislatore italiano, ovvero: quello che le norme non dicono…*, cit., p.p. 192-193, nt. 12, nonché C. PARODI, VoIP, Skype *e tecnologie d'intercettazione: quali risposte d'indagine per le nuove frontiere delle comunicazioni?*, cit., pp. 1309 ss. Cass., Sez. V, 7 novembre 2013, n. 45146, *inedita*, dà conto di come l'utilizzo del servizio *Skype* per conversare sia, addirittura, considerato elemento a carico dal Tribunale del riesame di Bologna: «la scelta del T. di ricorrere alla piattaforma *Skype* per colloquiare con F.G., prima ancora di sapere la ragione della telefonata, [deve ritenersi] univocamente indicativa della natura illecita dei rapporti tra i due indagati. Come noto, infatti, il metodo di comunicazione in parola consente di evitare le intercettazioni». La Corte di Cassazione, correttamente, nell'annullare l'ordinanza impugnata, evidenzia che il semplice invito di ricorrere a *Skype* per conversare ben poteva giustificarsi in base ad una maggiore economicità del mezzo di comunicazione prescelto. Ad ogni modo, è opportuno sottolineare che la situazione, a seguito dell'acquisizione del servizio ad opera di *Microsoft*, appare oggi mutata, giacché, di recente, alcune sentenze dei giudici di legittimità accennano a conversazioni *Skype* quale patrimonio probatorio utilizzato dal giudice di merito. V., al riguardo, fra le più recenti, Cass., Sez. III, 18 luglio 2014, n. 31864, *inedita*.

[231] Si veda, al riguardo, C. PARODI, *La disciplina delle intercettazioni telematiche*, cit., 2003, p. 893.

D'altro canto, non si può trascurare il fatto che la lesione a beni costituzionalmente tutelati con riserva di legge e di giurisdizione quale la libertà e la segretezza delle comunicazioni (art. 15 Cost.) connaturata ad ogni intercettazione di flussi informatici sembra imporre, in assenza di precisi dati testuali in senso contrario, un'interpretazione restrittiva dell'art. 13, L. 203/1991. Dunque, devono ritenersi sussistenti, anche con riferimento alle ipotesi di contrasto alla criminalità organizzata, i limiti all'attività captativa previsti dall'art. 267 c.p.p.[232].

4.2 Il captatore informatico quale prova atipica

Il progresso tecnologico ha portato all'emersione di una nuova tecnica investigativa. Strumenti di tradizionale appannaggio della criminalità informatica quali *spyware*, *sniffer*, *trojan horses* e, più in generale, *malware*[233] vengono utilizzati dagli inquirenti per ottenere informazioni contenute o in transito su strumentazione informatica.

Tali programmi-spia, una volta inseriti dentro un sistema informatico, consentono, per un verso, di monitorare il flusso di comunicazioni in entrata ed uscita da quest'ultimo (*online surveillance*)[234]. Per altro verso, essi consentono di prendere visione e di fare copia della totalità dei dati contenuti nel sistema "infetto": sia quelli preesistenti nel sistema sia, in tempo reale, di quelli in corso di formazione (*one time copy* o *online search*). Non solo; chi controlla il *malware* può operare direttamente sulla macchina "bucata", con l'inserimento di *file*, l'attivazione del microfono o della videocamera, e così via.

Si tratta, com'è agevole intuire, di uno strumento investigativo in grado di violare sotto più profili la libertà del soggetto avente la disponibilità della

---

[232] In questo senso anche C. DI MARTINO, *op. cit.*, p. 225, la quale ritiene ineludibile, ai sensi dell'art. 15 Cost., la garanzia della predeterminazione tassativa delle limitazioni alla libertà di comunicare; garanzia che, nel caso di specie, verrebbe a mancare.

[233] Con tale termine si indicano una serie di *software* dannosi per l'utente (*malicious software*). R. FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d.* online durchsuchung, in *Riv. trim. dir. pen. econ.*, 2009, p. 697, richiama anche i *keylogger*, programmi in grado di memorizzare qualsiasi tasto digitato sulla tastiera del *computer*, attacchi *exploits*, vale a dire esecuzioni di codici non previsti in grado di portare all'acquisizione dei privilegi di amministratore in capo a colui che ha realizzato l'attacco, nonché le metodologie di *social engineering*.

[234] Ed è opportuno sottolineare che *tutte* le informazioni in transito possono, astrattamente, essere oggetto di acquisizione.

strumentazione infetta. In prima battuta, quale diritto passibile di lesione viene in considerazione l'inviolabilità del domicilio di cui all'art. 14 Cost. Ciò, in una duplice prospettiva; violazione del domicilio inteso quale luogo dove il *computer* si trova, qualora il *trojan* venga installato mediante un'azione diretta sulla strumentazione informatica; ovvero, violazione del domicilio informatico, laddove il *virus* sia installato a distanza, ad esempio attraverso l'invio di un allegato di posta elettronica.

Pare, altresì, configurabile una lesione dell'art. 15 Cost., giacché, in astratto, simili *malware* consentono di prendere cognizione di ogni attività posta in essere mediante la rete *internet* dal soggetto monitorato, incluse le *chat* intercorse e le *e-mail*.

Da ultimo, viene in considerazione l'art. 8 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali[235], il quale impone il rispetto della vita privata e familiare, del domicilio e della corrispondenza.

Come noto, perché l'autorità pubblica possa inficiare i diritti sopra menzionati, è prevista una riserva di legge (artt. 14 Cost. e 8 C.E.D.U.) o una duplice riserva di legge e di giurisdizione (art. 15 Cost.).

Alla luce di queste sia pur brevi considerazioni, si evidenziano due piani di ricerca, attinenti, l'uno, alla collocazione sistematica del mezzo di ricerca della prova in questione, anche al fine di verificare il rispetto della riserva di legge e di giurisdizione posta dalle norme di rango sovraordinato, e l'altro alla compatibilità con i suesposti principi fondamentali.

Con riferimento al primo dei due momenti di indagine, deve, anzitutto, evidenziarsi che, fra le attività che i programmi-spia possono svolgere, quella di *online surveillance* rappresenta, di fatto, un monitoraggio e/una captazione di un flusso informatico intercorrente tra più sistemi informatici o telematici. Dunque, essa va ricondotta, quanto a presupposti e disciplina, alle intercettazioni di comunicazioni informatiche o telematiche di cui all'art. 266-*bis* c.p.p. L'attivazione del mezzo di ricerca della prova in parola dovrà, perciò, essere preceduta

[235] Sulla natura di norma interposta da attribuire alla C.E.D.U. non sussistono più dubbi, a seguito delle note sentenze n. 348 e 249 del 2007, nonché n. 38 del 2008, della Corte Costituzionale. Sul punto, cfr. S. MARCOLINI, *Le cosiddette perquisizioni* online *(o perquisizioni elettroniche)*, in *Cass. pen.*, 2010, p. 2863 ss.

dall'autorizzazione del giudice per le indagini preliminari unicamente laddove vi siano gravi indizi di reato[236] e il monitoraggio appaia indispensabile ai fini della prosecuzione delle indagini[237].

Si impone, però, una precisazione. Tale approdo sembra incontestabile laddove la captazione abbia per oggetto comportamenti comunicativi quali *e-mail* o *chat*. Quanto all'attività non comunicativa in senso stretto, quale la navigazione di pagine *web*, deve evidenziarsi come incontri ampio consenso, in dottrina[238] come in giurisprudenza[239], l'assunto secondo cui l'attività di captazione disciplinata dall'art. 266-*bis* c.p.p. condivide con le intercettazioni telefoniche il tratto comune costituito dalla «captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti che agiscano con l'intenzione di escludere altri e con modalità oggettivamente idonee allo scopo»[240].

In questa prospettiva, sarebbero escluse dall'ambito applicativo delle intercettazioni informatiche o telematiche quelle attività, quali la navigazione *web*, che rappresentano sì, in senso tecnico, un flusso di dati tra sistemi, ma cui farebbe difetto il carattere della comunicazione o conversazione privata[241]. Secondo questa ricostruzione, allora, l'eventuale captazione di quei flussi non dovrebbe rispettare i limiti imposti dagli artt. 266-*bis* e ss. c.p.p.

Quanto all'attività di *one time copy* o di *online search*, si può escludere *tout court* l'applicabilità dell'art. 266-*bis* c.p.p., dal momento che i dati captati, in tali ipotesi, non attengono ad un flusso di dati tra sistemi informatici o sistemi telematici.

---

[236] L'attività di monitoraggio di un sistema informatico o telematico, in qualsiasi forma essa si manifesti, non potrà, naturalmente, mai prescindere da una notizia di reato, onde evitare che lo strumento di ricerca della prova si traduca in un indebito mezzo di reperimento di *notitiae criminis*. Rischio che, come già evidenziato, appare ancor più accentuato nell'ambito delle indagini informatiche, a causa dell'immensa mole di dati dei quali gli inquirenti verrebbero a conoscenza.

[237] Naturalmente, perché possa essere ricompresa nell'art. 266-*bis* c.p.p., l'attività dovrà limitarsi alla captazione di flussi fra sistemi informatici e telematici. Non si potranno, invece, ad esempio, acquisire in copia, per mezzo del medesimo strumento, i *file* contenuti nel sistema infetto.

[238] Cfr. S. MARCOLINI, *Le cosiddette perquisizioni* online *(o perquisizioni elettroniche)*, cit., pp. 2859-2860.

[239] Cass., Sez. Un., 8 maggio 2000, D'Amuri, cit.

[240] Così, testualmente, S. MARCOLINI, *Le cosiddette perquisizioni* online *(o perquisizioni elettroniche)*, cit., p. 2859.

[241] In diversa prospettiva, cfr. Cass., Sez. I, 16 aprile 2005, Palamara, in *C.E.D. Cass.*, rv. 231591, che sembra – ma sul punto il *dictum* non brilla per chiarezza – accogliere una nozione più ampia di «comunicazione», facendo rientrare nell'alveo dell'art. 266-*bis* il monitoraggio di tutti i flussi informatici gestiti da un soggetto titolare di un determinato nome utente.

Si tratta, a questo punto, di verificare se tali attività, non rientranti nelle intercettazioni telematiche, abbiano un qualche referente codicistico oppure se, per sostenerne la legittimità, debba farsi necessariamente leva sul meccanismo di cui all'art. 189 c.p.p. e sul principio di atipicità dell'attività investigativa.

A tal proposito, viene in considerazione, in prima battuta, l'art. 247 c.p.p. Invero, l'utilizzo di un captatore informatico a fini investigativi è stato definito dalla dottrina perquisizione *online* o perquisizione elettronica[242], sulla scorta del rilievo secondo cui sia la perquisizione tradizionale sia quella informatica sono accomunate dall'essere atti a sorpresa aventi quale precipuo fine la ricerca di una *res* in possesso dell'indagato[243].

Come esattamente osservato, tuttavia, l'aspetto singolare delle perquisizioni informatiche risiede nella circostanza che esse prescindono dalla ricerca del corpo del reato o delle cose pertinenti al reato. Inoltre, a differenziare ulteriormente i due strumenti, sta il dato che, seppur entrambi atti a sorpresa, nel caso delle perquisizioni *online*, per la riuscita dell'operazione, è necessario che l'utilizzatore del sistema sotto controllo ignori di essere sottoposto ad un costante monitoraggio per tutta la durata di quest'ultimo, mentre il soggetto perquisito avverte di essere sottoposto ad un atto limitativo della libertà personale[244].

Lo strumento investigativo in parola non pare nemmeno riconducibile al *genus* dell'ispezione. Difatti, la raccolta di informazioni all'insaputa dell'indagato, che costituisce il "cuore" delle perquisizioni *online*, appare difficilmente assimilabile all'attività di osservazione e descrizione tipica dell'istituto di cui all'art. 244 c.p.p.[245].

Nell'unico precedente giunto allo scrutinio dei giudici di legittimità relativo all'utilizzo, da parte di una Procura della Repubblica, di un captatore informatico, lo strumento processuale utilizzato dalla pubblica accusa per acquisire, all'insaputa dell'utilizzatore, i dati memorizzati all'interno di un sistema informatico, nonché

---

[242] V., in proposito, S. MARCOLINI, *op. cit.*, p. 2855 ss.
[243] *Res* che, com'è agevole avvertire, nel caso della perquisizione *online*, è immateriale.
[244] Cfr. S. MARCOLINI, *op. cit.*, pp. 2858-2859. L'Autore sottolinea, inoltre, l'inapplicabilità alle perquisizioni elettroniche delle garanzie previste per le tradizionali perquisizioni, prima fra tutte la facoltà di partecipazione del difensore.
[245] In questo senso v. ancora S. MARCOLINI, *op. cit.*, cit. p. 2860.

quelli ancora da formare, è stato un decreto di acquisizione di documentazione ai sensi dell'art. 234 c.p.p.[246].

Ora, già si è avuto modo di chiarire che l'istituto della prova documentale mal si adatta alla *digital evidence*. Inoltre, balza agli occhi l'anomalia di un provvedimento di acquisizione di "documenti" – sempre che di documenti si tratti – non ancora formatisi, giacché il congegno tecnico consentiva l'acquisizione periodica[247] di tutti i dati, quelli già presenti così come quelli ancora da formare, nella memoria del *personal computer* dell'indagato.

Giunti a questo punto, unica strada in astratto percorribile per ritenere consentita agli inquirenti un'attività come quella descritta parrebbe la configurazione delle perquisizioni *online* come mezzo di ricerca atipico della prova[248].

Proprio questa è stata la soluzione prescelta dalla Corte di Cassazione nell'unico precedente noto sulla tematica[249]. I giudici partono da un assunto: nel caso di specie, la captazione era consistita nel prelevare e copiare documenti memorizzati sull'*hard disk*. Dunque, la captazione non aveva ad oggetto «un flusso di comunicazioni, richiedente un dialogo con altri soggetti, ma una relazione operativa tra microprocessore e video del sistema elettronico, ossia un flusso unidirezionale di dati confinato all'interno dei circuiti del *personal computer*»[250]. Di qui, l'esclusione dell'applicabilità dell'art. 266-*bis* c.p.p. e la riconducibilità dell'acquisizione di *file* mediante tale strumento, definito quale "captatore informatico", all'art. 189 c.p.p.

Questa attività investigativa, inoltre, secondo i giudici di legittimità, non avrebbe leso alcun bene di rilievo costituzionale. Non l'art. 14 Cost., poiché il *computer* monitorato non era collocato in un luogo di privata dimora, bensì in un ufficio comunale, e dunque in luogo aperto al pubblico. Neppure l'art. 15 Cost.,

---

[246] Cass., Sez. V, 29 aprile 2010, n. 16556, cit.
[247] Il controllo si era protratto, nel caso di specie, per otto mesi.
[248] Sulla configurabilità di mezzi di ricerca della prova atipici, cfr., proprio con riferimento alle perquisizioni *online*, G. BONO, *op. cit.*, p. 1528.
[249] Cass., Sez. V, 29 aprile 2010, n. 16556, cit.
[250] Cass., Sez. V, 29 aprile 2010, n. 16556, cit.

poiché i *file* acquisiti in copia non erano destinati alla trasmissione, quanto alla stampa su supporto cartaceo[251].

Senza entrare, per il momento, nel merito della fondatezza del *dictum*, preme evidenziare come quest'ultimo, lungi dal consentire l'utilizzo del captatore informatico in qualsiasi situazione, ne ammetteva l'impiego unicamente in base alle contingenze del caso di specie.

In realtà, con riguardo ad un possibile contrasto con l'art. 15 Cost., la tesi propugnata dalla Corte appare, oggi, non più sostenibile, tenuto conto delle caratteristiche dei più recenti *malware*. Gli attuali programmi-spia, invero, non si limitano all'acquisizione di documenti ma, come accennato, monitorano ogni attività compiuta attraverso il *computer* dall'utilizzatore, comprese attività di tipo comunicativo. Di tal ché, l'installazione di un *trojan* potrebbe comportare una indebita intercettazione telematica in assenza dei presupposti ed oltre i limiti di cui agli artt. 267 e ss. c.p.p.

Quanto al possibile contrasto con l'art. 14 Cost., il problema della compatibilità con la tutela costituzionale del domicilio potrebbe ritenersi addirittura superato, una volta per tutte, dai progressi compiuti nella progettazione dei *malware* utilizzati quali "programmi-spia". Invero, se al tempo della pronuncia dei giudici di legittimità era necessaria una installazione diretta sul sistema oggetto di futuro controllo, ora i *trojan* possono essere inseriti nel sistema da remoto, senza alcuna intrusione "fisica" nel luogo ove il *computer* è localizzato.

Eppure, tale ricostruzione non tiene in dovuto conto come la tutela del domicilio debba ritenersi, ormai, estesa anche al domicilio informatico, quale "luogo virtuale" in cui si esplica la libertà del cittadino[252]; basti por mente all'introduzione del reato di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615-*ter* c.p. Di più: a ben vedere, la condotta degli operanti che installano da remoto un *virus* sul *computer* del soggetto da monitorare sembra

[251] V., ancora, Cass., Sez. V, 29 aprile 2010, n. 16556, cit.
[252] In questa prospettiva, S. COLAIOCCO, *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *Arch. pen.*, 2014, p. 9.

integrare proprio la condotta prevista e punita da tale ultima disposizione[253]. Ed inoltre, quand'anche non si ritenesse il *computer* oggetto di tutela diretta ai sensi dell'art. 14 Cost., pare, comunque, indubbia la compressione al diritto alla *privacy* di cui all'art. 8 C.E.D.U.[254].

Si fa presto a scorgere, allora, dietro al tema che ci occupa, il quesito, già affrontato dalla giurisprudenza[255], dell'impiego processuale dei risultati di un mezzo di ricerca della prova "atipico" lesivo di principi costituzionali. È sufficiente richiamare, in proposito, l'approdo delle Sezioni Unite, secondo cui le prove atipiche lesive di diritti costituzionalmente tutelati non possono essere ammesse, in quanto prove illecite[256].

Se così è, proprio gli artt. 2, 14, 15 Cost. e art. 8 C.E.D.U rappresentano un invalicabile argine all'impiego del captatore informatico in fase investigativa attraverso il *passepartout* dell'art. 189 c.p.p. Ciò, perlomeno, in assenza di una disciplina che detti regole specifiche per l'utilizzo dello strumento in parola. Infatti, lo stesso si traduce – e non può non tradursi – in una violazione del domicilio informatico al di fuori dei casi e modi stabiliti dalla legge.

L'assunto trova conferma in una sentenza della Corte Costituzionale tedesca occupatasi proprio del problema relativo al conflitto fra attività di monitoraggio segreto di sistemi informatici e valori fondamentali[257].

Questo l'antefatto. Era stata introdotta, a livello regionale, una disposizione[258] che prevedeva espressamente che un organismo di *intelligence*

---

[253] La Corte di Cassazione, nella pronuncia Cass., Sez. V, 29 aprile 2010, n. 16556, cit., non sembra essersi soffermata su questo aspetto, vale a dire sull'ammissibilità di una prova atipica frutto di un'attività di per sé costituente reato.

[254] Spunti interessanti circa il diritto alla riservatezza informatica tutelato dall'art. 8 C.E.D.U., nonché dall'art. 7 della Carta dei diritti fondamentali dell'Unione Europea, si ritrovano in F. IOVENE, *Le perquisizioni c.d.* online, *tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in www.penalecontemporaneo.it, p. 7 ss.

[255] V., per tutte, Cass., Sez. Un., 28 luglio 2006, Prisco, in *C.E.D. Cass.*, rv. 234270.

[256] Cass., Sez. Un., 28 luglio 2006, Prisco, cit., secondo cui, invece, la sanzione dell'inutilizzabilità ai sensi dell'art. 191 c.p.p. attiene unicamente alle prove tipizzate dal legislatore.

[257] BVerfG 370/2007 e 595/2007, 27 febbraio 2008, in *CR*, 2008, p. 306 ss. Ne riferisce R. FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d.* online durchsuchung, cit., p. 695 ss.; cfr. anche ID., *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali nella recente giurisprudenza del* Bundesverfassungsgericht*: la decisione del 27 febbraio 2008 sulla* Online Durchsuchung *e la sua portata alla luce della sentenza del 2 marzo 2010 sul* data retention, in *Cib. dir.*, 2010, p. 359 ss., nonché ID., *Verso una rivalutazione dell'art. 615*-ter *c.p.?*, in www.penalecontemporaneo.it, p. 16.

potesse effettuare, da un lato, il monitoraggio e la ricognizione in segreto della rete *Internet*, dall'altro lato, accessi segreti a sistemi informatici. Il *Bundesverfassungsgericht* era stato chiamato a verificarne la tenuta costituzionale.

