Estratto

ISSN 0035-6182

ANNO LXVI (Seconda Serie) - N. 2 Marzo-Aprile 2011

RIVISTA

DI

DIRITTO PROCESSUALE

FONDATA NEL 1924 DA

G. CHIOVENDA, F. CARNELUTTI e P. CALAMANDREI

GIÀ DIRETTA DA

E.T. LIEBMAN, G. TARZIA e E.F. RICCI

DIRETTORI

C. PUNZI e B. CAVALLONE

COMITATO DI DIREZIONE

M. ACONE - G. BONGIORNO - V. COLESANTI
L.P. COMOGLIO - C. CONSOLO - G. COSTANTINO
C. FERRI - R.E. KOSTORIS - S. LA CHINA - G. MONTELEONE
R. ORIANI - N. PICARDI - A. SALETTI - B. SASSANI
N. TROCKER - R. VACCARELLA

CASA EDITRICE DOTT. ANTONIO MILANI
2011

LA PROVA DIGITALE NEL PROCESSO PENALE (*)

SOMMARIO: 1. L'universalità della prova digitale. – 2. L'immaterialità della prova digitale. – 3. La dispersione della prova digitale. – 3.1. Il debole accentramento delle indagini informatiche nazionali. – 3.2. L'autarchia nelle indagini informatiche sovranazionali. – 4. La promiscuità della prova digitale e i pericoli per la riservatezza. – 4.1. L'agevole accessibilità dei sistemi informatici. – 4.2. Le aporie del regime di conservazione delle prove digitali. – 5. La modificabilità della prova digitale. – 5.1. Antidoti alla modificabilità: l'uso delle migliori tecniche informatiche. – 5.2. L'attuazione del contraddittorio tecnico.

1. – Stanno diventando indispensabili in un numero crescente di processi prove che si trovano nascoste all'interno di sistemi informatici (1): *files* che contengono testi, suoni o immagini o che registrano gli eventi occorsi nei sistemi, oppure tracce lasciate dall'utilizzo dei sistemi; più esattamente, prove «digitali», in quanto originate da una manipolazione elettronica di numeri (2).

Prove di questo genere non sono utili solo per la repressione dei reati informatici, cioè i reati commessi contro un sistema informatico o grazie allo stesso (3). Esse possono produrre conoscenze rilevanti ai fini dell'accertamento di qualunque reato, e dunque hanno un ambito operativo potenzialmente illimitato (4). Lo riconosce a chiare lettere l'art. 14 § 2 *c* Convenzione di Budapest, il quale invita gli

---

(*) Testo della relazione, con integrazioni e note, svolta al Convegno «Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali» (Como, 21 e 22 maggio 2010). Il lavoro è frutto dell'attività di ricerca svolta nell'ambito del Progetto di Ateneo «Criminalità informatica ed accertamento penale» (codice CPDA084200/08), finanziato dall'Università degli Studi di Padova.

(1) Cioè *computers* e reti informatiche come internet: v. le definizioni previste dall'art. 1 lett. *a* della Convenzione del Consiglio d'Europa sulla criminalità informatica, stipulata a Budapest il 23 novembre 2001.

(2) Dall'inglese «digit» («cifra»): *wikipedia*, voce *Digitale (informatica)*.

(3) Si vedano L. Picotti, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in Aa.Vv., *Il diritto penale dell'informatica nell'epoca di internet*, a cura di L. Picotti, Padova 2004, p. 86 s.; C. Sarzana di S. Ippolito, *Informatica, internet e diritto penale*, 3ª ed., Milano 2010, p. 61 s.

(4) Cfr. L. Luparia, *La disciplina processuale e le garanzie difensive*, in L. Luparia, G. Ziccardi, *Investigazione penale e tecnologia informatica*, Milano 2007, p. 130 s.; R. Orlandi, *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc.* 2009, p. 128 s.

Stati contraenti ad apprestare un'apposita disciplina finalizzata a «*la collecte des preuves électroniques de toute infractions pénales*».

La grande fruibilità processuale delle prove digitali dipende dal costante incremento della diffusione dei sistemi informatici e della digitalizzazione delle conoscenze nella società moderna, con le sempre maggiori occasioni di interconnessione tra il mondo fisico e il mondo digitale che ne derivano (5).

Di fronte all'irrompere delle prove digitali sulle scene dei crimini era indispensabile un intervento del legislatore, tale da predisporre specifiche regole volte a disciplinarne la raccolta e l'utilizzazione in giudizio. Diversamente – come è già iniziato ad accadere – dovrebbe essere la giurisprudenza a farsi carico dei problemi generati dalle indagini informatiche, con il pericolo di interpretazioni non ispirate da un disegno unitario.