Dopo aver preso atto dell'ineludibile conflitto tra l'esigenza investigativa di accertare reati ed i diritti fondamentali dell'individuo, la Corte ha finito per teorizzare un diritto alla riservatezza e all'integrità dei sistemi informatici, quale nuova manifestazione, frutto del progresso tecnologico, del più generale diritto alla personalità (artt. 1.1 e 2.1 del *Grundgesetz*)[259]. Tale diritto, secondo il *Bundesverfassungsgericht*, può essere leso soltanto laddove «*actual indications exist of a concrete danger to a predominantly important legal interest*», vale a dire «*life, limb and freedom of the individual or such interests of the public a threat to which affects the basis or continued existence of the state or the basis of human existence*»[260].

Così come strutturata, invece, la disciplina scrutinata, per un verso, ledeva il principio di determinatezza, giacché, con riferimento all'ipotesi del monitoraggio *online*, era carente sotto il profilo della «*clarity of provisions and determinedness of provisions*»[261]. Per altro verso, con riguardo all'ipotesi dell'accesso in segreto a periferiche, non era rispettato il principio di proporzionalità, siccome la lesione al diritto alla riservatezza e all'integrità dei sistemi informatici era eccessiva rispetto alla gravità dei motivi che la giustificavano[262].

---

[258] Legge sulla protezione della Costituzione del North Rhein Westfalia, come modificata il 20 dicembre 2006, § 5, comma 2, n. 11, in *Law and Ordinance Gazette of North Rhine-Westphalia* (*GVBl NW*), 2006, p. 620.

[259] Ciò, in quanto i *computer*, al giorno d'oggi, secondo la Corte, «*can be used for a large number of different purposes, such as for the comprehensive administration and archiving of an individual's personal and business matters, as a digital library or in many ways as an entertainment appliance. Accordingly, the significance of personal computers for the development of personality has increased considerably*». BVerfG 370, 595/2007, 27 febbraio 2008, cit. Le citazioni in lingua inglese provengono dal testo ufficiale della sentenza, reperibile *online* su www.bundesverfassungsgericht.de.

[260] BVerfG 370/2007 e 595/2007, 27 febbraio 2008, cit.

[261] I limiti dell'attività dell'organismo di *intelligence*, infatti, erano ricavabili tramite due rinvii normativi, uno ad altra disposizione della stessa Legge, la quale prevedeva l'impiego della sorveglianza *online* per l'acquisizione di informazioni rilevanti per la tutela della Costituzione, l'altro all'art. 10 della *Grundgesetz* a tutela della segeretezza delle comunicazioni. Cfr. R. FLOR, *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali nella recente giurisprudenza del* Bundesverfassungsgericht, cit., p. 370.

[262] Pienamente condivisibili le argomentazioni dei giudici tedeschi, che appare opportuno riportare, sul punto, vista l'estrema chiarezza, per intero. «*Data collection by the state from complex information technology systems shows considerable potential for researching the personality of the person concerned. This already applies to one-off, partial access, such as the seizure or copying of storage media of such systems [...]. Such secret access to an information technology system provides the acting state agency with access to a stock of*

Proprio questo *dictum* può rappresentare un monito, *mutatis mutandis*, per il legislatore italiano, qualora decidesse di disciplinare il fenomeno dal punto di vista normativo[263], ponendo così fine al proliferare di prassi devianti non adeguatamente censurate in sede di legittimità[264]. Allo stato, la sentenza della Corte Costituzionale tedesca conforta nel ritenere simili pratiche irrispettose di diritti fondamentali del cittadino. Di qui, la necessaria espunzione dal procedimento – *rectius*: l'impossibilità di ingresso – di tale illecita attività investigativa.

---

data which may far exceed traditional sources of information in terms of its scope and diversity. This is a result of the many different possibilities for use offered by complex information technology systems which are associated with the creation, processing and storage of personal data. In particular, according to the current habits of use, such appliances are typically used deliberately to also store personal data of increased sensitivity, for example private text, pictorial or sound files. The available data stock may include detailed information on personal circumstances and on the life of the person concerned, the private and business correspondence made via various communication channels, or indeed diary-like personal records. State access to such comprehensive data stocks entails the obvious risk that the collected data in an overall view facilitates comprehensive conclusions to be drawn on the personality of the person concerned, ranging to the formation of conduct and communication profiles». Così BVerfG 370/2007 e 595/2007, 27 febbraio 2008, cit.

[263] L'ipotesi è stata presa in considerazione, di recente, in Olanda e in Spagna, come riporta F. IOVENE, *Le perquisizioni c.d.* online, *tra nuovi diritti fondamentali ed esigenze di accertamento penale*, cit., p. 4. Negli Stati Uniti, è stato messo a punto dal *Federal Investigation Bureau* un apposito *software*, denominato *Magic Lantern*, in grado di installare su un'apparecchiatura informatica un *keystroke logging program*. Cfr., in proposito, C. WOO-M. SO, *The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance*, in *15 Harv. L. Tech.*, 2002, p. 521 ss.

[264] È indubbio che captatori informatici di vario tipo siano attualmente utilizzati dalle Procure italiane. I *mass media* si sono occupati del *virus*, battezzato – con buona dose d'ironia – "Querela", di recente utilizzato dalla Procura della Repubblica di Napoli; cfr., in proposito, l'articolo del quotidiano *La Repubblica*, 22 giugno 2011, *Un virus per* pc *inchioda Bisignani. Lo Stato diventa hacker a fin di bene*, reperibile *online* su www.repubblica.it.

Capitolo III – Integrità del dato digitale e continuità probatoria. *Digital forensics* e garanzie difensive

1. La procedimentalizzazione dell'indagine informatica urgente. La duplicazione dei dati informatici tra rilievo ed accertamento tecnico

La L. 48/2008 ha dedicato particolare attenzione all'indagine informatica urgente, modificando le disposizioni del titolo IV del Libro V relative alle attività a iniziativa della polizia giudiziaria. Le ragioni dell'intervento legislativo si spiegano facilmente. Il "pericolo" di smarrimento dell'informazione, presupposto dell'attività disciplinata dagli artt. 352 e ss. c.p.p., sussiste, nel caso della *digital evidence*, *in re ipsa*, viste le caratteristiche di immaterialità e fragilità del dato digitale[265]. Di qui, la necessità di dedicare precipua attenzione al tema delle operazioni da compiere in sede di primo contatto tra operanti e *digital evidence*[266].

In quest'ottica, è bene rilevare che la normativa in commento è senza dubbio apprezzabile nella misura in cui riserva particolare attenzione al tema della genuinità e immodificabilità del dato informatico a rischio di deperimento[267], ponendo fine alle prassi devianti invalse prima dell'intervento novellatore[268].

Tuttavia, prima di analizzare approfonditamente la nuova disciplina, è opportuno un chiarimento circa l'effettiva incidenza della riforma sull'ambito dei soggetti cui è permesso operare sul dato informatico in fase investigativa. Deve recisamente escludersi che l'assenza di disposizioni dettate con precipuo riguardo al pubblico ministero e al difensore in materia di indagini informatiche indifferibili imponga di considerare, quali soggetti ammessi a compiere attività urgenti sul dato digitale, unicamente gli ufficiali di polizia giudiziaria. Va, parimenti, scartata l'ipotesi che le cautele volte a preservare la genuinità delle informazioni probatorie

---

[265] In questo senso E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, cit., p. 143.
[266] Per un'analisi tecnica dei modelli di investigazione digitale, nonché per una panoramica generale su metodi e strumenti d'indagine per l'acquisizione e l'analisi della *digital evidence*, v. A. FIORE, *L'informatica forense e i modelli di investigazione digitale*, in *Cib. dir.*, 2014, p. 99 ss.
[267] Proprio il rischio di deperimento ha suggerito al legislatore di prevedere che l'operazione di duplicazione di dati, informazioni o programmi informatici debba essere «immediata», a differenza di quanto previsto, ad esempio, dall'art. 260 c.p.p.
[268] Ne riferisce E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, cit., p. 139 ss.

debbano essere osservate soltanto dalla polizia giudiziaria e non, più in generale, da qualsiasi soggetto che venga a contatto col dato informatico.

A militare in favore della tesi contraria sta, anzitutto, il dato letterale, solare nel limitare, ai sensi dell'art. 354, comma 2, c.p.p., l'intervento spontaneo della polizia giudiziaria ai casi in cui «il pubblico ministero non può intervenire tempestivamente ovvero non ha ancora assunto la direzione delle indagini». Dunque, qualora il pubblico ministero abbia già assunto le redini investigative, è lui a decidere se e come operare e a fornire agli ufficiali di polizia giudiziaria le disposizioni cui questi ultimi devono attenersi.

Inoltre, ineludibili esigenze di parità delle parti impongono, come già evidenziato, che anche il difensore possa operare sul dato, sia pure muovendosi negli spazi angusti tracciati dagli artt. 233, comma 1-*bis* e 391-*sexies* c.p.p.

Ciò chiarito, è opportuno passare in rassegna, più in dettaglio, le nuove disposizioni[269].

Anzitutto, si è novellato l'art. 353 c.p.p., relativo all'acquisizione, in casi di urgenza, di plichi o di corrispondenza. A seguito delle interpolazioni della L. 48/2008, gli ufficiali di polizia giudiziaria, qualora abbiano fondato motivo di ritenere che gli oggetti di corrispondenza spediti in forma elettronica contengano notizie utili alla ricerca e all'assicurazione di fonti di prova a rischio di dispersione, possono informare con il mezzo più celere il pubblico ministero, il quale può autorizzarli ad accertarne il contenuto (art. 353, comma 1, c.p.p.). Ai sensi del comma 2 della medesima disposizione, gli ufficiali di polizia giudiziaria, in caso di urgenza, possono ordinare a chi è preposto al servizio telematico o di telecomunicazione di sospendere l'inoltro degli oggetti di corrispondenza in forma elettronica o inoltrati per via telematica, se ne è consentito il sequestro; qualora quest'ultimo non sia disposto entro 48 ore dal pubblico ministero, i messaggi saranno inoltrati.

In secondo luogo, l'art. 352, comma 1-*bis*, c.p.p. prevede ora la possibilità, per gli ufficiali di polizia giudiziaria, di effettuare perquisizioni di sistemi

[269] Una panoramica sulle modifiche è offerta da A. BARBIERI, *Le attività d'indagine della polizia giudiziaria su sistemi informatici e telematici*, in *Dir. internet*, 2008, p. 516 ss.

informatici o telematici, se vi è fondato motivo per ritenere i dati, le informazioni, i programmi o le tracce pertinenti al reato ivi occultati soggetti al rischio di cancellazione o dispersione. Con una previsione che ricalca quanto stabilito in sede di perquisizione "statica" ai sensi dell'art. 247, comma 1-*bis*, c.p.p., si tutela la genuinità e la non alterazione del dato digitale mediante l'imposizione di misure tecniche tali da garantirne la conservazione.

In ultimo, si è modificato l'art. 354, comma 2, c.p.p., il quale contempla il potere, in capo agli ufficiali di polizia giudiziaria, di compiere accertamenti e rilievi sullo stato dei luoghi e delle cose, se vi è pericolo che le tracce e le cose pertinenti al reato si disperdano o modifichino, nonché di sequestrare le medesime. Qualora tale attività sia compiuta in relazione a dati, informazioni, programmi informatici o sistemi informatici o telematici, dovranno essere adottate misure tecniche idonee ad assicurare la conservazione e ad impedire l'alterazione del dato. Si specifica, inoltre, che gli ufficiali devono provvedere, ove possibile, all'immediata duplicazione dei dati informatici su adeguati supporti, attraverso una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità.

La normativa in parola sembra orientata a favorire la *live analysis* del sistema informatico, laddove ragioni di urgenza lo consiglino[270]; ad esempio, qualora si rinvenga, in sede di perquisizione locale, un sistema informatico acceso. In effetti, un'analisi *in loco* presenta l'indubbio vantaggio di consentire l'analisi di quei dati che verrebbero cancellati da un eventuale *reboot* del sistema[271].

Non solo. In una ipotesi di flagranza del reato di cui all'art. 600-*quater* c.p., ad esempio qualora gli operanti abbiano rinvenuto un *computer* acceso con aperto un *file* raffigurante una immagine pedopornografica, una perquisizione urgente del sistema informatico può orientare correttamente la polizia giudiziaria

[270] In questa direzione si è mossa, già da tempo, la dottrina statunitense: v., per tutti, E.E. KENNEALLY, *Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection*, in *5 UCLA J. L. & Tech.*, 2005, p. 1 ss.

[271] Nel caso di attrezzatura accesa, le *best practices* consigliano uno spegnimento del sistema mediante scollegamento della spina dalla presa elettrica, possibilmente dopo aver effettuato una copia dei dati contenuti nella memoria RAM. Qualora si spegnesse il *computer* utilizzando l'ordinaria procedura, invece, molti dati verrebbero riscritti e, dunque, inevitabilmente persi. Cfr. G. ZICCARDI, *L'ingresso della* computer forensics *nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, cit., p. 173.

sull'opportunità di procedere all'arresto, consentito, come noto, unicamente se il materiale detenuto è di ingente quantità (art. 600-*quater*, comma 2, c.p.).

Utili spunti per un primo ordine di riflessioni sulla normativa descritta possono trarsi analizzando le penetranti critiche mosse in dottrina alle nuove disposizioni.

In primo luogo, si è censurato[272] l'innesto nell'impianto codicistico di una disciplina delle indagini informatiche urgenti mediante ritocchi *ad hoc* alle disposizioni previgenti del titolo IV del Libro V. Disposizioni apparse, ai più attenti commentatori, strettamente legate all'entità materiale delle *res* da ricercare e, dunque, poco adattabili ad indagini relative a dati volatili ed immateriali. Rilievo, questo, pienamente condivisibile.

In secondo luogo, si è evidenziato che la decisione di concentrare le modifiche al testo normativo in tema di indagine informatica urgente nel titolo IV dedicato alla polizia giudiziaria, inquadrando le attività di duplicazione del dato digitale tra gli "Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro" dell'art. 354 c.p.p.[273], senza modificare, al contempo, gli artt. 359 e 360 c.p.p., non ha risolto il quesito, a lungo dibattuto in dottrina e nella prassi, circa la natura ripetibile o meno dell'attività di clonazione di un supporto.

Certo, presupposto per gli accertamenti urgenti di polizia giudiziaria ai sensi dell'art. 354 c.p.p. è l'impossibilità di intervento tempestivo da parte del pubblico ministero; quest'ultimo, soprattutto qualora non abbia ancora assunto la titolarità dell'indagine, non potrebbe conferire l'incarico ad un consulente tecnico in tempo utile a svolgere le necessarie operazioni urgenti. Ciò non significa, però, che la riconduzione della copia forense ai rilievi (art. 354 c.p.p.) fosse opzione necessitata.

Invero, l'attività di duplicazione di dati informatici difficilmente può assimilarsi ai tradizionali rilievi di polizia giudiziaria, giacché si tratta di «azioni ad alto contenuto tecnologico che già implicano scelte metodologiche e delicate valutazioni […]»[274]. Proprio tali considerazioni avevano indotto alcune Procure

---

[272] Cfr. E. LORENZETTO, *op. cit.*, p. 139.

[273] In questo senso L. LUPARIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa (L. 18 marzo 2008 n. 48). I profili processuali*, cit., p. 720.

[274] In questi termini L. LUPARIA, Computer Crimes *e procedimento penale*, cit., p. 384. Sotto questo profilo, pare possibile tracciare un parallelo tra l'attività di duplicazione del dato informatico e lo *stub – test*

della Repubblica a procedere, antecedentemente alla L. 48/2008, alla clonazione di un *hard disk* mediante accertamento tecnico, qualificato in taluni casi come ripetibile, in altri come irripetibile[275].

Riallacciandosi a quest'ultimo aspetto, deve segnalarsi che l'opzione del legislatore in favore di una mera attività conservativa del dato digitale da acquisire a rischio deperimento da parte della polizia giudiziaria, prodromica a successive valutazioni da parte di un esperto, non lascia trasparire una presa di posizione netta circa la sua ripetibilità. Non può, infatti, ricavarsi un'indicazione in proposito dall'inserimento della relativa disciplina nell'art. 354, comma 2, c.p.p. Com'è noto, per costante orientamento giurisprudenziale, è ben possibile che anche attività destinate a transitare nel fascicolo del dibattimento a causa della loro irripetibilità originaria rientrino fra quelle compiute dagli ufficiali di polizia giudiziaria ai sensi dell'art. 354, comma 2, c.p.p.[276].

Ai fini dell'indagine che si sta conducendo, sembra opportuno muovere dagli approdi a cui si è pervenuti circa il collocamento sistematico dell'attività di duplicazione. Al riguardo, preme ribadire che, se pure la creazione di una copia forense, nell'ambito di una indagine informatica avente ad oggetto dati deperibili, assolve anche alla funzione essenziale di tutela della genuinità del dato[277], essa resta, comunque, inquadrabile nel *genus* dei provvedimenti idonei ad apporre un vincolo probatorio[278]. Ne consegue che, allorquando la polizia giudiziaria proceda alla duplicazione in parola di propria iniziativa, sarà necessaria una convalida da parte del pubblico ministero secondo quanto previsto dall'art. 355 c.p.p.

Difatti, realizzando una copia forense, gli inquirenti entrano in possesso, tramite una complessa operazione tecnica, di una vasta mole di dati, i quali

---

impiegato per ricercare residui di polvere da sparo – o i rilievi dattiloscopici: attività ricondotte ai rilievi di cui all'art. 354, comma 2, c.p.p., per le quali sono, tuttavia, necessarie competenze specialistiche. V., a tale riguardo, F. CASASOLE, *Le indagini tecnico-scientifiche: un connubio tra scienza e diritto in perdurante attesa di disciplina*, in *Dir. pen. proc.*, 2008, p. 1443 ss.

[275] In proposito, v. L. LUPARIA, *op. e loc. ult. cit.*

[276] Cfr., *ex multis*, con riferimento ai prelievi di polvere da sparo, Cass., Sez. I, 30 novembre 2005, Fummo, in *Arch. nuova proc. pen.*, 2007, p. 247.

[277] Cfr. E. LORENZETTO, *Utilizzabilità dei dati informatici incorporati su* computer *in sequestro: dal contenitore al contenuto passando per la copia*, in *Cass. pen.*, 2010, p. 1528.

[278] Circa la multifunzionalità dello strumento della copia forense, v. S. FASOLIN, *La copia di dati informatici nel quadro delle categorie processuali*, cit., p. 372 ss.

verranno, successivamente, selezionati e analizzati con idonea strumentazione; dati da cui potrà emergere la responsabilità penale dell'indagato.

Si tratta, a questo punto, di compiere un ulteriore passo in avanti nella ricerca e mettere in luce le criticità di simile metodo ablativo. Non si tratta di una mera apprensione di una *res* materiale, quanto, piuttosto, di una complessa operazione tecnica avente ad oggetto beni immateriali in grado di mettere a rischio la genuinità del dato.

Tanto basta per adombrare l'inidoneità di una mera facoltà del difensore di assistere, senza diritto di preavviso (art. 356 c.p.p.), alle operazioni di duplicazione di cui all'art. 354 c.p.p. a garantire un adeguato *standard* difensivo, come pure imposto dall'art. 24, comma 2, Cost.

La conseguenza di maggior rilievo che scaturisce dalle suesposte considerazioni è che il nodo problematico circa la ripetibilità o meno delle attività da porre in essere si riflette sulle garanzie difensive e, segnatamente, sulla necessità o meno di un previo avviso al difensore sul compimento dell'attività di *legal imaging*.

La giurisprudenza ha escluso la necessità di preavviso al difensore allorché gli ufficiali di polizia giudiziaria intendano procedere alla duplicazione di dati informatici, poiché si tratterebbe di una «operazione meramente meccanica, riproducibile per un numero indefinito di volte»[279]. Più in particolare, «l'attività di riproduzione dei *files* memorizzati non comporta, se effettuata da persona esperta della materia e con tutti gli accorgimenti necessari ad escludere le variazioni dello stato di fatto dei *file*, l'alterazione né la distruzione dell'archivio informatico, che rimane immutato e quindi consultabile ed accessibile nelle medesime condizioni, anche dopo l'intervento della polizia giudiziaria». Si tratterebbe, infatti, «di un'attività sempre reiterabile, alla cui esecuzione non è necessaria la partecipazione del difensore, poiché la stessa può essere ripetuta in contraddittorio, se ciò è richiesto dallo sviluppo dibattimentale del procedimento»[280].

[279] Cass., Sez. II, 4 aprile 2011, n. 13450, *inedita*. In termini Cass., Sez. II, 20 gennaio 2014, n. 2230 e n. 2231, *inedite*.
[280] Cass., Sez. II, 4 aprile 2011, n. 13450, *inedita*.

Tale impostazione rispetta la tradizionale distinzione tra accertamenti tecnici e rilievi invalsa in giurisprudenza[281]. Invero, secondo un orientamento costante, «mentre il rilievo consiste nell'attività di raccolta di dati pertinenti al reato, l'accertamento tecnico si estende al loro studio e valutazione critica secondo canoni tecnico-scientifici»[282].