Assolutamente doverosa, quindi, è stata la recezione in Italia della Convenzione di Budapest da parte della l. 18 marzo 2008 n. 48. Resta da stabilire in che misura la nuova disciplina tenga nel dovuto conto le caratteristiche delle prove digitali, che sono molto diverse da quelle delle prove tradizionali (6). Se si vogliono salvaguardare le finalità cognitive del processo devono essere le norme e le loro applicazioni concrete a piegarsi alle esigenze del mondo digitale, e non viceversa.

2. – Di fronte alle prove digitali i processualisti si trovano a disagio, in quanto sono abituati a pensare alle prove come a degli oggetti fisici, dotati di un'evidente corporeità. Le prove digitali si presentano, invece, come entità immateriali. Ciò non significa che esse non abbiano una loro fisicità: concettualmente si tratta di impulsi elettrici che rispondono ad una sequenza numerica prestabilita e che, convogliati in un supporto informatico dotato di una memoria, originano informazioni intellegibili. È, però, una fisicità che, in assenza del supporto, non può essere percepita come tale.

Ciò spiega perché, in passato, si tendessero a confondere le prove digitali con gli oggetti in cui le medesime sono contenute.

Una traccia di questa più risalente e fuorviante concezione emerge in modo chiaro dal previgente art. 491 *bis* c.p. (7), il quale identificava il «documento informatico» con qualunque «supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli».

Se le cose stessero in questi termini non sorgerebbero particolari questioni in tema di raccolta delle prove digitali: sarebbe sufficiente applicare le disposizioni in materia di acquisizione delle prove documentali. I supporti materiali contenenti in-

---

(5) Si veda C. Sarzana di S. Ippolito, *Informatica*, cit., p. 7 s.

(6) Sulla conseguente necessità di ripensare tutte le comuni regole probatorie, originariamente concepite per le prove tradizionali, v. O.S. Kerr, *Digital evidence and the new criminal procedure*, in *105 Columbia law rev.* 2005, p. 290 s.

(7) Introdotto dalla l. 23 dicembre 1993 n. 547, ed ora abrogato dalla l. n. 48 del 2008.

formazioni digitali reperiti nel corso delle indagini potrebbero essere prodotti in giudizio ed inseriti nel fascicolo per il dibattimento ai sensi degli artt. 495 comma 3 e 515 c.p.p. L'unico spazio per il contraddittorio si aprirebbe in sede di discussione finale, e riguarderebbe il valore conoscitivo delle informazioni.

Oggi nessuno dubita più del fatto che le prove digitali esistano indipendentemente dai supporti in cui si trovano, i quali sono solo involucri esterni di per sè processualmente irrilevanti (8). Spesso vi è, anzi, un'assoluta sproporzione tra le prove digitali ed i loro recipienti: un supporto di piccole dimensioni è in grado di contenere una massa enorme di informazioni digitali.

La definizione di documento informatico è stata opportunamente aggiornata dall'art. 1 comma 1 lett. *p* d.lgs. 7 marzo 2005 n. 82 (codice dell'amministrazione digitale): ora essa si impernia non più sul supporto materiale del documento, ma sulla «rappresentazione» informatica di atti, fatti o dati giuridicamente rilevanti.

Fortunatamente anche la legge n. 48 del 2008 appare consapevole dell'immaterialità delle prove digitali. Il nuovo comma 1 *bis* c.p.p. dell'art. 247 c.p.p. disciplina la ricerca di «dati, informazioni, programmi informatici o tracce comunque pertinenti al reato» che «si trovino in un sistema informatico» (9), mostrando di percepire la differenza tra le prove digitali ed i loro contenitori.

3. – Dalla immaterialità discendono ulteriori caratteristiche delle prove digitali, che creano non pochi inconvenienti in rapporto alla loro acquisizione processuale.

Si pensi, anzitutto, al rischio della loro dispersione. Molto più frequentemente delle prove tradizionali, le prove digitali di un reato si trovano dislocate in luoghi distanti tra loro: ad esempio in *servers* e in *personal computers* fisicamente molto lontani. Considerata l'estensione mondiale delle reti informatiche, potenzialmente la dispersione può riguardare l'intero globo terrestre (10).

Di qui la necessità che il legislatore fissi regole precise per individuare la competenza degli organi inquirenti, in modo da evitare che si sovrappongano più procedimenti in rapporto agli stessi episodi criminosi. Tale problematica non riguarda solo i rapporti tra gli organi italiani, ma anche le relazioni tra gli organi italiani e quelli stranieri, quando il reato, lasciando delle tracce digitali anche all'estero, assume una dimensione sovranazionale.