Ora, poiché l'attività di duplicazione del dato informatico non importa né uno studio né una valutazione critica del dato in sé, la giurisprudenza qualifica *tout court* l'attività di acquisizione del dato quale rilievo[283]. Nonostante tale acquisizione venga realizzata mediante l'impiego di complesse attività tecnico-scientifiche, tale aspetto non viene considerato dirimente per collocare l'attività in parola nell'alveo degli accertamenti piuttosto che dei rilievi.

Ebbene, l'orientamento citato appare criticabile laddove assolutizza le proprie conclusioni in ordine alla ripetibilità delle operazioni che possono compiersi su dati informatici. A maggior ragione se si considera che non è affatto chiaro se, con l'espressione «attività di riproduzione di *files*», si intenda far riferimento alla mera creazione di una copia forense dei dati oppure ad un'analisi dei medesimi.

È doveroso ricordare, infatti, che, come si è osservato in dottrina, le attività investigative aventi ad oggetto il dato informatico potrebbero essere, in determinate ipotesi, impossibili da riprodurre in giudizio, sia per «caratteristiche intrinseche dell'operazione compiuta, di per sé insuscettibile di essere reiterata, sia [per] l'intervento di variazioni nella cosa oggetto di interesse non riconducibili all'azione umana,durante il tempo necessario per giungere al dibattimento»[284].

Ciononostante, l'esegesi giurisprudenziale appare in massima parte condivisibile. Ma non già in ragione della presunta ripetibilità dell'operazione di duplicazione, quanto per un diverso e duplice ordine di considerazioni. Seppure l'eventuale intervento del difensore possa, in determinate ipotesi, essere utile a verificare l'adempimento delle misure tecniche di conservazione del dato imposte dall'art. 354 c.p.p., deve giocoforza rilevarsi, a sostegno della conclusione cui

[281] V., in proposito, le osservazioni di S. FASOLIN, *La copia di dati informatici nel quadro delle categorie processuali*, cit., p. 375 ss.
[282] Così, per tutti, Cass., Sez. II, 10 luglio 2009, n. 34149, in *C.E.D. Cass.*, rv. 244950.
[283] Cfr. S. FASOLIN, *op. cit.*, p. 375 ss.
[284] Così S. FASOLIN, *op. cit.*, pp. 373-374.

pervengono i giudici di legittimità, che, in primo luogo, l'urgenza dell'acquisizione/conservazione del dato non pare consentire un previo avviso alla difesa. In secondo luogo, la preventiva informazione circa le attività d'indagine da compiere rischia di rendere inutile il successivo atto acquisitivo, giacché sarebbe concreto il rischio di inquinamento del dato probatorio.

2. La ripetibilità delle operazioni di analisi del dato digitale

Già si è avuto modo di chiarire che, per assicurare il dato digitale, la polizia giudiziaria può, ai sensi dell'art. 354 c.p.p., adottare le misure tecniche o impartire le prescrizioni necessarie ad assicurarne la conservazione, fino a poter creare un duplicato del dato mediante *bit stream image*[285]. In tal caso, il difensore potrà assistere all'atto senza aver diritto di essere previamente avvisato; ciò al fine di evitare il rischio di inquinamento probatorio e correlativo smarrimento delle informazioni utili a fini investigativi.

Qualora le analisi sul dato digitale acquisito vengano realizzate, in accordo con le miglior prassi della *digital forensics*, non già sulla memoria che in origine conteneva i dati né sulla copia forense di quest'ultima, bensì su un ulteriore duplicato del dato, può fondatamente sostenersi che ogni attività posta in essere dal consulente tecnico dell'accusa rientri fra gli accertamenti tecnici ripetibili di cui all'art. 359 c.p.p.[286]. Ed invero, gli accertamenti potranno essere ripetuti potenzialmente infinite volte, poiché il primo duplicato resterà a disposizione delle parti per qualsiasi verifica durante l'ulteriore corso del procedimento[287].

Si sarebbe tentati, allora, di concludere che non vi sia spazio alcuno per gli accertamenti tecnici irripetibili in ambito informatico. Le cose, però, non stanno in questi termini.

---

[285] Per i profili tecnici legati alla tecnica del *legal imaging*, v. F. NOVARIO, *L'attività di accertamento tecnico difensivo disposta su elementi informatici e la sua ripetibilità*, in *Cib. dir.*, 2011, pp. 79-80.

[286] Naturalmente, si presuppone che l'operazione di duplicazione sia stata compiuta mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità, come imposto dall'art. 354, comma 2, c.p.p.

[287] Sulle garanzie difensive offerte dalla procedura di duplicazione mediante *bit stream image*, cfr. A.E. RICCI, Digital evidence, *sapere tecnico-scientifico e verità giudiziale*, cit., p. 350 ss.

Ed invero, con precipuo riferimento all'analisi del dato, la principale condizione ostativa che impedisce di ritenere doveroso un preavviso al difensore, vale a dire il rischio di dispersione delle evidenze digitali, potrebbe, di fatto, non sussistere.

Nella prassi, come noto, l'acquisizione del dato informatico in senso stretto (*file*, *software* e così via) avviene solo successivamente all'apprensione dell'intero supporto informatico contenente il dato, quale ad esempio un *hard disk*. Ebbene, in simili ipotesi, non è azzardato sostenere la necessità di un accertamento tecnico irripetibile ai sensi dell'art. 360 c.p.p. sia per l'estrazione di *files* dall'attrezzatura sia, qualora non si sia potuto o voluto procedere alla creazione di una copia forense, per l'analisi dell'apparecchiatura[288].

Difatti, in tali casi, è insussistente il pericolo che l'indagato disperda o cancelli le informazioni contenute nel supporto informatico, giacché quest'ultimo non si trova più nella sua disponibilità. Appare, dunque, opportuno recuperare l'insegnamento di quell'attenta dottrina che sottolinea il diverso rischio, assai concreto, che qualsiasi operazione compiuta sul dato informatico si traduca in una irreparabile modifica dello stesso; e ciò, anche qualora si utilizzino i più moderni strumenti di *digital forensics*[289].

Di qui, la necessità di informare, senza ritardo, la persona sottoposta alle indagini, la persona offesa dal reato e i difensori dell'ora e del luogo fissati per il conferimento dell'incarico al tecnico specializzato in *digital forensics*, nonché avvisare la parte circa la facoltà di nominare propri consulenti tecnici (art. 360,

---

[288] In questo senso, v. M. DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche*, in *Cass. pen.*, 2012, p. 441 ss. *Contra* F. NOVARIO, *L'attività di accertamento tecnico difensivo disposta su elementi informatici e la sua ripetibilità*, in *Cib. dir.*, 2011, p. 84 ss. L'Autore ritiene, comunque, di ricondurre all'art. 360 c.p.p. il caso di «acquisizione di un'immagine forense di dati *a priori* difficile da cristallizzare per difficoltà tecniche, tali da rendere impossibile una corretta e completa immagine dei dati: ad esempio sistemi *software* personalizzati o *hardware* artiginali».

[289] Sul punto, v. L. LUPARIA, *La disciplina processuale e le garanzie difensive*, cit., p. 151 ss. Circa la «irripetibilità intrinseca» delle operazioni di *computer forensics*, v. A.E. RICCI, Digital evidence *e irripetibilità delle operazioni acquisitive*, in *Dir. pen. proc.*, 2010, p. 345. Con intenzione limitativa circa l'utilizzabilità del congegno di cui all'art. 360 c.p.p., si è, però, sostenuto in dottrina che non ogni modificazione del dato digitale riverbera sulla qualifica dell'accertamento tecnico informatico come attività ripetibile o meno. In quest'ottica, «la modificazione è rilevante quando snatura il risultato di un accertamento compiuto in prosieguo: qualora […] le variazioni non incidano sull'esito dell'operazione, consentendo di giungere allo stesso risultato, e sulla sua attendibilità, risulta evidente come le stesse non impediscano il compimento di un nuovo accertamento con caratteristiche del tutto identiche al precedente». Così S. FASOLIN, *op. cit.*, p. 380.

comma 1, c.p.p.). Difensori e consulenti tecnici potranno, quindi, partecipare agli accertamenti sul dato digitale, nonché formulare osservazioni e riserve circa le metodologie impiegate dall'esperto (art. 360, comma 2, c.p.p.).

Considerazioni analoghe valgono, a maggior ragione, con riferimento a quelle ipotesi in cui il dato digitale d'interesse investigativo si trovi contenuto in uno *smartphone*[290]. Vista l'impossibilità di realizzare un *legal imaging* del contenuto di quest'ultimo e, dunque, di operare i necessari accertamenti tecnici su un duplicato del dato, e considerata, altresì, la complessità e il pericolo di modifica del dato, è senza dubbio opportuna una anticipazione del contraddittorio alla fase delle indagini.

A questo punto, è doveroso chiedersi quale sia la sorte degli accertamenti informatici irripetibili, qualora il pubblico ministero non abbia adempiuto al proprio dovere di preavvisare il difensore. In astratto, due vie appaiono percorribili: ritenere sussistente una nullità di genere intermedio, poiché l'avviso al difensore è senza dubbio finalizzato all'assistenza dell'indagato, ai sensi dell'artt. 178, lett. *c*), c.p.p.; oppure, la più radicale sanzione dell'inutilizzabilità delle risultanze nel prosieguo del procedimento.

Non si tratta di una scelta di poco momento: se gli effetti delle due forme di invalidità consistono, in ambo i casi, nell'espunzione degli esiti degli accertamenti scientifici dal materiale probatorio, e nonostante entrambe le patologie siano rilevabili d'ufficio, sono, però, diversi i termini di rilevazione: entro i termini previsti dall'art. 180 c.p.p. e, in particolare, entro la deliberazione della sentenza di primo grado, qualora l'invalidità si sia verificata durante le indagini, in caso di nullità di *tertium genus*; rilevabilità in ogni stato e grado, qualora si ritenga sussistente una ipotesi di inutilizzabilità ai sensi dell'art. 191 c.p.p. Non solo: come noto, le due patologie differiscono quanto a sanatoria e rinnovazione degli atti invalidi, nonché quanto a conseguenze dell'invalidità sugli atti derivati.

In dottrina, la tesi che ravvisa, nell'ipotesi in parola, una nullità ha trovato maggior consenso, sull'assunto che non sarebbe prevista esplicitamente

[290] Fra le poche sentenze aventi ad oggetto il tema dell'utilizzabilità di dati contenuti in un telefono cellulare, si segnala, pur antecedentemente alla L. 48/2008, Cass., Sez. IV, 29 gennaio 2004, Lanzetta, in *Cass. pen.*, 2006, p. 536 ss., con nota di S. Renzetti.

l'inutilizzabilità dei risultati, ai sensi dell'art. 191 c.p.p., qualora il pubblico ministero non rispetti l'obbligo di avvisare senza ritardo il difensore degli accertamenti irripetibili da compiere (art. 360, comma 1, c.p.p.)[291].

Secondo tale orientamento, dal dovere del pubblico ministero di preavviso al difensore non potrebbe neppure ricavarsi un divieto probatorio implicito. Simile operazione ermeneutica condurrebbe, infatti, alla creazione di tanti divieti di utilizzazione quante sono le norme che disciplinano la formazione delle prove, «indipendentemente dall'importanza dei valori sottesi a ciascuna disposizione, con il rischio di pregiudicare l'accertamento dei fatti»[292]. Di qui, l'affermazione secondo cui il mancato preavviso al difensore integrerebbe una nullità di ordine intermedio degli accertamenti compiuti.

Una simile impostazione del problema va, però, recisamente disattesa. Appare agevole, infatti, ricavare il divieto probatorio in questione dall'art. 360, commi 4 e 5, c.p.p. Quest'ultima disposizione prevede che, qualora la persona sottoposta alle indagini abbia formulato richiesta di incidente probatorio e il pubblico ministero abbia deciso, nonostante gli accertamenti fossero differibili, di procedere ugualmente, i relativi risultati non possono essere utilizzati nel dibattimento.

Ora, è persino banale rilevare che, qualora il pubblico ministero non abbia avvisato l'indagato, quest'ultimo non potrà certo formulare la riserva in questione. Se così è, deve ritenersi che anche il mancato preavviso al difensore del compimento degli accertamenti, in quanto logico passaggio precedente alla riserva di incidente probatorio da parte dell'indagato, comporti l'inutilizzabilità dei risultati delle attività compiute. Ritenendo altrimenti, il sistema risulterebbe del tutto illogico: difatti, per evitare che i risultati investigativi siano colpiti da inutilizzabilità, al pubblico ministero basterebbe omettere ogni avviso al difensore. Conseguenza, questa, chiaramente inaccettabile, che si eleva a spia dell'erroneità della premessa.

---

[291] V., per tutti, M. DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche*, cit., p. 444.
[292] Così M. DANIELE, *op. e loc. ult. cit.*

Per fissare le idee, pare opportuno tirare le fila di quanto esposto finora. Laddove la perquisizione informatica, con successiva acquisizione del dato informatico – da intendersi quale sequestro *sui generis* – venga operata mediante verifica dei dati del sistema[293] e successiva duplicazione delle memorie mediante *bit stream image* in sede di primo contatto tra operanti e dato digitale, il preavviso alla difesa non pare doveroso, stante la natura di atto a sorpresa di simili mezzi di ricerca della prova e l'elevato rischio di smarrimento di dati digitali. Non vi sono, in questo caso, ostacoli a configurare le successive attività come ripetibili, qualora si proceda su un duplicato della copia forense ottenuta.

Viceversa, allorché sia stata sequestrata l'intera attrezzatura informatica e, dunque, contenitore (*hard disk*) e dati in esso contenuti (*file*, programmi ecc.), come quotidianamente accade, per lo meno in caso di apprensione presso privati, ragioni di cautela consigliano che ogni successiva attività sui medesimi venga posta in essere con l'anticipazione del contraddittorio ai sensi dell'art. 360 c.p.p.

Invero, in tal caso, il rischio di inquinamento probatorio non è certo da attribuire a condotte dolose dell'indagato, quanto, piuttosto, ad attività involontarie del consulente tecnico dell'accusa[294]; il che suggerisce una anticipazione del contraddittorio alla fase investigativa.

Qualora, poi, il pubblico ministero abbia proceduto ad accertamenti tecnici informatici irripetibili senza avvisare il difensore, i relativi risultati non potranno essere utilizzati, ai sensi dell'art. 360, comma 5, c.p.p.

Deve, però, registrarsi che la giurisprudenza è pervenuta a conclusioni antitetiche[295]. Segnatamente, si rinvengono, nelle pronunce dei giudici di legittimità, asserzioni *tranchant* quali «la lettura dell'*hard disk* di un *computer* sequestrato […] è attività di polizia giudiziaria volta, anche con urgenza, all'assicurazione delle fonti di prova»[296], ovvero «l'estrazione dei dati contenuti in un supporto informatico, se

---

[293] Ad esempio con attività di *preview*. Al riguardo, per i profili di *computer forensics*, cfr. G. COSTABILE, Computer forensics *e informatica investigativa alla luce della Legge n. 48 del 2008*, in *Cib. dir.*, 2010, pp. 497-498.

[294] Cfr. A.E. RICCI, Digital evidence *e irripetibilità delle operazioni acquisitive*, cit., p. 344.

[295] Per una panoramica dei *dictum* giurisprudenziali in tema, v. I.V. FELCHER, *Una rassegna giurisprudenziale con riferimento alla Legge n. 48 del 2008 e alle investigazioni digitali*, in *Cib. dir.*, 2013, p. 143 ss.

[296] Cass., Sez. III, 28 dicembre 2010, n. 45571, *inedita*.

eseguita da personale esperto in grado di evitare la perdita dei medesimi dati, costituisce un accertamento tecnico ripetibile»[297]. A sostegno di tale ultima affermazione, ricorre spesso il postulato secondo cui l'attività di estrazione di copia di un *file* da un *computer* costituisce atto ripetibile poiché è «sempre comunque assicurata la riproducibilità di informazioni identiche a quelle contenute nell'originale»[298].

Ebbene, deve preliminarmente rilevarsi che ad ingenerare perplessità e confusione nell'interprete, in una materia in cui l'utilizzo di un linguaggio tecnico è una necessità ineludibile, sta l'utilizzo, da parte dei giudici di legittimità, di termini eccessivamente generici, come emerge dal riferimento alla «lettura» del dato informatico. In prima battuta, tale sostantivo parrebbe evocare la mera operazione di apertura di un *file*; attività che potrebbe, in caso di urgenza, rientrare effettivamente tra le perquisizioni di polizia giudiziaria di cui all'art. 352, comma 1-*bis*, c.p.p. Tuttavia, il successivo richiamo ad un «*hard disk* sequestrato» chiarisce che, con il termine in questione, si è inteso richiamare un'attività valutativa più propriamente da ricondurre all'attività di un esperto ai sensi dell'art. 360 c.p.p. o, quantomeno, all'art. 359 c.p.p.

Ad ogni modo, l'orientamento in parola non coglie nel segno, poiché dimentica le peculiarità dell'accertamento su dati informatici. Più in dettaglio, l'inconfutabile dato che ogni sistema informatico o telematico presenta caratteristiche particolari sconsiglia l'adozione di un approccio unitario al fenomeno dell'analisi e gestione della prova informatica.

---

[297] Cfr., ancora, Cass., Sez. III, 28 dicembre 2010, n. 45571, *inedita*.

[298] Così Cass., Sez. I, 2 aprile 2009, Aversano Stabile, in *Dir. pen. proc.*, 2010, p. 338. Cfr. anche Cass., Sez. Un., 21 aprile 2010, n. 15208, *inedita*. Quest'ultima sentenza presenta, quale ulteriore profilo di interesse, la circostanza che, nel caso di specie, le attività di indagine sul dato digitale fossero state svolte in Gran Bretagna «con il rispetto delle regole procedurali inglesi»; secondo la Corte di Cassazione, tali attività «dev[ono] ritenersi legittim[e] anche per l'ordinamento italiano, in base alle convenzioni internazionali».V. anche Cass., Sez. I, 2 aprile 2009, Aversano Stabile, in *Cass. pen.*, 2010, p. 1522 ss., secondo cui «l'attività di estrazione di copia di "*file*" da un *computer* oggetto di sequestro […] 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». Pare cogliere nel segno, al riguardo, quella dottrina che imputa a tale orientamento giurisprudenziale di non aver colto la necessità di «rielaborazione del concetto di "irripetibilità" in rapporto all'atto di riproduzione elettronica». Tale ultima attività può avere, oltre che natura indifferibile, poiché il dato è soggetto a modificazione inevitabile, anche carattere non reiterabile, a seconda del *modus procedendi* adottato dal consulente tecnico. Di qui, l'importanza di verificare il protocollo utilizzato per le operazioni tecniche. Cfr. E. LORENZETTO, *Utilizzabilità dei dati informatici incorporati su* computer *in sequestro: dal contenitore al contenuto passando per la copia*, cit., p. 1530 ss.

In altre parole, è opportuno evitare, in materia di *digital evidence*, di cadere nella trappola dei postulati validi con riguardo ad ogni situazione. Quest'ultima soluzione appare, altresì, imposta dalle variabili fattuali con cui l'accusa, gli operanti o i consulenti devono fare i conti, prima fra tutte il rinvenimento di un attrezzatura digitale accesa oppure spenta[299]; nonché, dalla circostanza che non tutti i *software* di *digital forensics* sono in grado di operare analisi sul dato senza apportarvi alcuna modifica.

Se così è, deve, allora, verificarsi caso per caso se il dato abbia subito una modifica oppure se le tecniche di *digital forensics* utilizzate ne hanno garantito la preservazione[300]. Resta da affrontare un ultimo profilo. Come noto, l'istituto di cui all'art. 360 c.p.p. rappresenta una deroga al principio di formazione dibattimentale della prova; di qui, la necessità di una particolare cautela nel suo impiego. In effetti, l'accertamento tecnico irripetibile «costituisce ancora un terreno infido, ove l'alto tasso di strategicità continua ad influenzare l'esito del processo tanto per l'indice di scientificità che connota la prova quanto per la tendenziale irreversibilità dei risultati dell'accertamento»[301].

Eppure, in determinati casi, il contraddittorio anticipato ai sensi dell'art. 360 c.p.p. pare il miglior bilanciamento tra esigenze investigative e garanzie difensive alla luce dei principi del processo penale[302]. Simile soluzione presenta risvolti

---

[299] V. G. COSTABILE, Computer forensics *e informatica investigativa alla luce della Legge n. 48 del 2008*, cit., p. 486.

[300] Attualmente, il protocollo di duplicazione del dato informatico invalso presso le sezioni specializzate della Guardia di Finanza, al fine di garantire genuinità ed inalterabilità del dato informatico, è il seguente. Dapprima, il supporto che contiene i dati ritenuti di interesse investigativo da acquisire viene collegato, tramite apposito connettore, ad uno strumento di duplicazione denominato *Forensic Dossier*, il quale contiene un disco fisso non formattato e privo di partizioni. Inizia, quindi, la "cattura" del contenuto del supporto originale. Non si tratta di una copia, quanto di un vero e proprio clone: invero, l'apparecchio è in grado di replicare, sia dal punto di vista logico sia dal punto di vista fisico, l'intero contenuto dell'*hard disk*, comprese le regioni libere e quelle non più nella disponibilità del sistema che le ha generate. Successivamente, l'*hardware* in parola riversa il contenuto del supporto sotto analisi all'interno del disco vuoto, sotto forma di *file* DD-Linux inseriti in una *directory* appositamente creata. Il processo di acquisizione produce un valore esadecimale di *hash* MD5 SHA-256 dell'intero disco acquisito, il quale identifica univocamente lo stato dei *file* contenuti nel supporto originale al momento della clonazione. Perché l'operazione di clonazione possa ritenersi avvenuta con successo e il dato non modificato, il valore dovrà corrispondere a quello del duplicato realizzato con l'ausilio del *Forensic Dossier*. All'esito delle attività descritte, si scollega l'apparecchio il disco fisso originale e il suo duplicato; il contenuto di quest'ultimo viene riservato su ulteriori supporti, i quali verranno utilizzati per le analisi successive del materiale ottenuto.

[301] Così F. GIUNCHEDI, *Irripetibilità della prova ed accertamenti tecnico scientifici*, in *Arch. pen.*, 2012, n. 2, p. 11.

[302] In giurisprudenza, una cauta apertura all'utilizzo dell'art. 360 c.p.p. per l'espletamento di accertamenti su materiale informatico può rinvenirsi in Cass., Sez. II, 22 novembre 2011, n. 42969, *inedita*, ove si afferma

positivi sia per l'accusa, che può contare sull'utilizzabilità in dibattimento degli accertamenti compiuti, sia per la difesa, che può formulare osservazioni e riserve al momento degli accertamenti sul dato.

Già si è ricordato che, prima del conferimento dell'incarico al consulente tecnico, l'indagato può paralizzare il compimento dell'accertamento tecnico formulando riserva di incidente probatorio (art. 360, comma 4, c.p.p.). Tuttavia, il differimento può non essere disposto dal pubblico ministero qualora il ritardo renda impossibile l'utile esperimento delle operazioni; il che potrebbe verificarsi spesso con riferimento ad un dato immateriale ad elevata volatilità quale quello digitale.

Proprio l'istituto di cui all'art. 392, comma 1, lett. *f*), c.p.p. rappresenta un'ulteriore ipotesi di formazione della prova informatica in contraddittorio nella fase investigativa. Tale disposizione prevede la possibilità di richiedere che si proceda con incidente probatorio ad una perizia, qualora la prova riguardi una *res* il cui stato è soggetto a modificazione non evitabile. Deve, però, segnalarsi come lo strumento dell'incidente probatorio, pur utilizzato in alcuni pionieristici casi[303], non abbia raccolto i favori della prassi con riferimento all'analisi del dato informatico[304]. Ciò, con ogni probabilità, a causa della rilevata incompatibilità tra le dinamiche temporali di richiesta e di espletamento dell'incombente ed il carattere deperibile delle risultanze digitali[305].

---

che «la prassi giudiziaria ha evidenziato una casistica in cui è concreto il pericolo che l'*hard disk* sul quale vengono compiuti gli accertamenti può subire modifiche irreversibili, sicché l'accertamento ben può essere qualificato, nelle ipotesi suddette, come rientrante in quello di cui all'art. 360 c.p.p.».

[303] V. Cass., Sez. III, 21 gennaio 2003, Manganello, in *Cass. pen.*, 2004, p. 1339.

[304] Una rara, recente ipotesi di perizia su materiale informatico espletata in sede di incidente probatorio si rinviene in Cass., Sez. IV, 20 dicembre 2012, n. 49556, *inedita*. Tra le decisioni della giurisprudenza di merito, si segnala Ufficio G.I.P. Trib. Arezzo, Ord. 26 maggio 2003, *inedita*, la quale rigetta una richiesta di incidente probatorio relativa ad una perizia avente ad oggetto un *hard disk* con una motivazione assai curiosa: «il pericolo di modificazione non evitabile della cosa deve dipendere dalla natura della cosa in sé e non dalle modalità di custodia della stessa […] (nel caso di specie il P.M. avrebbe potuto […] impartire le direttive necessarie ad evitare pericoli di deterioramento, es. autorizzando l'effettuazione di piccoli fori di areazione sul cartone in cui è custodito il *computer* sequestrato)».

[305] In dottrina si è sottolineata la necessità, per ritagliare uno spazio operativo per l'incidente probatorio anche con riferimento a reperti a rischio di deperimento, di sfruttare la possibilità offerta dall'art. 400 c.p.p. Come noto, ai sensi di tale disposizione, qualora sia indispensabile procedere con urgenza all'incidente probatorio per assicurare l'assunzione della prova, i termini previsti dagli artt. 392 ss. c.p.p. possono essere abbreviati dal giudice, con decreto motivato, nella misura necessaria. V., in proposito, F. GIUNCHEDI, *Irripetibilità della prova ed accertamenti tecnico scientifici*, cit., p. 12.

3. Custodia e conservazione dei dati digitali. Un riconoscimento legislativo della funzione di *hash*?

L'indagine si è concentrata, finora, sui risvolti processuali delle attività di ricerca della prova informatica, con particolare riferimento al momento acquisitivo del dato, nonché sull'analisi di quest'ultimo, con precipuo riguardo alla qualificazione giuridica delle attività di *digital forensics*.

È opportuno, a questo punto, approfondire la disciplina relativa alla custodia e alla conservazione del dato digitale nell'intervallo tra l'acquisizione del dato o dei supporti e l'analisi di questi ultimi, nonché esaminare le attività da compiere a seguito dell'espletamento di simili attività. In particolare, si dovranno sviscerare le modalità di conservazione dell'attrezzatura e la possibilità di ricostruire a posteriori le operazioni compiute sul dato informatico in fase investigativa.

La L. 48/2008 si è occupata del primo dei profili indicati. Segnatamente, con riferimento alla custodia di dati, informazioni o programmi informatici sequestrati, si è stabilito che il custode debba essere avvertito, all'atto della consegna, circa l'obbligo di «impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria» (art. 259, comma 2, c.p.p.).

Inoltre, l'art. 260, comma 1, c.p.p. prevede che le cose sequestrate possano essere assicurate con il sigillo dell'ufficio giudiziario o «con altro mezzo, anche di carattere elettronico o informatico, idoneo a indicare il vincolo imposto a fini di giustizia».

Quest'ultima modifica è stata favorevolmente salutata quale riconoscimento legislativo della certificazione di conformità tra copia e originale tramite *hash functions*[306]. Appare, però, censurabile che la garanzia dell'apposizione di sigilli informatici sulle cose sequestrate sia stata prevista come meramente facoltativa.

[306] La funzione di *hash* serve a trasformare dei dati di lunghezza arbitraria in una stringa di dimensione fissa (valore di *hash*). Nella *digital forensics*, viene utilizzata per garantire la conformità all'originale del duplicato di dati informatici. V. L. LUPARIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa (L. 18 marzo 2008 n. 48). I profili processuali*, cit., p. 721, in particolare nt. 25, nonché, anteriormente alla novella,

Anche la giurisprudenza si è occupata dell'impiego della funzione di *hash* nell'ambito della *digital forensics*. Tuttavia, non già in riferimento alla disposizione dell'art. 260 c.p.p., quanto con riguardo all'utilizzo del sigillo digitale come «misura tecnica idonea ad assicurare la conservazione dei dati digitali e ad impedirne l'alterazione» ai sensi degli artt. 247, comma 1-*bis*, e 354, comma 2, c.p.p.[307].

A ben vedere, il tema affrontato dalla Suprema Corte va più propriamente ricondotto al novellato art. 260 c.p.p. Proprio i giudici di legittimità riconoscono che le procedure di *hashing* servono «a verificare l'integrità e la conformità all'originale del dato informatico sequestrato e conservato in copia su un apposito supporto»: tematica, questa, chiaramente attinente all'art. 260, comma 1, c.p.p., mentre il richiamo legislativo all'assicurazione dei dati digitali al momento della perquisizione informatica o dell'acquisizione in copia forense prevista dagli artt. 247, comma 1-*bis* e 354, comma 2, c.p.p. pare riferirsi al diverso problema della tutela della genuinità del dato al momento della duplicazione o della *live analysis* e, dunque, ad *hardware* di diverso tipo, quali i *write blocker*.

Secondo la Corte, «ogni […] valutazione di ordine tecnico circa la necessità di effettuare l'*hashing* per poter eventualmente verificare se la copia del *file* nel *compact disc* masterizzato sia uguale all'originale (e, quindi, se il *file* sia stato modificato o meno) è estranea al giudizio di legittimità, sia perché attiene essenzialmente alle modalità esecutive del sequestro sia perché comunque la normativa […] non individua specificamente le misure tecniche da adottare, limitandosi a richiamare le esigenze da salvaguardare attraverso idonei accorgimenti»[308].

S. ATERNO, *Acquisizione e analisi della prova informatica*, cit., p. 63. Anche la dottrina statunitense ha sottolineato l'importanza dell'utilizzo dell'algoritmo di *hash*: grazie alla creazione di questa "impronta digitale", l'esaminatore potrà verificare se stia lavorando o meno su una copia esatta dell'*hard-disk* originale, così come l'attività di quest'ultimo sarà in seguito verificabile da parte degli attori processuali. Cfr. P.H. LUEHR, *Real Evidence, Virtual Crimes. The Role of Computer Forensic Experts*, in *20 Crim. Just.*, 2005, p. 16 ss.

[307] Cfr. Cass., Sez. II, 13 marzo 2009, Bruno, in *Guida dir.*, 2009, n. 17, p. 84 ss., con commento di A. Cisterna.

[308] Così Cass., Sez. II, 13 marzo 2009, Bruno, cit., p. 86. Sul punto, nella giurisprudenza di merito, v. anche App. Milano, 11 novembre 2009, M.M.D.D., *inedita*, secondo cui l'utilizzo di un programma certificato per eseguire la copia forense di un *hard disk* (nel caso di specie, il *software Encase forensic*) assicura la corrispondenza tra copia e originale senza necessità di esperire la funzione di *hash*. Secondo la Corte,

Eppure, il tema della gestione del dato digitale appare meritevole di un maggior approfondimento, essendo legato a doppio filo a quella tutela della genuinità del dato che il legislatore ha inteso far assurgere a principio chiave in tema di indagini informatiche.

Viene in considerazione, a tal proposito, l'esigenza di documentare l'intera attività svolta, come garanzia di un corretto impiego delle *operating procedures* in presenza di un dato volatile e, dunque, soggetto a mutazione. Ciò appare tanto più necessario alla luce della scelta del legislatore di non accogliere un metodo unico per l'acquisizione e l'analisi della prova digitale, preferendo teorizzare una serie di principi cardine riassumibili, in ultima istanza, nella necessità di conservare e non alterare il dato informatico[309].

Inoltre, la redazione di una "traccia" delle operazioni tecniche poste in essere, ad esempio, in forma di *report* da allegare a quello conclusivo da parte dell'esperto[310] è di sicuro interesse anche per l'accusa, giacché essa consente di poter evitare contestazioni successive circa i risultati dell'analisi.

Simile documentazione cronologica, definibile quale catena di custodia[311], è, altresì, essenziale nel caso di analisi del dato informatico successivo al sequestro avvenuto ai sensi degli artt. 254 e 254-*bis* c.p.p. Nelle investigazioni in ambito informatico e telematico, invero, obiettivo dell'investigatore non deve essere un indiscriminato sequestro dell'intero materiale reperibile, ma il compimento di decisioni ragionate e registrate tali da poter essere sottoposte a critica nella successiva ricostruzione giudiziale.

Per assicurare la continuità probatoria, dunque, e, per tale via, escludere alterazioni indebite del materiale digitale, è necessario tenere un registro dell'intero materiale acquisito, numerando ogni supporto informatico oggetto dell'analisi,

---

dunque, «la procedura di "encase" di fatto supera, rendendola inutile, quella di "*hashing*" e cioè di verifica di corrispondenza tra i *files*». Cfr. A. CISTERNA, *Esperibilità della procedura di* hashing *valutabile solo in sede di merito*, in *Guida dir.*, 2009, n. 17, p. 84 ss.

[309] V., sul punto, S. FASOLIN, *La copia di dati informatici nel quadro delle categorie processuali*, cit., p. 373.

[310] Un'elencazione esaustiva delle informazioni che possono risultare da questo documento può rinvenirsi in V. CASINI, *Sanzionata dalla Cassazione l'omessa catena di custodia*, in *Dir. pen. proc.*, 2010, p. 1079.

[311] Sull'importanza di una corretta *chain of custody*, definita quale «metodologia di custodia e di trasporto, sia fisico sia virtuale delle *digital evidences*, […] finalizzata a consentire la tracciabilità e ri-percorribilità dell'acquisizione e dell'analisi degli elementi di prova digitali in qualunque fase del processo», cfr., già antecedentemente alla L. 48/2008, S. ATERNO, *op. e loc. ult. cit.* In proposito, v. anche A.E. RICCI, Digital evidence, *sapere tecnico-scientifico e verità giudiziale*, cit., pp. 348-349.

possibilmente effettuando rilievi fotografici, nonché annotando i numeri seriali; permettendo, così, alla difesa di poter ricostruire «*who handled the evidence [...] [to] keep track of where each piece of evidence came from and where it went after collection*»[312].

Una *chain of custody* così dettagliata si rende necessaria per quella differenza "ontologica" della prova informatica, cui si è più volte fatto cenno, strettamente connessa alla natura del dato oggetto del sequestro. Mentre nel caso del sequestro del corpo del reato o delle cose pertinenti al reato necessarie per l'accertamento dei fatti, ai sensi dell'art. 253 c.p.p., laddove esse abbiano carattere materiale, può essere sufficiente un'opera di catalogazione, nel caso in cui il dato trattato abbia natura informatica le possibilità di smarrimento, anche involontario, nonché di mancata analisi di importanti *byte* aumentano a dismisura. Corollario di tale ultima annotazione è che gli obblighi di repertazione devono essere più specifici e stringenti in relazione alle peculiarità della materia su cui si opera.

Anche la giurisprudenza ha evidenziato la necessità di garantire, in ogni fase del procedimento, l'identità del bene su cui si sono svolte le analisi rispetto alla *res* oggetto di sequestro. Ed allora, una volta che venga sollevata[313] siffatta questione, dal perito come dal difensore, si palesa come obbligatorio lo svolgimento di «accertamenti per stabilire se, nonostante la mancanza dei sigilli, [debbano] escludersi ipotesi di manomissione o di confusione tra reperti»[314].

Tuttavia, secondo la Corte di Cassazione, la mancata apposizione di sigilli non impedisce l'utilizzabilità della prova[315]. Segnatamente, la Corte ha ritenuto che la «mancata verbalizzazione dei modelli e degli altri elementi identificativi dei *computers* sequestrati, sia la mancata apposizione dei sigilli, non determinano alcuna nullità o, in genere, invalidità, del sequestro, dovendo considerarsi semplici irregolarità formali, prive di conseguenze sulla validità del provvedimento cautelare

---

[312] Così E. CASEY, *Digital evidence and Computer Crime*. *Forensic science*, *Computers and the Internet*, 2nd edition, Academic Press, 2004, p. 107.
[313] Nel caso di specie, lo stesso consulente tecnico aveva segnalato che il materiale da lui esaminato era difforme rispetto a quanto verbalizzato dagli operanti in sede di sequestro, e che la strumentazione informatica non era stata sigillata.
[314] Così Cass., Sez. III, 19 gennaio 2010, Pirrotta, cit., p. 1077.
[315] Cfr., ancora, Cass., Sez. III, 19 gennaio 2010, Pirrotta, cit., p. 1077.

e comunque inidonee a determinarne l'inutilizzabilità»[316]. Insomma, eventuali scorrettezze nella gestione della prova non possono trovare sanzione sul piano dell'invalidità, ma soltanto su quello del libero convincimento del giudice.

Lungo la direttrice giurisprudenziale, dunque, si è realizzata un'erosione del contenuto precettivo delle nuove disposizioni, esplicitamente additate quali «prescrizioni meramente indicative, la cui inosservanza non è prevista a pena di nullità»[317].

Si tratta, come si avrà modo di vedere a breve, di un'asserzione giurisprudenziale che attraversa quale *fil rouge* l'intera tematica della prova informatica, dal fallimento della catena di custodia al mancato rispetto dei canoni di genuinità e non alterazione del dato informatico.

[316] Cass., Sez. VI, 25 luglio 2011, n. 29652, *inedita*.
[317] Così, testualmente, Cass., Sez. III, 18 maggio 2012, n. 19085, *inedita*.

Capitolo IV – Le indagini informatiche tra esigenze di accertamento e diritti fondamentali

1. La disciplina in tema di conservazione di dati informatici da parte del *service provider*

Il decreto del pubblico ministero volto all'acquisizione di dati di traffico conservati dal fornitore di servizi di comunicazione elettronica costituisce, in un gran numero di procedimenti, tappa essenziale, seppure non decisiva, verso l'identificazione dell'autore di una condotta criminosa posta in essere in ambiente *Internet*. L'analisi dei dati di traffico in possesso del *provider* si rivela, altresì, utile per l'indagine giacché consente di ricostruire l'attività posta in essere in rete mediante una determinata connessione[318].

La conservazione dei dati di traffico e le modalità di accesso a questi ultimi sono disciplinate dall'art. 132 del D. Lgs. 196/2003, come modificato, da ultimo, dal D.L. 109/2008[319]. Tale disposizione, come noto, rappresenta un'eccezione al principio di non conservazione (*data protection*) accolto, in via generale, dall'art. 123, comma 1 del medesimo *corpus* normativo, secondo cui «i dati relativi al traffico riguardanti abbonati ed utenti trattati dal fornitore di una rete pubblica di comunicazione o di un servizio di comunicazione elettronica accessibile al pubblico sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica»[320].

---

[318] Cfr., in proposito, G. VACIAGO, *La disciplina normativa sulla* data retention *e il ruolo degli* Internet service provider, in L. LUPARIA (a cura di), Internet provider *e giustizia penale*, Giuffrè, Milano, 2012, p. 141.

[319] Decreto legge 30 maggio 2008, n. 109, *Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE*, in *G.U.*, 18 giugno 2008, n. 141.

[320] Cfr., in proposito, C. FATTA, *La tutela della* privacy *alla prova dell'obbligo di* data retention *e delle misure antiterrorismo*, in *Dir. inf.*, 2008, p. 399, nonché S. ATERNO-A. CISTERNA, *Il legislatore interviene ancora sul* data retention, *ma non è finita*, in *Dir. pen. proc.*, 2009, p. 282 ss.

L'art. 132, comma 1, del D. Lgs. 196/2003 prevede che l'*Internet service provider* conservi, per dodici mesi dalla data della comunicazione, i dati relativi al traffico telematico, esclusi i contenuti delle comunicazioni, «per finalità di accertamento e repressione dei reati»[321]. L'acquisizione di tali dati presso il fornitore avviene con decreto motivato del pubblico ministero, il quale può essere sollecitato in tal senso anche dal difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private (art. 132, comma 3, D. Lgs. 196/2003). Il difensore può, comunque, decidere di domandare direttamente i dati al *service provider* mediante la richiesta di documentazione di cui all'art. 391-*quater* c.p.p.