3.1. – Purtroppo la l. n. 48 del 2008 ha affrontato la questione della dispersio-

---

(8) Cfr. L. Picotti, *La ratifica della Convenzione cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc*. 2008, p. 702 s.; P. Tonini, *Documento informatico e giusto processo*, in *Dir. pen. proc.* 2009, p. 402.

(9) Nello stesso senso l'art. 352 comma 1 *bis* c.p.p.

(10) Cfr., fra i molti, M.L. Di Bitonto, *L'accentramento investigativo delle indagini sui reati informatici*, in *Dir. internet* 2008, p. 503 s.

ne della prova digitale unicamente dal punto di vista interno al nostro ordinamento, e per di più l'ha risolta in un modo che non appare soddisfacente.

La scelta è stata quella di affidare le indagini relative ai reati informatici specificamente indicati dall'art. 51 comma 3 *quinquies* c.p.p. alle procure «presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente» (11). Si intendeva così – come si esprimono i compilatori della legge – «facilitare il coordinamento delle indagini e la formazione di gruppi di lavoro specializzati in materia» (12). È dubbio, però, che un tale obiettivo sia stato raggiunto (13).

a) La norma in esame non è in grado di creare una titolarità esclusiva della raccolta delle prove digitali a favore delle procure distrettuali. Le ben più numerose procure presso i tribunali possono continuare ad acquisire qualunque prova digitale relativa ai reati – informatici ed anche comuni – diversi da quelli ricompresi nell'elenco dell'art. 51 comma 3 *quinquies*, e non connessi con gli stessi. Esse, di conseguenza, non potrebbero astenersi dallo sviluppare per proprio conto le competenze tecniche che le indagini informatiche richiedono.

b) Non è stato istituito un organo centrale simile alla Direzione nazionale antimafia, con la conseguenza che il coordinamento è soggetto al buon volere delle procure di volta in volta coinvolte nelle indagini, tramite lo strumento del collegamento stabilito dall'art. 371 c.p.p. (14).

c) Non è raro che il luogo di consumazione di un reato informatico non risulti determinabile in modo univoco (15). In tali situazioni operano i criteri suppletivi di attribuzione della competenza stabiliti dall'art. 9 c.p.p. (16), il cui comma 3 impone

---

(11) Conseguentemente l'art. 328 comma 1 *quater* c.p.p. prescrive che le relative funzioni di giudice per le indagini preliminari vanno esercitate «da un magistrato del tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente».

(12) In questi termini la Relazione che accompagna il disegno di legge C 2807, da cui la l. n. 48 del 2008 è derivata.

(13) In chiave giustamente critica nei confronti della disciplina v. H. Belluta, *Cybercrime e responsabilità degli enti*, in Aa.Vv., *Sistema penale e criminalità informatica*, a cura di L. Luparia, Milano 2009, p. 100 s.; F. Cassibba, *L'ampliamento delle attribuzioni del pubblico ministero distrettuale*, in Aa.Vv., *Sistema penale*, cit., p. 123 s.; L. Luparia, *I correttivi alle distorsioni sistematiche contenute nella recente legge di ratifica della Convenzione sul cybercrime*, in Aa.Vv., *Le nuove norme sulla sicurezza pubblica*, a cura di S. Lorusso, Padova 2008, p. 65 s. A favore, invece, delle scelte operate dall'art. 51 comma 3 *quinquies* c.p.p., M.L. Di Bitonto, *L'accentramento investigativo*, cit., p. 504 s.

(14) Cfr. al riguardo R. Orlandi, *Questioni attuali*, cit., p. 132 s.

(15) Si pensi all'accesso abusivo in un sistema informatico (art. 615 *ter* c.p.): esso si consuma già con l'ingresso nel sistema oppure successivamente, al momento dell'apprensione delle informazioni contenute nel sistema? Cfr. sul punto R. Flor, *Permanenza non autorizzata in un sistema informatico o telematico, violazione del segreto d'ufficio e concorso nel reato da parte dell'*extraneus, in *Cass. pen*. 2009, p. 1517 s.

(16) I criteri dell'art. 9 c.p.p. operano anche nel caso di connessione tra reati distinti: cfr. Cass., Sez. un., 16 luglio 2009, n. 40537.

di riferirsi, qualora ogni altro criterio risulti inapplicabile, al luogo in cui l'iscrizione della notizia di reato è avvenuta per prima (17). Una disciplina del genere, lungi dal favorire il coordinamento, stimola al più la rapidità della conduzione delle indagini, la via più sicura per ottenerne il monopolio.

3.2. – Altrettanto censurabile è l'ottica monocolare dell'intervento della l. n. 48 del 2008, interamente calibrato sulla disciplina interna senza tenere conto dei rapporti con gli altri Stati in tutte le ipotesi in cui le indagini informatiche assumono un carattere sovranazionale.

I criteri di attribuzione della giurisdizione tradizionalmente impiegati in questa materia, da tempo previsti dal nostro codice penale, ed in parte ripresi dalla stessa Convenzione di Budapest, sono inadatti alle indagini informatiche, o comunque hanno una natura autarchica: non impediscono agli altri Stati di adottare soluzioni analoghe, e quindi non eliminano il pericolo della sovrapposizione di procedimenti in rapporto ai medesimi fatti (18).

a) Il criterio della commissione del reato nel proprio territorio (19) non sempre risulta utilizzabile, in quanto si impernia su un dato che, come si diceva, per i reati informatici spesso resta incerto.

b) I criteri della commissione del reato all'estero da parte di un proprio cittadino (20), o tale da ledere un proprio interesse (21), dal canto loro, non impediscono che un procedimento sia iniziato pure dalle autorità dello Stato estero, qualora il fatto sia penalmente rilevante anche nell'ambito di quest'ultimo.

A fronte di questi possibili conflitti di giurisdizione, l'art. 22 § 5 della Convenzione di Budapest prescrive la consultazione tra gli Stati interessati, «al fine di stabilire la competenza più appropriata per esercitare l'azione penale»: un rimedio preventivo di cui la l. n. 48 del 2008 si è disinteressata.

Né è stato ascoltato il richiamo della Convenzione all'adozione di misure di cooperazione specificamente calibrate sulle indagini informatiche (artt. 23 s.). La cooperazione, in questa materia, nel nostro sistema continua ad essere affidata al metodo tradizionale della rogatoria: uno strumento che, a causa dei suoi tempi e delle sue viscosità, non sempre risponde alle esigenze di celerità imposte dalla raccolta delle prove digitali, la quale richiede in molti casi ingressi in tempo reale nei sistemi informatici (22).

4. – Un'ulteriore caratteristica delle prove digitali, che deriva sempre dalla loro immaterialità, è la promiscuità. Queste prove possono trovarsi collocate in spazi

---

(17) V. H. Belluta, *Cybercrime*, cit., p. 98; M.L. Di Bitonto, *L'accentramento*, cit., p. 505 s.

(18) Cfr. D. Micheletti, *Reato e territorio*, in *Criminalia* 2009, p. 579 s.

(19) Artt. 4 e 6 c.p., e 22 § 1 *a*, *b* e *c* Convenzione di Budapest.

(20) Artt. 9 c.p., e 22 § 1 *d* Convenzione di Budapest.

(21) Artt. 7, 8 e 10 c.p.

(22) Cfr. E. Selvaggi, *Cooperazione giudiziaria veloce ed efficace*, in *Guida dir.* 2008, n. 16, p. 72 s.

virtuali enormi e pieni di dati di ogni tipo. Non è raro che siano mescolate ad informazioni irrilevanti rispetto al reato, e magari attinenti alla vita privata dell'indagato o di altre persone.

Le indagini informatiche, dunque, sono sempre potenzialmente in grado di pregiudicare la riservatezza degli individui (23). La loro capacità lesiva della *privacy* è addirittura superiore a quella delle intercettazioni; queste ultime si limitano a carpire le informazioni che la persona intercettata ha deciso di rivelare ad altri, mentre l'analisi dei sistemi informatici e delle reti possono rivelare il contenuto di intere esistenze: abitudini, opinioni politiche, preferenze di ogni genere. In ogni caso, dati riservati che nulla hanno a che fare con la commissione dei reati, e che sono facilmente divulgabili proprio grazie alle tecnologie informatiche e ad internet, in grado di renderle conoscibili da un numero sterminato di persone.

È inevitabile che il legislatore tenga conto anche di questa ulteriore peculiarità delle prove digitali, apprestando delle procedure in grado di contemperare la tutela della riservatezza e le esigenze di accertamento. Un difficile bilanciamento che può essere realizzato agendo sia sul profilo dell'accessibilità dei sistemi informatici che su quello della conservazione delle prove digitali (24).

4.1. – Al fine di proteggere la riservatezza una via sarebbe regolamentare in modo preciso e con il massimo delle garanzie l'accessibilità dei sistemi informatici (25). Si potrebbero prevedere requisiti analoghi a quelli delle intercettazioni (26): autorizzazione di un giudice alle operazioni di apprensione, preesistenza di gravi indizi di uno dei reati previsti in un elenco legislativo, vaglio preventivo sulla indispensabilità del mezzo.