[321] La L. 48/2008 ha, inoltre, interpolato nell'art. 132 del D. Lgs. 196/2003 due commi, 4-ter e 4-quater, ai sensi dei quali il Ministero dell'interno, o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica e telematica della Polizia, dei Carabinieri o della Guardia di finanza, nonché i soggetti indicati nell'art. 226 disp. att. c.p.p., possono ordinare la conservazione e la protezione di dati relativi al traffico telematico ai fini delle investigazioni preventive di cui all'art. 226 disp. att. c.p.p., ovvero per «finalità di accertamento e repressione di specifici reati». Il provvedimento è prorogabile, per esigenze motivate, per una durata complessiva non superiore a sei mesi; esso può contenere specifiche modalità di custodia dei dati, nonché l'eventuale indisponibilità dei medesimi da parte dei fornitori, degli operatori di servizi informatici o telematici o di terzi. A tale ordine il fornitore deve ottemperare «senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento». Il fornitore è, altresì, obbligato a mantenere il segreto sull'ordine ricevuto e sulle attività poste in essere. Per una panoramica sulla nuova normativa, v. A. NOVELLINO, *Il Viminale può chiedere di conservare i dati*, in *Guida dir.*, 2008, n. 16, p. 69 ss., nonché G. DA VALLE, *L. 18.3.2008, n. 48 (Criminalità informatica) – Art. 10*, in *Legisl. pen.*, p. 306 ss. Numerosi i rilievi critici sollevati in dottrina sulle nuove disposizioni. In proposito, v. F. CERQUA, *Il difficile equilibrio tra la protezione dei dati personali e le indagini informatiche*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, cit., p. 236 ss., che evidenzia il «*deficit* di precisione nella formulazione della norma», giacché il richiamo non solo ai fornitori, bensì anche agli operatori di servizi informatici o telematici lascerebbe intendere che l'ordine di congelamento possa essere rivolto anche ai «soggetti che offrono direttamente servizi di comunicazione elettronica a gruppi delimitati di persone, [ai] gestori di siti *Internet* che diffondono contenuti sulla rete […] ed [ai] gestori di motori di ricerca». Cfr. anche C. FATTA, *La tutela della* privacy *alla prova dell'obbligo di* data retention *e delle misure antiterrorismo*, cit., p. 403; per l'Autrice, la formula relativa all'«accertamento e repressione di specifici reati» costituirebbe una «"valvola di apertura" che appare irragionevole, in quanto contenuta in una norma di carattere eccezionale e suscettibile di ampliare (più che risolvere) le perplessità che già circondano la disciplina della *data retention*». Ancora, cfr. A. STRACUZZI, Data retention*: il faticoso percorso dell'art. 132 Codice* privacy *nella disciplina della conservazione dei dati di traffico*, in *Dir. inf.*, 2008, p. 612 ss., secondo cui la conservazione dei dati di traffico telematico prevista dall'art. 132, commi 4-*ter* e 4-*quater* sfuggirebbe all'obbligo di applicare le misure di sicurezza di cui all'art. 132, comma 5, D. Lgs. 196/2003, poiché tale ultima disposizione non è stata modificata affinché ricomprendesse i nuovi commi 4-*ter* e 4-*quater*. Da ultimo, v. E. FORLANI, *La conservazione preventiva di dati informatici per l'accertamento di reati*, in *Dir. internet*, 2008, p. 520 ss., la quale ritiene che la conservazione preventiva dei dati rischia di trasformarsi in un indebito strumento di acquisizione di notizie di reato, nonché S. ATERNO, *Art. 10. Modifiche all'articolo 132 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196*, in G. CORASANITI-G. CORRIAS LUCENTE, Cybercrime*, responsabilità degli enti, prova digitale. Commento alla Legge 18 marzo 2008, n. 48*, Cedam, Padova, 2009, p. 231 ss. secondo cui il divieto, in capo al gestore, di trattare i dati richiesti non consente a quest'ultimo di rispondere compiutamente al richiedente.

La normativa, nata per recepire le indicazioni della Direttiva 2002/58/CE[322], è stata più volte modificata. Anteriormente alla riforma del 2008, il D.L. 144/2005[323] aveva previsto un "doppio binario"[324] per la conservazione dei dati relativi al traffico telematico[325]. Le informazioni dovevano essere conservate per sei mesi. Trascorso questo termine, i dati erano conservati per ulteriori sei mesi, ma al solo fine di accertare e reprimere i delitti di cui all'art. 407, comma 2, lett. *a*), c.p.p., nonché quelli in danno di sistemi informatici o telematici. Successivamente, l'acquisizione era autorizzata dal giudice, qualora egli ritenesse sussistere indizi sufficienti della commissione di uno fra i delitti richiamati. In caso di urgenza, il pubblico ministero poteva, ad ogni modo, disporre l'acquisizione con decreto motivato, da comunicare immediatamente e, comunque, non oltre ventiquattro ore

---

[322] La direttiva 2002/58/CE prevede, quale regola generale, all'art. 6, che i dati sul traffico – vale a dire, a mente dell'art. 2, «qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione» – debbano essere cancellati o resi anonimi quando non più necessari ai fini della trasmissione di una comunicazione (paragrafo 1), nonché ai fini della fatturazione e dei pagamenti di interconnessione (paragrafo 2) o ai fini della commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, qualora l'utente abbia prestato il consenso (paragrafo 3). Tuttavia, a tale principio generale gli Stati possono derogare qualora la restrizione al diritto alla protezione dei dati personali rappresentasse «una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero nell'uso non autorizzato del sistema di comunicazione elettronica» (articolo 15, paragrafo 1). La direttiva non precisa il tempo per cui i dati possano essere conservati, limitandosi ad un generico riferimento ad un «periodo limitato di tempo». In seguito, la direttiva 2006/24/CE ha precisato la forbice temporale entro cui gli Stati possono individuare il termine di conservazione ritenuto opportuno, vale a dire da sei mesi a due anni (art. 6, paragrafo 1). Eppure, l'art. 12 della medesima direttiva 2006/24/CE ha vanificato il disposto dell'art. 6, giacché si prevede espressamente che «uno Stato membro che si trovi ad affrontare circostanze particolari che giustificano una proroga, per un periodo limitato, del periodo massimo di conservazione di cui all'articolo 6, può adottare le necessarie misure». Sui profili critici della disciplina comunitaria v., ampiamente, C. FATTA, *La tutela della* privacy *alla prova dell'obbligo di* data retention *e delle misure antiterrorismo*, cit., p. 404 ss.

[323] Decreto legge 27 luglio 2005, n. 144, *Misure urgenti per il contrasto del terrorismo internazionale*, in *G.U.*, 27 luglio 2005, n. 173.

[324] Al riguardo, sia pure con riferimento alla conservazione dei dati di traffico telefonico, cfr. A. CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, cit., p. 622, nonché F. CERQUA, *Il difficile equilibrio tra la protezione dei dati personali e le indagini informatiche*, cit., p. 227 il quale sottolinea come, in realtà, la disciplina si riducesse «ad un unico obbligo per il fornitore di conservare […] i dati per il complessivo periodo, riferendosi la dualità unicamente ai diversi presupposti per l'acquisizione dei dati stessi da parte dell'autorità giudiziaria».

[325] Prima ancora del D.L. 144/2005, il Decreto legge 24 dicembre 2003, n. 354, *Disposizioni urgenti per il funzionamento dei tribunali delle acque, nonché interventi per l'amministrazione della giustizia*, in *G.U.* 29 dicembre 2003, n. 300, aveva eliminato il riferimento alla telefonia nell'art. 132, cosicché il riferimento alla conservazione *tout court* dei dati di traffico ben si prestava a ricomprendere anche i dati delle comunicazioni informatiche o telematiche. Tuttavia, la legge di conversione aveva nuovamente ridotto lo spettro applicativo della norma al solo traffico telefonico. In proposito, circa l'ampio dibattito sviluppatosi in sede legislativa sui pericoli di una tale «schedatura di massa», v. A. CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. proc. pen.*, 2005, p. 633 ss.

al giudice; quest'ultimo avrebbe dovuto decidere sulla convalida entro quarantotto ore; in assenza di convalida, i dati non sarebbero potuti essere utilizzati[326].

Oltre a ricondurre ad unità il termine di conservazione dei dati – dodici mesi, a prescindere dal titolo di reato per cui si procede – il D.L. 109/2008 ha, altresì, chiarito l'ambito applicativo dell'art. 132 D. Lgs. 196/2003. Ciò, per un verso, fornendo, in attuazione della direttiva 2006/24/CE, la definizione di dati relativi al traffico e all'ubicazione[327], nonché di indirizzo di protocollo *Internet* univocamente assegnato[328] (art. 1); per altro verso, elencando, all'art. 3, i dati, di futuro possibile interesse investigativo, che i fornitori devono provvedere a conservare[329].

---

[326] Sulle criticità della disciplina previgente v., ampiamente, F. CERQUA, *Il difficile equilibrio tra la protezione dei dati personali e le indagini informatiche*, cit., p. 227 ss.

[327] Ai sensi del D.L. 109/2008, è dato relativo al traffico «qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione, ivi compresi i dati necessari per identificare l'abbonato o l'utente», mentre costituisce dato relativo all'ubicazione «ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico, ivi compresi quelli relativi alla cella da cui una chiamata di telefonia mobile ha origine o nella quale si conclude».

[328] Il D.L. 109/2008 precisa che l'indirizzo di protocollo (IP) deve consentire «l'identificazione diretta dell'abbonato o utente che effettua comunicazioni sulla rete pubblica».

[329] L'elenco prevede sei categorie di dati da conservare; al loro interno, i dati da conservare variano a seconda che si tratti di telefonia da rete fissa o mobile, di accesso alla rete *Internet*, di posta elettronica oppure, in ultimo, di telefonia o invio di *fax*, *sms* e *mms* via *Internet*. Una delle categorie, quella relativa ai dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile, attiene, naturalmente, soltanto alla telefonia mobile. Per quanto riguarda le cinque categorie che qui interessano, anzitutto, con riferimento ai dati che occorrono per rintracciare ed identificare la fonte di una comunicazione, per l'accesso internet, occorrono «nome e indirizzo dell'abbonato o dell'utente registrato a cui al momento della comunicazione sono stati univocamente assegnati l'indirizzo di protocollo internet (*IP*), un identificativo di utente o un numero telefonico»; per la posta elettronica, «indirizzo *IP* utilizzato e indirizzo di posta elettronica ed eventuale ulteriore identificativo del mittente; indirizzo *IP* e nome a dominio pienamente qualificato del *mail exchanger host*, nel caso della tecnologia *SMTP* ovvero di qualsiasi tipologia di *host* relativo ad una diversa tecnologia utilizzata per la trasmissione della comunicazione»; per la telefonia o invio di *fax*, *sms* e *mms* via *Internet*, occorrono indirizzo *IP*, numero telefonico ed eventuale altro identificativo dell'utente chiamante, nonché i dati anagrafici dell'utente registrato che ha effettuato la comunicazione. Quanto ai dati necessari per rintracciare ed identificare la destinazione di una comunicazione, per la posta elettronica, è necessario conservare «l'indirizzo di posta elettronica, ed eventuale ulteriore identificativo, del destinatario della comunicazione; indirizzo *IP* e nome a dominio pienamente qualificato del *mail exchanger host* (nel caso della tecnologia *SMTP*), ovvero di qualsiasi tipologia di *host* (relativamente ad una diversa tecnologia utilizzata) che ha provveduto alla consegna del messaggio; indirizzo *IP* utilizzato per la ricezione ovvero la consultazione dei messaggi di posta elettronica da parte del destinatario indipendentemente dalla tecnologia o dal protocollo utilizzato»; quanto alla telefonia o invio di *fax*, *sms* e *mms* via *Internet*, «indirizzo *IP*, numero telefonico ed eventuale altro identificativo dell'utente chiamato; dati anagrafici dell'utente registrato che ha ricevuto la comunicazione; numero o numeri a cui la chiamata è trasmessa, nei casi di servizi supplementari come l'inoltro o il trasferimento di chiamata». Ancora, con riferimento ai dati necessari per determinare la data, l'ora e la durata di una comunicazione, i dati utili concernono, per l'accesso *Internet*, «data e ora (GMT) della connessione e della disconnessione dell'utente del servizio di accesso internet, unitamente all'indirizzo *IP*, dinamico o statico, univocamente assegnato dal fornitore di accesso *Internet* a una comunicazione e l'identificativo dell'abbonato o dell'utente registrato»; per la posta elettronica, «data e ora (*GMT*) della connessione e della disconnessione dell'utente del servizio di posta elettronica su *Internet* ed indirizzo *IP* utilizzato, indipendentemente dalla tecnologia e dal protocollo impiegato»; per la telefonia o invio di *fax*, *sms* e *mms* via *Internet*, «data e ora (*GMT*) della connessione e della disconnessione dell'utente

Così brevemente ricostruito l'*excursus* della disciplina in tema di *data retention*, deve precisarsi che la ragione dei continui aggiustamenti va ricercata nella difficoltà, da parte del legislatore, di addivenire ad un soddisfacente contemperamento di interessi: da un lato, le esigenze di accertamento dei reati; dall'altro lato, la necessaria tutela dei dati personali dell'utente[330].

Si tratta, a ben vedere, di una questione già emersa in ambito europeo. Difatti, nei *considerando* della direttiva 2006/24/CE, si affronta, in via preliminare, il problema della compatibilità di una disciplina in grado di imporre agli Stati membri la predisposizione di una normativa in materia di conservazione di dati con i dettami dell'art. 8 C.E.D.U., il quale, come noto, tutela il diritto al rispetto della vita privata e familiare, nonché del domicilio e della corrispondenza[331].

Secondo il Parlamento europeo ed il Consiglio, l'adozione di uno strumento concernente la conservazione dei dati costituirebbe una misura necessaria (considerando n. 9, Direttiva 2006/24/CE) in ragione dell'efficacia della conservazione di dati quale strumento investigativo, con particolare riguardo a reati di criminalità organizzata o terrorismo. In base a tale ricostruzione, la normativa sulla *data retention* troverebbe fondamento nel comma 2 del medesimo art. 8 C.E.D.U., il quale prevede la possibilità di misure limitative, previste dalla legge, al diritto alla riservatezza, laddove necessarie per la sicurezza nazionale o pubblica, nonché per la difesa dell'ordine e al fine di prevenire la commissione di reati.

La direttiva 2006/24/CE prevedeva una forbice temporale entro cui gli Stati potevano individuare il termine di conservazione ritenuto opportuno, vale a dire da

---

del servizio utilizzato su *Internet* ed indirizzo *IP* impiegato, indipendentemente dalla tecnologia e dal protocollo usato». Con riferimento ai dati necessari per determinare il tipo di comunicazione, essi concernono, per la posta elettronica e la telefonia via *Internet*, il servizio *Internet* utilizzato. In ultimo, quanto ai dati necessari per determinare le attrezzature di comunicazione degli utenti o quelle che si presume essere le loro attrezzature, essi consistono, per l'accesso *Internet* e telefonia o invio di *fax*, *sms* e *mms* via *Internet*, nel numero telefonico chiamante per l'accesso commutato (*dial-up access*), nonché nel *digital subscriber line number* (*DSL*) o altro identificatore finale di chi è all'origine della comunicazione.

[330] Sul diritto alla protezione dei dati personali, cfr. F. CERQUA, *Il difficile equilibrio tra la protezione dei dati personali e le indagini informatiche*, cit., p. 221 ss. Secondo l'Autore, il diritto in parola è «autonomo rispetto al più generale diritto alla riservatezza e non ha contenuto esclusivamente patrimoniale»; cfr. anche A. RODOLFI, *Il regime normativo della* data retention *nell'ordinamento italiano. Stato attuale e problematiche concrete*, in *Cib. dir.*, 2010, p. 147 ss.

[331] Si è sottolineato come le esigenze di ricerca della prova (informatica) debbano confrontarsi con «"nuove" manifestazioni dei diritti inviolabili dei cittadini, quali il diritto all'integrità, sicurezza e riservatezza dei sistemi informatici ed il diritto all'autodeterminazione informativa, […] da ricondurre alle manifestazioni dei diritti della personalità». Cfr. R. FLOR, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di Internet*, in www.penalecontemporaneo.it.

sei mesi a due anni (art. 6, paragrafo 1)[332]. Eppure, la portata precettiva di quest'ultima disposizione era vanificata già dall'art. 12 della medesima direttiva, in base alla quale «uno Stato membro che si trov[asse] ad affrontare circostanze particolari che giustificano una proroga, per un periodo limitato, del periodo massimo di conservazione di cui all'articolo 6, [poteva] adottare le necessarie misure»[333]. Per di più, le misure di sicurezza a protezione del dato erano lasciate alla totale discrezione dei Paesi membri.

Il problema del difficile contemperamento tra *data retention* e diritto alla riservatezza si è, in seguito, riproposto con riferimento alle singole normative di recepimento degli Stati Europei, con particolare riguardo ai diversi termini di conservazione dei dati.

Anche la Corte Costituzionale tedesca si è pronunciata sul tema. Segnatamente, con la sentenza 2 marzo 2010, le disposizioni di cui ai par. 113*a* e 113*b* del *Telekommunikationsgesetz*[334], nonché di cui al par. 100 del Codice di procedura penale tedesco, le quali prevedevano, in ossequio alla Direttiva 2006/24/CE, un termine semestrale di conservazione dei dati di traffico telefonico e telematico, sono state ritenute in contrasto con l'art. 10 della Costituzione tedesca, che tutela il segreto delle telecomunicazioni[335].

A parere dei giudici tedeschi, la conservazione di dati relativi al traffico telematico rappresenta una intrusione nella sfera privata del cittadino, giacché consente a chi analizzerà il dato di poter tratteggiare un quadro dell'appartenenza politica o della vita di relazione del soggetto i cui dati vengono conservati. Tale conservazione potrebbe, altresì, provocare la sensazione, in capo a coloro che usufruiscono dei servizi dell'*Internet service provider*, di essere oggetto di un

---

[332] Ciò, per l'accertamento di non meglio precisati «crimini gravi».

[333] Sui profili critici della disciplina comunitaria v., ampiamente, C. FATTA, *La tutela della* privacy *alla prova dell'obbligo di* data retention *e delle misure antiterrorismo*, cit., p. 404 ss.

[334] Introdotte nell'ordinamento tedesco dal *Gesetz zur Neuregelung der Telekommunikationsüberwachung* del 21 dicembre 2007.

[335] Per un'analisi della sentenza, v. R. FLOR, Data retention *e limiti al potere coercitivo dello Stato in materia penale: le sentenze del* Bundesverfassungsgericht *e della* Curtea Constiuţională, in *Cass. pen.*, 2011, p. 1954 ss.

costante monitoraggio[336]; la disciplina si risolverebbe, dunque, in ultimo, in una limitazione, sia pure indiretta, all'esercizio dei diritti fondamentali degli utenti.

Ciò non significa, per il *Bundesverfassungsgericht*, che il legislatore non possa prevedere *tout court* alcuna conservazione dei dati delle comunicazioni. La conservazione di dati deve, però, rappresentare l'eccezione, e non la regola. Ed invero, perché possano comprimersi i diritti fondamentali dell'individuo, dev'essere individuato, quantomeno, un concreto pericolo per la vita o per la libertà personale, oppure per la pubblica sicurezza; ed inoltre, la conservazione dei dati deve essere prevista solo con riferimento a ipotesi delittuose determinate. Mentre la creazione di un archivio di prove relativo a tutte le telecomunicazioni e per qualsiasi reato farebbe perdere proprio quel collegamento tra custodia dei dati ed esigenza repressiva che potrebbe, in astratto, giustificare siffatte misure.

Chiaro, insomma, l'insegnamento della Corte costituzionale tedesca: la normativa deve caratterizzarsi per precisione, trasparenza e deve essere improntata alla sicurezza nella conservazione del dato.

2. Il difficile bilanciamento tra diritto alla riservatezza ed utilità investigativa alla luce della sentenza 8 aprile 2014 della Corte di Giustizia Europea

La ricostruzione dei giudici tedeschi ha trovato un importante avallo da parte della Corte Europea di Giustizia, con la sentenza 8 aprile 2014 nelle cause riunite C-293/12 e C-594/12[337].

La questione sottoposta all'attenzione dei giudici europei risiedeva nella verifica circa la compatibilità fra la disciplina della Direttiva 2006/24/CE sulla conservazione dei dati di navigazione, atto prodromico allo svolgimento di indagini

[336] Interessanti spunti, a questo proposito, si rinvengono in J. PALFREY, *The Public and the Private at the United States Border with Cyberspace*, in *Miss. L. J.*, 2008, p. 241 ss.

[337] Per un commento, v. E. COLOMBO, "Data retention" *e Corte di Giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della direttiva 2006/24/CE*, in *Cass. pen.*, 2014, p. 2705 ss., nonché R. FLOR, *La Corte di Giustizia considera la Direttiva europea 2006/24 sulla c.d.* "Data retention" *contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in www.penalecontemporaneo.it.

informatiche sulla commissione di un fatto di reato, ed i diritti fondamentali dell'individuo stabiliti dalla Carta di Nizza.

Si tratta, com'è agevole avvertire, di una tematica che rileva ben oltre i confini della *data retention*. Ed invero, l'interrogativo cui i giudici europei erano chiamati a rispondere affonda le radici nella *vexata quaestio* del conflitto tra garanzie individuali e strumenti di indagine aventi ad oggetto *digital evidence*. Per tale ragione, appare utile ripercorrere i passaggi centrali del discorso sviluppato con impeccabile coerenza nella pronuncia in questione.

I parametri rispetto ai quali verificare la tenuta delle previsioni della Direttiva 2006/24/CE erano individuati dai giudici rimettenti[338] negli artt. 7, 8 e 11 della Carta fondamentale dei Diritti Europei. Più in dettaglio, l'immagazzinamento dei dati di carattere personale affinché le autorità nazionali competenti possano eventualmente accedervi potrebbe, in astratto, comprimere i diritti garantiti dagli articoli 7 e 8 della Carta; inoltre, la conservazione di dati inciderebbe sull'utilizzo, da parte degli abbonati o degli utenti registrati, dei mezzi di comunicazione e, di conseguenza, sull'esercizio della loro libertà di espressione, garantita dall'art. 11 Carta fondamentale. Di qui, la necessità di verificare se la normativa rispetti i doverosi requisiti di protezione dei dati appresi.

Preliminarmente, la Corte afferma che l'obbligo di conservazione di dati relativi alla vita privata di una persona e alle sue comunicazioni costituisce di per sé un'ingerenza nel diritto al rispetto della vita privata e della vita familiare di cui all'art. 7 della Carta di Nizza. Questo – si badi bene – a prescindere che le informazioni memorizzate abbiano carattere sensibile o meno e a prescindere dagli effetti di tale conservazione. Si tratta, allora, di verificare se le deroghe in parola siano necessarie e rispettino il contenuto essenziale dei diritti in questione; nonché, se siano rispondenti a finalità di interesse generale riconosciute dall'Unione, ovvero derivino dalla necessità di proteggere diritti e libertà altrui, conformemente all'art. 52 della Carta.

Ebbene, a parere dei giudici europei, quanto al primo aspetto, la *data retention* non pregiudica il contenuto essenziale dell'art. 7 della Carta di Nizza,

[338] Vale a dire, la *High Court* irlandese e la *Verfassungsgerichtshof* austriaca.

giacché è escluso che i *provider* e l'autorità giudiziaria vengano a conoscenza del contenuto delle conversazioni. Non è, parimenti, leso il nucleo fondamentale del diritto al trattamento dei dati personali (art. 8 Carta di Nizza), poiché l'art. 7 della Direttiva 2004/26/CE prevede regole specifiche in tema di protezione e sicurezza dei dati.

Quanto alla seconda problematica, l'obiettivo della disciplina oggetto dello scrutinio di compatibilità con la Carta di Nizza è individuato nella necessità di garantire la disponibilità dei dati a fini di indagine, accertamento e perseguimento di reati gravi; il che si inserisce nel più generale obiettivo di interesse generale di mantenimento della sicurezza e della pace.

Nonostante ciò, la normativa europea sulla conservazione dei dati di navigazione incontra, secondo la Corte, un insormontabile ostacolo nel principio di proporzionalità, inteso, sulla scia della costante giurisprudenza della Corte medesima[339], quale capacità di realizzare gli obiettivi perseguiti dalla normativa e senza superare i limiti di ciò che è idoneo e necessario al conseguimento degli obiettivi stessi, secondo un giudizio di adeguatezza del mezzo adoperato rispetto al fine.

Ed invero, il diritto al rispetto della vita privata rappresenta un diritto fondamentale le cui restrizioni devono palesarsi come strettamente necessarie. E ciò, soprattutto, in tutti quei casi in cui la conservazione di dati sensibili avviene automaticamente e laddove vi sia un concreto rischio di «*unlawful access and use*» di tali dati.

Questi i rilievi critici dei giudici comunitari. In primo luogo, la Direttiva 2006/24/CE concerne ogni comunicazione elettronica o traffico di dati senza alcuna differenziazione a seconda della gravità del reato che si intende accertare; la conservazione riguarda tutti i cittadini dell'Unione, a prescindere da qualsiasi elemento che indichi la commissione di un crimine e da eventuali obblighi di segretezza; inoltre, non vi è alcun rapporto tra il dato immagazzinato e la potenziale minaccia alla pubblica sicurezza[340].

---

[339] V., per tutti, Case C-343/09, Afton Chemical, EU:C:2010:419.

[340] In particolare, la conservazione dei dati «*is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely*

In secondo luogo, la Direttiva non prevede alcun *objective criterion* cui ancorare i limiti dell'accesso e conseguente uso dei dati conservati. Né si prevede alcuna specifica procedura per l'accesso al dato, così come non si specifica a quali fini il dato deve essere utilizzato.

In terzo luogo, si sottolinea la mancanza di una distinzione a seconda della gravità del crimine nella determinazione della forbice edittale, unitamente all'assenza di un criterio oggettivo in base al quale limitare la conservazione al periodo strettamente necessario.

Logico corollario è che, «*by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter*»[341]; di qui, l'invalidità della Direttiva.

Ora, la declaratoria di illegittimità in parola è destinata a ripercuotersi, sia pure in via soltanto indiretta[342], sulle normative di attuazione degli Stati membri dell'Unione e, dunque, anche della disciplina dettata nell'ordinamento italiano dal Codice *privacy*; anche se dovranno essere le Corti interne a stabilire la compatibilità delle singole norme di recepimento – tra loro assai diverse – della Direttiva 2006/24/CE.

Più in generale, i principi dettati dalla Corte Europea appaiono di grande rilevanza se mutuati sul terreno delle investigazioni informatiche. Quanto rilevato dai giudici europei, infatti, smentisce seccamente quella tesi, già propugnata nei considerando della Direttiva 2006/24/CE, secondo cui, nelle investigazioni in ambito digitale, il fine (l'indagine su fatti criminosi, anche gravissimi) giustifica i mezzi (la reiterata violazione o compressione di diritti e garanzie individuali).

---

to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences». Sono considerazioni che, all'evidenza, ben si adattano anche alla normativa dettata in Italia dal D.lgs 196/2003.

[341] La Corte, invece, non prende posizione circa la compatibilità della Direttiva 2006/24/CE con l'art. 11 della Carta di Nizza, ritenendo assorbenti le censure svolte rispetto agli artt. 7 ed 8 del testo convenzionale.

[342] E. COLOMBO, "Data retention" *e Corte di Giustizia*, cit., p. 2713, auspica che «gli Stati membri, di propria iniziativa, si adoperino per adeguare la disciplina della *data retention* ai diritti della persona […] così da individuare chiaramente quelle norme che oggi sono divenute contrarie al diritto comunitario (come interpretato dalla sentenza della Corte) e che, di conseguenza, devono essere disapplicate».

Quanto rilevato dalla Corte rappresenterà, dunque, punto di partenza necessario per il doveroso ripensamento, in ambito europeo, della normativa in tema di conservazione di dati, nonché per l'interpretazione delle norme vigenti nei singoli ordinamenti in tema di indagini informatiche.

3. La prova digitale "incostituzionale"

Già prima della sentenza *Digital Rights* c. Irlanda della Corte Europea di Giustizia, un altro giudice europeo aveva affrontato, sia pure in diversa prospettiva, il tema della lesione a principi fondamentali in conseguenza dell'invasività delle indagini informatiche. Segnatamente, la Corte Europea dei Diritti dell'Uomo, nella nota sentenza Robathin c. Austria[343], aveva affermato che la perquisizione con successivo sequestro di materiale informatico, realizzata all'interno di uno studio legale, integra una violazione dell'art. 8 C.E.D.U., *sub specie* del principio di non ingerenza nella corrispondenza, qualora non vengano rispettate le garanzie necessarie affinché sia assicurata una tutela effettiva al segreto professionale forense[344].

Sulla scia di questo *dictum*, la dottrina si è interrogata se l'orientamento giurisprudenziale in parola fosse idoneo a fondare «la costruzione di un'inutilizzabilità di tipo convenzionale, applicabile dal giudice italiano anche in assenza della sua previsione da parte della normativa processuale interna»[345].

In altre parole, stante l'assenza di un divieto probatorio esplicito che imponga di espungere dal materiale probatorio quello ottenuto mediante indagini informatiche irrispettose di diritti fondamentali, ci si è chiesti se tale divieto possa

---

[343] Corte Europea dei Diritti dell'Uomo, 16 gennaio 2008, n. 74336/01, in *Dir. inf.*, 2008, p. 82 ss.

[344] In particolare, nel caso di specie, erano emerse numerose criticità: durante le operazioni era mancato un effettivo controllo da parte del rappresentante del Consiglio Forense, il quale era impegnato a verificare la correttezza delle procedure relative al simultaneo sequestro di materiale cartaceo; non era stato redatto alcun verbale di sequestro; all'interessato non era stata data tempestiva informazione circa la documentazione informatica sequestrata, ovverosia i singoli *file* duplicati. A seguito del riconoscimento della violazione dell'art. 8 C.E.D.U., la Corte ha riconosciuto la spettanza al ricorrente di una somma di denaro a titolo di risarcimento per il danno non patrimoniale subito e per le spese giudiziarie sostenute. In proposito, v., *amplius*, M. STRAMAGLIA, *Il sequestro di documenti informatici: quale tutela per il segreto professionale forense?*, cit., pp. 834-835.

[345] Così M. DANIELE, *Indagini informatiche lesive della riservatezza. Verso un'inutilizzabilità convenzionale?*, in *Cass. pen.*, 2013, p. 371. La questione, naturalmente, appare ancor più rilevante ed attuale oggi a seguito della sentenza *Digital Rights* c. Irlanda.

desumersi dall'art. 8 della C.E.D.U., anche in considerazione del suo rango di norma interposta ai sensi dell'art. 117 Cost. Per tale via, dunque, il tema della prova informatica assunta in violazione di disposizioni di legge dettate in ambito convenzionale viene ad intersecarsi con il dibattuto tema della prova incostituzionale[346].

Va detto subito che, circa la possibilità di ricostruire una siffatta *exclusionary rule*, ha prevalso, fra i commentatori, l'orientamento negativo, sulla scorta di un duplice rilievo. Da un lato, si è rilevato che alla violazione dell'art. 8 C.E.D.U. non consegue automaticamente l'iniquità del processo ai sensi dell'art. 6 C.E.D.U. ed il dovere di ripetizione del giudizio[347]. Dall'altro lato, si è sostenuto che non ogni statuizione della Corte Europea dei Diritti dell'Uomo sarebbe vincolante; a maggior ragione in un ambito – le investigazioni informatiche – nel quale le regole dettate nel sistema italiano sarebbero già in grado di rispondere efficacemente agli obiettivi perseguiti dalla Corte, con particolare riguardo ai presupposti delle operazioni da compiere, alle modalità di svolgimento delle attività acquisitive, nonché ai controlli giurisdizionali su queste ultime[348].

Più in generale, la dottrina ha criticato la stessa configurabilità di una regola di esclusione su base convenzionale o costituzionale in presenza delle più comuni attività di indagine informatica, vale a dire le perquisizioni ed i sequestri

---

[346] Sull'argomento, è sempre attuale l'insegnamento di V. GREVI, *Insegnamenti, moniti e silenzi della Corte Costituzionale*, in *Giur. cost.*, 1973, p. 1181. V. anche G. ALLENA, *Riflessioni sul concetto di incostituzionalità della prova*, in *Riv. it. dir. proc. pen.*, 1989, p. 514 ss.; A. CAMON, *Sulla inutilizzabilità nel processo penale dei tabulati di traffico telefonico degli apparecchi «cellulari», acquisiti dalla polizia senza autorizzazione dell'autorità giudiziaria*, in *Cass. pen.*, 1996, p. 3721 ss.; ID., *Le riprese visive come mezzo di indagine, spunti per una riflessione sulle prove incostituzionali*, in *Cass. pen.*, 1999, p. 1206 ss.; F. CAPRIOLI, *Colloqui riservati e prova incostituzionale*, Giappichelli, Torino, 2000, *passim*; L. FILIPPI, *L'*home watching*: documento, prova atipica o prova incostituzionale*, in *Dir. pen. proc.*, 2001, p. 92 ss.; ID., *Ascolto e trascrizione di telefonate all'inquisito: sommarie informazioni o prova incostituzionale?*, in *Dir. pen. proc.*, 2001, p. 1396 ss.; C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Cedam, Padova, 2007, p. 153 ss. In giurisprudenza, in epoca recente, senza pretesa di completezza, si segnalano le seguenti pronunce: Corte Cost., sent. 11 aprile 2002, n. 135, in *Giur. cost.*, 2002, p. 2176 ss.; Corte Cost., Sez. Un., 28 marzo 2006, Prisco, in *Dir. pen. proc.*, 2006, p. 1213; C. Cost., sent. 7 maggio 2008, n. 149, in *Giur. cost.*, 2008, p. 1844 ss., con nota di E. Lamarque; C. Cost., sent. 30 novembre 2009, n. 320, in *Giur. cost.*, 2009, p. 4823 ss., con nota di M. Villani.

[347] V., a tal riguardo, anche con riferimento alla copiosa giurisprudenza della Corte Europea dei Diritti dell'Uomo citata, M. DANIELE, *Indagini informatiche lesive della riservatezza*, cit., p. 373, in particolare nt. 30 e 31. Invero, perché sia ravvisata una violazione dell'art. 6 C.E.D.U., è necessario, altresì, che i diritti della difesa non siano stati rispettati, e che le prove raccolte risultino inattendibili, tenendo conto le modalità con le quali sono state ottenute; ciò, anche tenendo conto dell'intero compendio probatorio a disposizione del giudicante. Si tratta, com'è agevole intuire, di criteri che implicano un alto tasso di discrezionalità in capo alla Corte.

[348] Cfr., ancora, M. DANIELE, *Indagini informatiche lesive della riservatezza*, cit., p. 372.

informatici, giacché si tratterebbe di attività sì potenzialmente lesive di diritti fondamentali, ma comunque disciplinate compiutamente dalla legge. Dunque, sarebbero le regole dettate dal legislatore a bilanciare «la protezione dei diritti fondamentali […] con le esigenze di accertamento dei fatti sulla base delle opzioni di politica criminale considerate preferibili […]». In altre parole, «in mancanza di una inutilizzabilità espressa, è lecito concludere che il legislatore abbia ritenuto che la violazione di un diritto fondamentale non sia sufficientemente grave da meritare la sanzione prevista dall'art. 191 c.p.p.»[349].

Il tema del rapporto fra diritti fondamentali e garanzie difensive, da un lato, e la necessaria invasività delle indagini informatiche nella sfera individuale, dall'altro, è stato affrontato in numerose pronunce anche dalla Corte di Cassazione. Segnatamente, i giudici di legittimità hanno affrontato l'argomento a seguito di ricorsi successivi alla apprensione di materiale informatico in possesso di un giornalista che abbia opposto il segreto professionale[350].

È bene chiarire che, in tali ipotesi, nemmeno la Corte di Cassazione si è spinta tanto in là da dichiarare l'invalidità degli elementi di prova ricavati dal materiale informatico appreso dagli operanti. Eppure, i giudici hanno riconosciuto la compressione delle garanzie costituzionali a seguito di tali attività: in particolare, «la disposta "clonazione" dell'intero *hard-disk* [del giornalista] implic[a] pesanti intrusioni nella sfera personalissima del giornalista»[351]; ed ancora, «l'attività investigativa [di perquisizione e sequestro informatici] comprom[ette] […] gravemente il diritto del giornalista alla riservatezza della corrispondenza e delle proprie fonti normative»[352].

Non solo. In un *dictum* relativo ad un caso analogo, la Suprema Corte ha dato atto della potenziale invasività degli strumenti investigativi in parola su «rilevanti posizioni presidiate costituzionalmente, quali il diritto di proprietà e, per una

---

[349] Cfr. M. DANIELE, *Indagini informatiche lesive della riservatezza*, cit., p. 370.
[350] V., per tutte, Cass., Sez. I, 4 luglio 2007, Pomarici, in *Cass. pen.*, 2008, p. 2946 ss. Quanto all'inutilizzabilità dei risultati investigativi per violazione dell'art. 8 C.E.D.U., la questione non risulta essere stata trattata diffusamente dalla Corte di Cassazione. La questione era stata sollevata dalla difesa in Cass., Sez. III, 24 luglio 2013, C.P., *inedita*, ma i giudici di legittimità non hanno affrontato in dettaglio il problema, giacché l'avvenuta restituzione del materiale in sequestro aveva reso, secondo i giudici, carente di interesse il gravame interposto.
[351] Cass., Sez. I, 4 luglio 2007, Pomarici, cit., p. 2951.
[352] V. nota precedente.

giornalista, anche la libertà d'informazione (art. 21 della Costituzione), alla quale sono connesse la garanzia del segreto professionale e la riservatezza delle fonti di informazione»[353].

Da qui al conferimento, in dottrina, di una patente di legittimità alla perquisizione ed al sequestro informatici connessa al rispetto di determinati canoni da parte degli inquirenti, il passo è stato breve. E così, si è sostenuto che, perché l'attività investigativa sia compatibile con l'art. 8 C.E.D.U., sarebbe necessaria «l'indicazione [nel decreto di perquisizione] di "parole chiave" specifiche rispetto all'oggetto di prova e comunque collegate alla regiudicanda; [nonché] la predisposizione di adeguate garanzie di "custodia" del materiale sequestrato, tali da evitare intrusioni arbitrarie da parte degli organi pubblici prima del compimento di ogni attività processuale […]»[354].

Si tratta di considerazioni pienamente condivisibili. Resta, però, aperto il problema circa l'esatta sanzione, sotto il profilo dell'invalidità, che deve conseguire alla violazione di canoni costituzionali nella ricerca della prova digitale; inoltre, deve tenersi a mente la difficoltà, per l'interprete, di rivenire il parametro costituzionale cui ancorare la declaratoria di invalidità della prova, con correlativo margine di discrezionalità in capo al giudice.

4. Violazione degli *standard* metodologici propri della *computer forensics* ed invalidità

Così come manca nel codice di rito una disposizione espressa che preveda l'inutilizzabilità di quelle risultanze probatorie frutto di attività lesive dei diritti fondamentali e, in particolare, del diritto alla riservatezza, manca, parimenti, un divieto d'uso esplicito relativo alle prove informatiche raccolte senza il rispetto dei

[353] Cass., Sez. I, 31 maggio 2007, Sarzanini, in *Dir. inf.*, 2008, p. 741.
[354] Così F.M. MOLINARI, *op. cit.*, p. 714. Sugli *step* necessari per tutelare la segretezza della corrispondenza informatica, tutelata dall'art. 15 Cost., v., altresì, A. LOGLI, *Sequestro probatorio di un* personal computer, cit., p. 2957 ss., nonché L. BACCHINI, *Il sequestro probatorio nei confronti del giornalista non indagato*, cit., p. 743 ss. Ancora, sul rapporto tra sequestro di un *personal computer* e la tutela della segretezza e della riservatezza, cfr. P. TROISI, *Sequestro probatorio del* computer *e segreto giornalistico*, cit., p. 768 ss.

requisiti essenziali della genuinità e non alterazione del dato informatico previsti dalla L. 48/2008.

In verità, il dibattito sulle eventuali patologie della prova conseguenti alla raccolta della *digital evidence* in violazione delle *best practices* acquisitive aveva appassionato la dottrina già anteriormente alle modifiche normative del 2008. Segnatamente, i primi commentatori avevano sostenuto, pur in assenza di regole *ad hoc* dettate per le indagini informatiche, che l'acquisizione della prova in spregio dei corretti criteri scientifici comportasse comunque l'inutilizzabilità delle risultanze, giacché queste ultime sarebbero state inidonee ad assicurare un accertamento attendibile dei fatti di reato[355].

A seguito dell'inserimento di una disciplina apposita per le indagini informatiche nel codice di rito, ha trovato ulteriore linfa la ricostruzione secondo cui il mancato rispetto dei requisiti di genuinità e non alterazione legislativamente imposti comporterebbe l'invalidità della prova. Non vi è, però, concordia circa l'effettiva sanzione processuale operante nei confronti del materiale probatorio spurio: nullità, secondo alcuni; inutilizzabilità, secondo altri[356].

Quanto alla prima tesi, si è affermato che «il modo col quale si raccoglie una certa informazione influisce direttamente sulla capacità dimostrativa della stessa informazione. Se, dunque, non fossero attuate le misure di conservazione e salvaguardia dei dati originali, l'ispezione o la perquisizione sarebbero nulle; di conseguenza, anche le prove raccolte […] sarebbero [nulle]»[357]. In sintesi, le misure di salvaguardia del dato rappresenterebbero uno «speciale requisito […] [che] si configura come un elemento costitutivo [delle fattispecie delle ispezioni e delle perquisizioni informatiche], sicché la sua imperfezione o la sua assenza impedisce l'integrazione delle medesime […] [e] comport[a] l'invalidità del mezzo di ricerca

---

[355] Teorizza tale inutilizzabilità per *unreliability* della prova L. LUPARIA, *Il caso "Vierika": un'interessante pronuncia in materia di* virus *informatici e prova penale digitale*, in *Dir. internet*, 2006, p. 157 ss.; v. anche ID., *La disciplina processuale e le garanzie difensive*, cit., p. 198.

[356] L'ardente dibattito dottrinale è ripercorso da F. CAJANI, *Il vaglio dibattimentale della* digital evidence, in *Arch. pen.*, 2013, p. 837 ss.; cfr. anche F. GIUNCHEDI, *Le* malpractices *nella* digital forensics*. Quali conseguenze sull'inutilizzabilità del dato informatico?*, in *Arch. pen.*, 2013, p. 821 ss., nonché D. LA MUSCATELLA, *La ricerca della prova digitale e la violazione delle* best practices*: un'attività investigativa complessa tra recenti riforme e principi consolidati*, in *Cib. dir.*, 2011, p. 221 ss.

[357] Così A. VITALE, *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico*, cit., p. 509.

della prova, il quale, più esattamente, risulterà nullo ai sensi degli artt. 178 lett. *c*) e 180 c.p.p.»[358].

Con riguardo alla seconda tesi, si è sostenuto che le prove informatiche acquisite in violazione dei canoni codicistici debbano essere considerate inutilizzabili, per diverse ragioni. Una corrente di pensiero afferma che la L. 48/2008 avrebbe inteso porre divieti probatori impliciti circa l'uso di risultanze probatorie informatiche inquinate, alla cui violazione consegue l'operatività dell'art. 191 c.p.p.[359]. Per un altro orientamento, giacché la tutela della genuinità della prova rappresenterebbe un'estrinsecazione del più generale diritto di difesa costituzionalmente tutelato, la violazione delle regole poste a tutela dell'integrità della prova dovrebbe condurre ad un'ipotesi di inutilizzabilità delle risultanze per violazione della legge fondamentale[360]. Ancora, un settore della dottrina ha affermato che la sanzione dell'inutilizzabilità si fonderebbe sulla inidoneità della fonte di prova acquisita in violazione dei canoni codicistici a provare alcunché, giacché l'attendibilità delle risultanze sarebbe irrimediabilmente compromessa[361].

---

[358] Ancora A. VITALE, *op. loc. ult. cit*.

[359] In questo senso L. MARAFIOTI, Digital evidence *e processo penale*, cit., p. 4522, nonché L. LUPARIA, Computer crimes *e procedimento penale*, cit., p. 389, secondo cui tale soluzione sarebbe imposta dalla «ricorsività di incisi codicistici […] facenti esplicito e continuo riferimento alla doverosità dell'utilizzo di metodiche che assicurino la genuinità della prova elettronica»; d'altra parte, secondo l'Autore, «pensare a questa normativa nei termini di una *lex imperfecta*, priva di penalità processuali per la sua violazione, sembra riecheggiare situazioni del passato, superate dalla riforma del 1988, e rischia di ingenerare prassi devianti e perniciose scorciatoie nell'operato dei protagonisti dell'inchiesta penale». Cfr. anche A. MONTI, *La nuova disciplina del sequestro informatico*, cit., pp. 208-209, nonché S. VENTURINI, *Sequestro probatorio e fornitori di servizi telematici*, in L. LUPARIA (a cura di), Internet Provider *e giustizia penale*, cit., p. 124.

[360] In quest'ottica, circa l'esistenza, accanto all'inutilizzabilità "patologica", di una inutilizzabilità "costituzionale", v. M. BERGONZI PERRONE, *Il mancato rispetto delle disposizioni della Legge n. 48 del 2008 in tema di acquisizione probatoria informatica: per una ipotesi sanzionatoria non prevista esplicitamente dal dato normativo*, in *Cib. dir.*, 2013, p. 128.

[361] Cfr. E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, cit., la quale parte dal presupposto che «la *digital evidence* ottenuta o duplicata con metodi impropri o comunque non verificabili equivale a un *quid* diverso da quello originariamente rinvenuto e […] mette a disposizione del giudice un dato adulterato. […] Sotto un profilo generale, dunque, quel *deficit* tecnico nell'acquisizione del dato informatico andrebbe ricondotto a una situazione di inidoneità probatoria della risultanza in sé e di qualsiasi ulteriore mezzo di prova finalizzato ad analizzarla. Ne deriverebbe il dovere giudiziale di escludere già in fase di ammissione della prova (art. 190 c.p.p.) l'evidenza digitale rilevata, con conseguente inutilizzabilità della stessa ovvero della sua successiva analisi tecnica in quanto acquisite, entrambe, in violazione di un divieto stabilito dalla legge (art. 191, comma 1, c.p.p.)». Secondo altri Autori, l'attendibilità della prova quale criterio per la sua ammissibilità (ed in seguito per la sua valutazione) troverebbe referente codicistico nell'art. 189 c.p.p. Tale disposizione non riguarderebbe soltanto la prova atipica, ma costituirebbe norma generale connaturata al processo accusatorio e, dunque, relativa a tutti i mezzi di ricerca della prova. Si tratta, com'è agevole intuire, di una ricostruzione debitrice, per un verso, di quella inutilizzabilità per *unreliability* già teorizzata antecedentemente alla L. 48/2008 e, per altro verso, della teoria anglosassone della *unfair evidence*. Cfr., in proposito, D. LA MUSCATELLA, *La genesi della prova digitale: analisi prospettica dell'ingresso dell'informatica forense nel processo penale*, in *Cib. dir.*, 2012, pp. 390-391.

Vi sono, però, anche esegesi del tutto antitetiche rispetto a quelle appena menzionate. Segnatamente, l'assenza di una espressa sanzione conseguente alla mancata osservanza dei canoni dettati dalla L. 48/2008 ha portato alcuni a ritenere che «l'inosservanza delle misure tecniche idonee ad assicurare la salvaguardia della genuinità dei dati e delle informazioni raccolte si risolv[a] sotto il profilo della valutazione della prova ed in particolare sul crinale della fondatezza dei risultati acquisiti»[362], e non sotto il profilo dell'invalidità. Di qui, la necessità che il giudice, al più, debba cercare elementi esterni di riscontro al materiale probatorio informatico "debole" in quanto non genuino oppure alterato.

Così ricomposto il mosaico degli indirizzi dottrinali, deve evidenziarsi che quest'ultima ricostruzione ha incontrato i favori della giurisprudenza. In particolare, già nel *leading case* "Vierika"[363], il Tribunale di Bologna enunciò una *regula iuris* destinata ad essere ripresa in maniera pressoché unanime dalla giurisprudenza successiva: vale a dire, il giudice non ha il potere di escludere a priori i risultati di una tecnica informatica utilizzata ai fini forensi solo perché alcune fonti ritengono che ne esistano di più corrette, «in assenza della allegazione di fatti che suggeriscano che si possa essere astrattamente verificata nel caso concreto una qualsiasi forma di alterazione dei dati e senza che venga indicata la fase delle procedure durante la quale si ritiene essere avvenuta la possibile alterazione»[364]. Tesi, questa, decisamente da respingere, giacché, com'è stato esattamente osservato, si tratta di «un *onus probandi* del tutto anomalo [che] si risolve in una vera e propria

[362] Così G. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, cit., p. 190.
[363] Questa, in breve, la vicenda: un consulente informatico era imputato dei reati previsti dagli artt. 615-*ter* e 615-*quinquies* c.p. per aver messo in circolazione un *virus* informatico denominato "Vierika". Il *worm* si diffondeva attraverso l'invio inconsapevole di *e-mail* da parte di quanti avessero incautamente aperto l'allegato "infetto" a loro pervenuto. Ben lungi dall'essere una semplice immagine digitale, l'accesso al *file* provocava una serie di modificazioni del sistema operativo fra cui la modifica della pagina iniziale del *browser* di navigazione. All'identificazione dell'imputato si era pervenuti a seguito dell'acquisizione di tracce informatiche registrate nel *server* dell'*Internet Service Provider*, mediante le quali era stato identificato l'amministratore del sito in questione. Un approfondita disamina del *dictum* si rinviene in L. LUPARIA, *Il caso "Vierika"*, cit., p. 156 ss.
[364] Così Trib. Bologna, 22 dicembre 2005, n. 1823, in *Dir. internet*, 2005, p. 153.

probatio diabolica, posto che il dato originario, dopo la modifica, risulta perlopiù irrecuperabile»[365].

Non solo. Secondo i giudici bolognesi, quand'anche il metodo utilizzato dalla polizia giudiziaria non dovesse ritenersi conforme alla miglior pratica scientifica, si perviene a risultati comunque liberamente valutabili dal giudice.

Si tratta di affermazione ancora oggi pedissequamente ripetuta dalle corti. Vero è che si sono registrate, di recente, timide aperture nel senso di ritenere inutilizzabile la prova non genuina[366]; tuttavia, è altrettanto vero che, nella maggior parte dei casi, persino laddove la difesa riesca a provare l'alterazione dei dati appresi, i giudici non rilevano l'invalidità della prova, ma, al più, si affrettano a rimarcare la presenza di elementi probatori esterni che la corroborano[367].

Ora, bastano pochi rilievi a denotare le carenze di una simile prospettiva. Il punto di partenza per la soluzione della questione appare offerto, ancora una volta, dalla natura fragile e volatile del materiale informatico. Da tali caratteri deriva un inevitabile corollario: l'impiego di metodi di acquisizione scorretti muta la natura stessa della prova, la quale perde, una volta per tutte, l'idoneità a provare alcunché, in quanto irrimediabilmente contaminata.

Detto altrimenti, occorre evidenziare che, con riferimento alla *digital evidence*, eventuali violazioni nelle modalità di apprensione del dato incidono inevitabilmente sull'essenza del medesimo, poiché il contenuto viene modificato[368].

Alla luce di quest'ultima precisazione, i canoni di genuinità e non alterazione della prova legislativamente imposti dalla L. 48/2008 assumono diversa valenza:

---

[365] Così L. MARAFIOTI, Digital evidence *e processo penale*, cit. p. 4521; in questo senso anche L. LUPARIA, *op. loc. ult. cit.*, p. 158, il quale ritiene che simile onere della prova si collochi «al di fuori dell'architettura sistematica del nostro ordinamento processuale»

[366] Ad esempio Cass., Sez. III, 16 ottobre 2014, n. 43304, *inedita*, secondo cui «le osservazioni contenute nel ricorso […] non sono sufficienti nel caso concreto a rendere dubbia la genuinità della prova acquisita e, quindi, a farla ritenere inutilizzabile».

[367] Ciò, persino in provvedimenti attenti al tema della genuinità del dato informatico. Cfr. Trib. Vigevano, 17 dicembre 2009, Stasi, *inedita*. La sentenza dà atto dell'intervenuta alterazione del materiale informatico a seguito di scorrette condotte di accesso da parte degli operanti in fase investigativa. Eppure, si ribadisce la necessità di riscontri esterni a simile materiale non genuino. Pare, dunque, cogliere nel segno chi ha teorizzato che, in ambito di *digital evidence*, «il libero convincimento diventa viatico per legittimare un approccio antiformalistico in tema di prova». Così L. MARAFIOTI, Digital evidence *e processo penale*, cit., p. 4521.

[368] In quest'ottica, sia pure con riferimento, più in generale, al tema della *scientific evidence*, C. CONTI, *Il volto attuale dell'inutilizzabilità: derive sostanzialistiche e bussola della legalità*, in *Dir. pen. proc.*, 2010, p. 790.

non già mere disposizioni d'auspicio, ma veri e propri divieti impliciti presidiati dalla sanzione dell'inutilizzabilità.

Si chiarisce in tal modo anche un altro aspetto della complessa tematica in esame, ovvero la ricerca del parametro cui ancorare la declaratoria di invalidità; precisamente, esso va rinvenuto nel dovere di adottare «misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione» previsto dagli artt. 244, comma 2, 247, comma 2, 352, comma 2, e 354, comma 2, c.p.p., e dall'obbligo di acquisire i dati informatici mediante «procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità» ai sensi degli artt. 254-*bis* e 260, comma 2, c.p.p.

Ciò precisato, l'attenzione si sposta sulla possibilità, assai dibattuta in dottrina, di configurare divieti probatori impliciti. Ebbene, sul punto, appare opportuno recuperare quell'insegnamento giurisprudenziale secondo cui «l'inutilizzabilità, ai sensi dell'art. 191, comma 1, c.p.p. può derivare soltanto dalla violazione di un divieto di acquisizione che, quando non sia esplicito, può riconoscersi come implicito […] in relazione alla natura o all'oggetto della prova […]»[369]. Ed appunto, come si è avuto modo di illustrare, le interpolazioni della L. 48/2008 tutelano proprio la natura volatile della prova informatica da possibili involontarie contraffazioni.

L'assunto che precede è avvalorato dall'analisi delle conseguenze cui approda quella tesi che assegna al giudice il compito di valutare l'idoneità probatoria di quelle risultanze digitali apprese mediante procedure scientificamente scorrette. Ebbene, per tale via, si assegna al magistrato un compito estremamente arduo di verifica, caso per caso, se le condotte scorrette degli operanti abbiano o meno compromesso l'attendibilità del materiale probatorio[370]. Dunque, una ricostruzione di tal guisa, ben lungi dal restituire al giudice la doverosa funzione di

[369] Cass., Sez. I, 27 maggio 1994, Mazzuoccolo, in *Arch. n. proc. pen.*, 1994, p. 504.
[370] Si ricordino, a tal proposito, le icastiche osservazioni di M.R. DAMAŞKA, *Il diritto delle prove alla deriva*, cit., p. 52: «non è forse il giudice medio […] perplesso riguardo ad arcane intuizioni scientifiche? La scienza moderna pone sempre più di fronte a tutti i giudici "generalisti", abbiano essi o no una preparazione giuridica, informazioni che solo degli esperti possono capire senza difficoltà. […] Per quanto attiene alle informazioni scientifiche, quindi, sia i giudici professionali sia i laici sono dei profani, ugualmente in difficoltà alla ricerca di spiegazioni».

gate-keeper rispetto all'ingresso della *junk science* nel processo, delega sempre più al sapere esterno dell'esperto la decisione[371].

Certo, *de jure condendo*, una riforma che chiarisca l'effettiva portata precettiva delle *reguale agendi* dettate nei confronti di coloro che operano sul dato informatico sarebbe auspicabile. Cionondimeno, allo stato, la tesi secondo cui la L. 48/2008 ha inteso dettare divieti probatori impliciti sembra la più rispettosa della *ratio legis*, nonché l'unica in grado di rispettare il principio garantistico per cui le regole di esclusione devono «garantire l'attendibilità dell'accertamento e tutelare il metodo di formazione delle prove da eventuali abusi»[372].

[371] A tal proposito, v., ancora, le premonitrici considerazioni di M.R. DAMAŞKA, *op. cit.*, p. 215: «dover fare affidamento su informazioni scientifiche impenetrabili aumenta le contraddizioni rispetto alla possibilità che l'organo giudicante analizzi la prova sulla base dei processi cognitivi ordinari. Una delle pietre angolari del diritto delle prove europeo moderno, e cioè il principio della libera valutazione delle prove, dovrà essere ripensato e riconcettualizzato nel prossimo futuro».

[372] Così F.M. GRIFANTINI, *Inutilizzabilità* (voce), in AA. VV, *Digesto delle discipline penalistiche*, VII, Utet, Torino, 1993, p. 2471. In quest'ottica, v. anche le annotazioni di L. LUPARIA, *Le scienze penalistiche nella "tempesta" digitale. Quali approdi?*, in *Arch. pen.*, 2013, p. 880, nonché ID., Computer crimes *e procedimento penale*, cit., p. 390.

BIBLIOGRAFIA

G. ALLENA, *Riflessioni sul concetto di incostituzionalità della prova*, in *Riv. it. dir. proc. pen.*, 1989, p. 514 ss.

G. AMATO, *L'attivazione regolare dell'operazione salva i risultati di molte azioni simulate*, in *Guida dir.*, 2005, n. 25, p. 67 ss.

E. APRILE, *Limiti alla utilizzabilità processuale del sequestro di materiale informatico acquisito mediante siti* web *"civetta"*, in *Dir. internet*, 2005, p. 43 ss.

E. APRILE, *Sull'utilizzabilità processuale della riproduzione a stampa di documenti informatici effettuata nel corso di una operazione di polizia giudiziaria*, in *Dir. internet*, 2007, p. 271 ss.

E. APRILE, *Sequestro del* computer *di un giornalista, clonazione della relativa memoria e tutela del segreto professionale*, in *Dir. internet*, 2007, p. 587 ss.

S. ATERNO, *In materia di sequestro di hd e acquisizione della prova informatica: un caso eclatante*, in *Dir. internet*, 2007, p. 367 ss.

S. ATERNO, *Acqusizione e analisi della prova informatica*, in *Dir. pen. proc.*, 2008, *Dossier prova scientifica*, p. 61 ss.

S. ATERNO, *Art. 8. Modifiche al titolo III del libro terzo del codice di procedura penale*, in G. CORASANITI-G. CORRIAS LUCENTE, Cybercrime*, responsabilità degli enti e prova digitale. Commento alla Legge 18 marzo 2008, n. 48*, Cedam, Padova, 2009, p. 193 ss.

S. ATERNO, *Art. 10. Modifiche all'articolo 132 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196*, in G. CORASANITI-G. CORRIAS LUCENTE, Cybercrime*, responsabilità degli enti, prova digitale. Commento alla Legge 18 marzo 2008, n. 48*, Cedam, Padova, 2009, p. 231 ss.

S. ATERNO, *Le investigazioni informatiche e l'acquisizione della prova digitale*, in *Giur. merito*, 2013, p. 955 ss.

S. ATERNO-A. CISTERNA, *Il legislatore interviene ancora sul* data retention, *ma non è finita*, in *Dir. pen. proc.*, 2009, p. 282 ss.

S. ATERNO-M. MATTIUCCI, Cloud forensics *e nuove frontiere delle indagini informatiche nel processo penale*, in Arch. pen., 2013, p. 876 ss.

L. BACCHINI, *Il sequestro probatorio nei confronti del giornalista non indagato: il problema del bilanciamento di interessi costituzionalmente garantiti ed il rischio di elusione delle tutele*, in *Dir. inf.*, 2008, p. 743 ss.

A. BARBIERI, *Le attività d'indagine della polizia giudiziaria su sistemi informatici e telematici*, in *Dir. internet*, 2008, p. 516 ss.

P.L. BELLIA-S. FREIWALD, *Fourth Amendment Protection for Stored E-mail*, in *41 U.S.F. L. Rev.*, 2006-2007, p. 559 ss.

H. BELLUTA, Cybercrime *e responsabilità degli enti*, in in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, p. 83 ss.

M. BERGONZI PERRONE, *Il mancato rispetto delle disposizioni della Legge n. 48 del 2008 in tema di acquisizione probatoria informatica: per una ipotesi sanzionatoria non prevista esplicitamente dal dato normativo*, in *Cib. dir.*, 2013, p. 119 ss.

G. BONO, *Illegittimità dei provvedimenti di perquisizione e sequestro delle credenziali di accesso al sistema di prenotazione di voli aerei* on line, in *Cass. pen.*, 2013, p. 1523 ss.

G. BRAGHÒ, *Le indagini informatiche fra esigenze di accertamento e garanzie di difesa*, in *Dir. inf.*, 2005, p. 517 ss.

G. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, Giuffrè, Milano, 2012, p. 181 ss.

F. CAJANI, *La Convenzione di Budapest nell'insostenibile salto all'indietro del Legislatore italiano, ovvero: quello che le norme non dicono…*, in *Cib. dir.*, 2010, p. 185 ss.

F. CAJANI, *Il vaglio dibattimentale della* digital evidence, in *Arch. pen.*, 2013, p. 837 ss.

A. CAMON, *Sulla inutilizzabilità nel processo penale dei tabulati di traffico telefonico degli apparecchi «cellulari», acquisiti dalla polizia senza autorizzazione dell'autorità giudiziaria*, in *Cass. pen.*, 1996, p. 3721 ss.

A. CAMON, *Le riprese visive come mezzo di indagine, spunti per una riflessione sulle prove incostituzionali*, in *Cass. pen.*, 1999, p. 1206 ss.

A. CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. proc. pen.*, 2005, p. 594 ss.

F. CAPRIOLI, *Colloqui riservati e prova incostituzionale*, Giappichelli, Torino, 2000

F. CAPRIOLI, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cass. pen.*, 2008, p. 3520 ss.

M. CARDUCCI, *La cooperazione giudiziaria e di polizia nelle indagini sul* cybercrime*: l'esperienza del* pool *reati informatici presso la procura di Milano*, in

F. CAJANI-G. COSTABILE (a cura di), *Gli accertamenti informatici nelle investigazioni penali: una prospettiva europea*, Experta, Forlì, 2011, p. 17 ss.

S. CARNEVALE, *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare*, in *Dir. pen. proc.*, 2009, p. 472 ss.

F. CASASOLE, *Le indagini tecnico-scientifiche: un connubio tra scienza e diritto in perdurante attesa di disciplina*, in *Dir. pen. proc.*, 2008, p. 1443 ss.

E. CASEY, *Error, Uncertainty, and Loss in Digital Evidence*, in *Int. J. Dig. Evidence*, 2002, p. 1 ss.

E. CASEY, *Digital evidence and Computer Crime*. *Forensic science*, *Computers and the Internet*, 2nd edition, Academic Press, 2004

V. CASINI, *Sanzionata dalla Cassazione l'omessa catena di custodia*, in *Dir. pen. proc.*, 2010, p. 1078 ss.

F. CASSIBBA, *L'ampliamento delle attribuzioni del pubblico ministero distrettuale*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, Giuffrè, Milano, 2009, p. 113 ss.

F. CENTONZE, *Scienza spazzatura e scienza corrotta nelle attestazioni e valutazioni dei consulenti tecnici nel processo penale*, in *Riv. dir. proc. pen.*, 2001, p. 1234 ss.

F. CERQUA, *Il difficile equilibrio tra la protezione dei dati personali e le indagini informatiche*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, Giuffrè, Milano, 2012, p. 221 ss.

A. CHELO MANCHIA, *Sequestro probatorio di* computers*: un provvedimento superato dalla tecnologia?*, in *Cass. pen.*, 2005, p. 1634 ss.

A. CHELO, *Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria*, Cedam, Padova, 2014

A. CISTERNA, *Esplorazioni limitate sul* computer *del cronista anche se c'è rivelazione di segreti professionali*, in *Guida dir.*, 2007, n. 31, p. 63 ss.

A. CISTERNA, *Perquisizioni in caso di fondato motivo*, in *Guida dir.*, n. 16, 2008, p. 66 ss.

A. CISTERNA, *Esperibilità della procedura di* hashing *valutabile solo in sede di merito*, in *Guida dir.*, 2009, n. 17, p. 84 ss.

T.K. CLANCY, *The Fourth Amendment Aspects of Computer Searches and Seizures: a Perspective and a Primer*, in *Miss. L. J.*, 2005, 193 ss.

S. COLAIOCCO, *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *Arch. pen.*, 2014, p. 9 ss.

D. COLARUSSO, *Heads in the Cloud, a Coming Storm. The Interplay of Cloud Computing, Encryption, and the Fifth Amendment's Protection Against Self-Incrimination*, in *17 B.U. J. Sci. & Tech.*, 2011, p. 69 ss.

E. COLOMBO, "Data retention" *e Corte di Giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della direttiva 2006/24/CE*, in *Cass. pen.*, 2014, p. 2705 ss.

C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Cedam, Padova, 2007

C. CONTI, Iudex peritus peritorum *e ruolo degli esperti nel processo penale*, in *Dir. pen. proc.*, 2008, *Dossier prova scientifica*, p. 29 ss.

C. CONTI, *Il volto attuale dell'inutilizzabilità: derive sostanzialistiche e bussola della legalità*, in *Dir. pen. proc.*, 2010, p. 781 ss.

F. CORDERO, *Procedura penale*, IX ed., Giuffrè, Milano, 2012

L. CORDÌ, *L. 18.3.2008 n. 48 (Criminalità informatica) – Art. 8*, in *Legisl. pen.*, 2008, p. 281 ss.

G. COSTABILE, Scena criminis*, documento informatico e formazione della prova penale*, in *Dir. inf.*, 2005, p. 531 ss.

G. COSTABILE, Computer forensics *e informatica investigativa alla luce della Legge n. 48 del 2008*, in *Cib. dir.*, 2010, p. 465 ss.

D. CURTOTTI, *Le ragioni di un confronto di idee*, in *Arch. pen.*, 2013, p. 765 ss.

D. CURTOTTI NAPPI-L. SARAVO, *L'errore tecnico-scientifico sulla scena del crimine. L'errore inevitabile e le colpe dello scienziato, del giurista e del legislatore*, in *Arch. pen.*, 2011, p. 1 ss.

M. R. DAMAŠKA, *Il diritto delle prove alla deriva*, trad. it., Il Mulino, Bologna, 2003

M. DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, p. 283 ss.

M. DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche*, in *Cass. pen.*, 2012, p. 441 ss.

M. DANIELE, *Indagini informatiche lesive della riservatezza. Verso un'inutilizzabilità convenzionale?*, in *Cass. pen.*, 2013, p. 367 ss.

G. DA VALLE, *L. 18.3.2008, n. 48 (Criminalità informatica) – Art. 9*, in *Legisl. pen.*, p. 297 ss.

G. DA VALLE, *L. 18.3.2008, n. 48 (Criminalità informatica) – Art. 10*, in *Legisl. pen.*, p. 306 ss.

D. DELL'ORTO, *Pedopornografia* on line *e indagini informatiche – complessità e peculiarità tecnico-giuridiche della materia*, in *Cass. pen.*, 2007, p. 3042 ss.

M.L. DI BITONTO, *La ratifica della Convenzione del Consiglio d'Europa sul* cybercrime*: profili processuali*, in *Dir. internet*, 2008, p. 503 ss.

C. DI MARTINO, *Le intercettazioni telematiche e l'ordinamento italiano: una convivenza difficile*, in *Ind. pen.*, 2002, p. 219 ss.

G. DI PAOLO, voce *Prova informatica*, in *Enciclopedia del diritto. Annali*, VI, Giuffrè, Milano, 2013, p. 736 ss.

O. DOMINIONI, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Giuffrè, Milano, 2005

J. DUONG, *The Intersection of Fourth and Fifth Amendments in the Context of Encrypted Personal Data at the Border*, in *2 Drexel L. Rev.*, 2009, p. 313 ss.

S.J. EDGETT, *Double-Clicking on Fourth Amendment Protection: Encryption Creates a Reasonable Expectation of Privacy*, in *30 Pepp. L. Rev.*, 2003, p. 340 ss.

S. FASOLIN, *La copia di dati informatici nel quadro delle categorie processuali*, in *Dir. pen. proc*, 2012, p. 372 ss.

C. FATTA, *La tutela della* privacy *alla prova dell'obbligo di* data retention *e delle misure antiterrorismo*, in *Dir. inf.*, 2008, p. 395 ss.

P. FELICIONI, *Le ispezioni e le perquisizioni*, Giuffrè, Milano, 2012

I.V. FELCHER, *Una rassegna giurisprudenziale con riferimento alla Legge n. 48 del 2008 e alle investigazioni digitali*, in *Cib. dir.*, 2013, p. 131 ss.

P. FERRUA, *Metodo scientifico e processo penale*, in *Dir. pen. proc.*, 2008, *Dossier prova scientifica*, p. 12 ss.

F. FILIPPI, *L'intercettazione di comunicazioni*, Giuffrè, Milano, 1997

L. FILIPPI, *L'*home watching*: documento, prova atipica o prova incostituzionale*, in *Dir. pen. proc.*, 2001, p. 92 ss.

L. FILIPPI, *Ascolto e trascrizione di telefonate all'inquisito: sommarie informazioni o prova incostituzionale?*, in *Dir. pen. proc.*, 2001, p. 1396 ss.

A. FIORE, *L'informatica forense e i modelli di investigazione digitale*, in *Cib. dir.*, 2014, p. 99 ss.

R. FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d.* online durchsuchung, in *Riv. trim. dir. pen. econ.*, 2009, p. 695 ss.

R. FLOR, *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali nella recente giurisprudenza del* Bundesverfassungsgericht*: la decisione del 27 febbraio 2008 sulla* Online Durchsuchung *e la sua portata alla luce della sentenza del 2 marzo 2010 sul* data retention, in *Cib. dir.*, 2010, p. 359 ss.

R. FLOR, Data retention *e limiti al potere coercitivo dello Stato in materia penale: le sentenze del* Bundesverfassungsgericht *e della* Curtea Constiuţională, in *Cass. pen.*, 2011, p. 1952 ss.

R. FLOR, *Verso una rivalutazione dell'art. 615*-ter *c.p.?*, 2 maggio 2012, in www.penalecontemporaneo.it

R. FLOR, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di Internet*, 20 settembre 2012, in www.penalecontemporaneo.it

R. FLOR, *La Corte di Giustizia considera la Direttiva europea 2006/24 sulla c.d. "*Data retention" *contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, 28 aprile 2014, in www.penalecontemporaneo.it

G. FUMU, sub *art. 266*-bis, in AA.VV., *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, III agg., Utet, Torino, 1998, p. 132 ss.

A.M. GERSHOWITZ, *The iPhone Meets the Fourth Amendment*, in *56 UCLA L. Rev.*, 2008, p. 27 ss.

A.M. GERSHOWITZ, *Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest?*, in *96 Iowa L. Rev.*, 2011, p. 1125 ss.

F. GIUNCHEDI, *Irripetibilità della prova ed accertamenti tecnico scientifici*, in *Arch. pen.*, 2012, n. 2, p. 11 ss.

F. GIUNCHEDI, *Le* malpractices *nella* digital forensics. *Quali conseguenze sull'inutilizzabilità del dato informatico?*, in *Arch. pen.*, 2013, p. 821 ss.

V. GREVI, *Insegnamenti, moniti e silenzi della Corte Costituzionale*, in *Giur. cost.*, 1973, p. 1181 ss.

F.M. GRIFANTINI, *Inutilizzabilità* (voce), in AA. VV, *Digesto delle discipline penalistiche*, VII, Utet, Torino, 1993, p. 2471 ss.

A. GRILLO-U.E. MOSCATO, *Riflessioni sulla prova informatica*, in *Cass. pen.*, 2011, p. 370 ss.

P. GUALTIERI, *Prova informatica e diritto di difesa*, in *Dir. pen. proc.*, 2008, *Dossier prova scientifica*, p. 70 ss.

M. GUERNELLI, *La legge di ratifica dela Convenzione sul* Cybercrime*: considerazioni sostanziali e processuali*, in *Riv. trim. dir. pen. ec.*, 2008, p. 753 ss.

F. IOVENE, *Le perquisizioni c.d.* online, *tra nuovi diritti fondamentali ed esigenze di accertamento penale*, 22 luglio 2014, in www.penalecontemporaneo.it

E.E. KENNEALLY, *Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection*, in *5 UCLA J. L. & Tech.*, 2005, p. 1 ss.

O.S. KERR, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy"?*, in *33 Conn. L. Rev.*, 2001, p. 33 ss.

O. KERR, *Search Warrants in an Era of Digital Evidence*, in *75 Miss. L. J.*, 2005, 85 ss.

O. KERR, *Digital Evidence and the New Criminal Procedure*, in *105 Colum. L. Rev.*, 2005, p. 291 ss.

O. KERR, *Searches and Seizures in a Digital World*, in *119 Harv. L. Rev.*, 2005, p. 531 ss.

O. KERR, Ex Ante *Regulation of Computer Search and Seizure*, in *96 Va. L. Rev.*, 2010, p. 1241 ss.;

J.E.D. LARKIN, *Compelled Production of Encrypted Data*, in *14 Vand. J. Ent. & Tech. L.*, 2012, p. 264 ss.

D. LA MUSCATELLA, *La ricerca della prova digitale e la violazione delle* best practices*: un'attività investigativa complessa tra recenti riforme e principi consolidati*, in *Cib. dir.*, 2011, p. 221 ss.

D. LA MUSCATELLA, *La genesi della prova digitale: analisi prospettica dell'ingresso dell'informatica forense nel processo penale*, in *Cib. dir.*, 2012, p. 385 ss.

D. LA MUSCATELLA, *La ricerca delle fonti di prova sulle reti di* cloud computing*: le nuove frontiere delle investigazioni digitali tra profili giuridici e questioni operative*, in *Cib. dir.*, 2013, p. 477 ss.

A. LOGLI, *Sequestro probatorio di un* personal computer. *Misure* ad explorandum *e tutela della corrispondenza elettronica*, in *Cass. pen.*, 2008, p. 2952 ss.

E. LORENZETTO, *Utilizzabilità dei dati informatici incorporati su* computer *in sequestro: dal contenitore al contenuto passando per la copia*, in *Cass. pen.*, 2010, p. 1524 ss.

E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, Giuffrè, Milano, 2012, p. 135 ss.

S. LORUSSO, *Investigazioni scientifiche, verità processuale ed etica degli esperti*, in *Dir. pen. proc.*, 2010, p. 1345 ss.

P.H. LUEHR, *Real Evidence, Virtual Crimes. The Role of Computer Forensic Experts*, in *20 Crim. Just.*, 2005, p. 16 ss.

L. LUPARIA, *Le investigazioni informatiche in materia di pornografia minorile tra nuovi e vecchi abusi degli strumenti processuali*, in *Dir. internet*, 2005, p. 481 ss.

L. LUPARIA, *Il caso "Vierika": un'interessante pronuncia in materia di* virus *informatici e prova penale digitale*, in *Dir. internet*, 2006, p. 157 ss.

L. LUPARIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa (L. 18 Marzo 2008 n. 48). I profili processuali*, in *Dir. pen. proc.*, 2008, p. 717 ss.

L. LUPARIA, *I correttivi alle distorsioni sistematiche contenute nella recente legge di ratifica della Convenzione sul* Cybercrime, in S. LORUSSO (a cura di), *Le nuove norme sulla sicurezza pubblica*, Cedam, Padova, 2008, p. 63 ss.

L. LUPARIA, Computer crimes *e procedimento penale*, in AA.VV., *Trattato di procedura penale*, diretto da G. Spangher, vol. VII, Tomo I, Utet, Torino, 2011, p. 369 ss.

L. LUPARIA, *Il sistema penale ai tempi dell'*internet. *La figura del* provider *tra diritto e processo*, in ID. (a cura di), Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Giuffrè, Milano, 2012, p. 1 ss.

L. LUPARIA, *Le scienze penalistiche nella "tempesta" digitale. Quali approdi?*, in *Arch. pen.*, 2013, p. 880 ss.

L. LUPARIA-G. ZICCARDI, *Investigazione penale e tecnologia informatica*, Giuffrè, Milano, 2007.

A. MACRILLÒ, *Le nuove disposizioni in tema di sequestro probatorio e di custodia ed assicurazione dei dati informatici*, in *Dir. internet*, 2008, p. 511 ss.

D. MANZIONE, *L. 18.3.2008 N. 48 (Criminalità informatica) – Art. 11 – Competenza*, in *Legisl. pen.*, 2008, p. 314 ss.

L. MARAFIOTI, *Scelte autodifensive dell'indagato e alternative al silenzio*, Giappichelli, Torino, 2000

L. MARAFIOTI, *Digital evidence* e processo penale, in *Cass. pen.*, 2011, p. 4509 ss.

S. MARCOLINI, *Le cosiddette perquisizioni* online *(o perquisizioni elettroniche*), in *Cass. pen.*, 2010, p. 2855 ss.

C. MARINELLI, *L'attività dell'agente provocatore per il contrasto alla pedopornografia: "straripamenti" investigativi e relative implicazioni processuali*, in *Cass. pen.*, 2005, p. 2683 ss.

N.K. MCGREGOR, *The Weak Protection of Strong Encryption: Passwords, Privacy, and Fifth Amendment Privilege*, in *12 Vand. J. Ent. & Tech. L.*, 2010, p. 581 ss.

M. MEYERS-M. ROGERS, *Computer Forensics: The Need for Standardization and Certification*, in *2 Int. J. Dig. Evidence*, 2004, p. 4 ss.

M.F. MIQUELON-WEISMANN, *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*, in 23 *J. Marshall J. Computer & Info. L.*, 2005, p. 347 ss.

F.M. MOLINARI, *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. pen.*, 2012, p. 696 ss.

A. MONTI, *No ai sequestri indiscriminati di* computer, in *Dir. internet*, 2007 p. 265 ss.

A. MONTI, *La nuova disciplina del sequestro informatico*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, Giuffrè, Milano, 2012, p. 197 ss.

A. NATALINI, *Pedopornografia e diritti della difesa. Per le attività di contrasto niente* analogia iuris, in *Dir. giust*., 2003, n. 41, p. 16 ss.

G. NICOSIA-D.E. CACCAVELLA, *Indagini della difesa e alibi informatico: utilizzo di nuove metodiche investigative, problemi applicativi ed introduzione nel giudizio*, in *Dir. internet*, 2007, p. 520 ss.

F. NOVARIO, *L'attività di accertamento tecnico difensivo disposta su elementi informatici e la sua ripetibilità*, in *Cib. dir.*, 2011, p. 75 ss.

A. NOVELLINO, *Il Viminale può chiedere di conservare i dati*, in *Guida dir.*, 2008, n. 16, p. 69 ss.

R. ORLANDI, *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc.*, 2009, p. 129 ss.

J. PALFREY, *The Public and the Private at the United States Border with Cyberspace*, in *Miss. L. J.*, 2008, p. 241 ss.

B.M. PALFREYMAN, *Lessons from the British and American Approaches to Compelled Decryption*, in *75 Brook. L. Rev.*, 2009, p. 345 ss.

C. PARODI, *La disciplina delle intercettazioni telematiche*, in *Dir. pen. proc.*, 2003, p. 889 ss.

C. PARODI, VoIP*,* Skype *e tecnologie d'intercettazione: quali risposte d'indagine per le nuove frontiere delle comunicazioni?*, in *Dir. pen. proc.*, 2008, p. 1309 ss.

P.P. PAULESU, *Notizia di reato e scenari investigativi complessi: contrasto alla criminalità organizzata, operazioni «sotto copertura», captazione di dati digitali*, in *Riv. dir. proc.*, 2010, p. 787 ss.

C. PECORELLA, *Diritto penale dell'informatica*, Cedam, Padova, 2006

P. PERRI, voce Computer forensics *(indagini informatiche)*, in *Dig. pen.*, VI ed., Agg., Utet, Torino, 2011, p. 95 ss.

G. PIERRO, *Introduzione allo studio dei mezzi di ricerca della prova informatica*, in *Dir. pen. proc.*, 2011, p. 1516 ss.

A.E. RICCI, Digital evidence *e irripetibilità delle operazioni acquisitive*, in *Dir. pen. proc.*, 2010, p. 339 ss.

A.E. RICCI, Digital evidence*, sapere tecnico-scientifico e verità giudiziale*, in C. CONTI (a cura di), *Scienza e processo penale. Nuove frontiere e vecchi pregiudizi*, Giuffrè, Milano, 2011, p. 341 ss.

L.R. ROBINTON, *Courting Chaos: Conflicting Guidance from Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Data*, in *12 Yale J. L.*, 2010, p. 311 ss.

A. RODOLFI, *Il regime normativo della* data retention *nell'ordinamento italiano. Stato attuale e problematiche concrete*, in *Cib. dir.*, 2010, p. 147 ss.

F. RUGGIERI, *Profili processuali nelle investigazioni informatiche*, in L. PICOTTI, *Il diritto penale dell'informatica nell'epoca di* Internet, Cedam, Padova, 2004, p. 153 ss.

G.M. RUOTOLO, Hey! You! Get Off My Cloud! *Accesso autoritativo alle nuvole informatiche e diritto internazionale*, in *Arch. pen.*, 2013, p. 853 ss.

C. SARZANA DI SANT'IPPOLITO, *La Convenzione europea sulla cibercriminalità*, in *Dir. pen. proc.*, 2002, p. 509 ss.

E. SELVAGGI, *Cooperazione giudiziaria veloce ed efficace*, in *Guida dir.*, 2008, n. 16, p. 72 ss.

E. SELVAGGI, *Task force operativa 24 ore al giorno*, in *Guida dir.*, 2008, n. 16, p. 74 ss.

N. SOARES, *The Right to Remain Encrypted: the Self-Incrimination Doctrine in the Digital Age*, in *49 Am. Crim. L. Rev.*, 2012, p. 2001 ss.

A. STRACUZZI, Data retention*: il faticoso percorso dell'art. 132 Codice* privacy *nella disciplina della conservazione dei dati di traffico*, in *Dir. inf.*, 2008, p. 585 ss.

M. STRAMAGLIA, *Il sequestro di documenti informatici: quale tutela per il segreto professionale forense?*, in *Dir. inf.*, 2008, p. 831 ss.

P. TONINI, *La prova scientifica: considerazioni introduttive*, in *Dir. pen. proc.*, 2008, *Dossier prova scientifica*, p. 7 ss.

P. TONINI, *Documento informatico e giusto processo*, in *Dir. pen. proc.*, 2009, p. 401 ss.

P. TONINI, *L'influenza della sentenza Franzese sul volto attuale del processo penale*, in *Dir. pen. proc.*, 2012, p. 1225 ss.

S. TREPEL, *Digital Searches, General Warrants, and the Case for the Courts*, in *10 Yale J. L. & Tech.*, 2007, p. 120 ss.

P. TROISI, *Sequestro probatorio del* computer *e segreto giornalistico*, in *Dir. pen. proc.*, 2008, p. 765.

A.J. UNGBERG, *Protecting Privacy Through a Responsible Decryption Policy*, in *22 Harv. J. Law. Tech.*, 2009, p. 537 ss.

G. VACIAGO, Digital Evidence, Giappichelli, Torino, 2012

G. VACIAGO, *La disciplina normativa sulla* data retention *e il ruolo degli* Internet service provider, in L. LUPARIA (a cura di), Internet provider *e giustizia penale*, Giuffrè, Milano, 2012, p. 141 ss.

S. VENTURINI, *Sequestro probatorio e fornitori di servizi telematici*, in L. LUPARIA (a cura di), Internet Provider *e giustizia penale*, Giuffrè, Milano, 2012, p. 107 ss.

A. VITALE, *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico*, in *Dir. internet*, 2008, p. 506 ss.

A.M. WEBER, *The Council of Europe's Convention on Cybercrime*, in *18 Berkeley Tech. L.J.*, 2003, p. 437 ss.

R.B. WELLS, *The Fog of Cloud Computing: Fourth Amendment Issues Raised by the Blurring of Online and Offline Content*, in *12 U. Pa. J. Const. L.*, 2014, p. 223 ss.

C. WOO-M. SO, *The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance*, in *15 Harv. L. Tech.*, 2002, p. 521 ss.

F. ZACCHÈ, *La prova documentale*, Giuffrè, Milano, 2012

G. ZICCARDI, *L'ingresso della* computer forensics *nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, Giuffrè, Milano, 2012, p. 165 ss.