Le scelte operate dal legislatore, però, non sono andate in questa direzione: la disciplina vigente consente di entrare negli spazi digitali di pertinenza dei privati e dei fornitori di servizi informatici in base a modalità ben più agevoli. Le indagini informatiche sono configurate come ispezioni, perquisizioni e sequestri: mezzi di ricerca della prova che possono essere disposti anche dal pubblico mi-

---

(23) V., per tutti, F. Ruggieri, *Profili processuali nelle investigazioni informatiche*, in Aa.Vv., *Il diritto penale dell'informatica*, cit., p. 158 s.

(24) Per tale distinzione cfr. C. Conti, *L'attuazione della direttiva Frattini: un bilanciamento insoddisfacente tra riservatezza e diritto alla prova*, in Aa.Vv., *Le nuove norme sulla sicurezza*, cit., p. 30 s., nonché Corte cost., 6 novembre 2006, n. 372.

(25) In questo senso cfr. il § 14 della Risoluzione del XVIII Congresso internazionale di diritto penale (Istanbul, 20-27 settembre 2009), commentata da R.E. Kostoris, *La lotta al terrorismo e alla criminalità organizzata tra speciali misure processuali e tutela dei diritti fondamentali nella Risoluzione del XVIII Congresso internazionale di diritto penale*, in *Riv. dir. proc.* 2010, p. 330 s. Similmente, in rapporto all'acquisizione dei dati di traffico, C. Conti, *L'attuazione della direttiva*, cit., p. 30 s.

(26) I quali operano già in forza dell'art. 266 *bis* c.p.p. in rapporto all'acquisizione delle comunicazioni in corso tramite sistemi informatici.

nistero (27) o, nella flagranza del reato o nei casi d'urgenza, dalla stessa polizia (28), i cui atti vanno poi convalidati dal pubblico ministero (29).

La previsione relativa alle ispezioni – che consistono in ricerche puramente visive – ha, in realtà, un ambito operativo ridotto: le prove digitali, come si diceva, difficilmente sono percepibili con i soli occhi, e le ispezioni possono perlopiù servire per osservare in via preliminare il sistema informatico nelle sue componenti esterne (30).

Dunque il presupposto principale delle indagini informatiche coincide con quello delle perquisizioni, vale a dire il fondato motivo di ritenere che tracce digitali di un qualunque reato si trovino in un dato sistema informatico. È una condizione il cui riscontro va adeguatamente giustificato, ma non difficile da osservare: la integra la presenza di qualunque elemento – al più anche mere supposizioni logiche basate sulla tipologia del reato commesso – in grado di qualificare quel sistema come un potenziale contenitore di prove, senza la necessità di individuare in anticipo che cosa sarà trovato (31).

Le prove digitali rinvenute a seguito della perquisizione devono essere sequestrate, in originale o in copia, in base all'art. 253 comma 1 c.p.p., se consistono nel corpo del reato o in cose pertinenti al reato necessarie per l'accertamento dei fatti. In alternativa, ove materialmente consentito, il sequestro può avere ad oggetto i supporti che contengono le prove, ai fini della loro successiva analisi ed eventuale copia.

Lo stesso *standard* è richiesto per i dati attinenti al traffico, qualificabili come prove digitali quando riguardano comunicazioni avvenute tramite sistemi informatici (32) oppure l'uso di sistemi informatici (33). L'art. 132 comma 3 d.lgs. 30 giugno 2003 n. 196 (codice della *privacy*) prescrive che essi sono acquisibili presso i

---

(27) Si vedano gli artt. 244 comma 2, 247 comma 1 *bis*, 248 comma 2, 254 comma 1, 254 *bis*, 256 comma 1, 260 comma 2 c.p.p.

(28) Cfr. in particolare gli artt. 352 comma 1 *bis* e 354 comma 2 c.p.p.

(29) Artt. 352 comma 4 e 355 c.p.p.

(30) Cfr. S. Aterno, *Art. 8*, in Aa.Vv., *Cybercrime, responsabilità degli enti, prova digitale*, a cura di G. Corasaniti e G. Corrias Lucente, Padova 2009, p. 205 s. In senso diverso v. A. Cisterna, *Perquisizioni in caso di fondato motivo*, in *Guida dir*. 2008, n. 16, p. 66, secondo cui rientrerebbero nelle ispezioni operazioni come il sequestro in copia dell'*hard disk*.

(31) Così, in rapporto alle perquisizioni in generale, tra le molte, Cass., Sez. II, 19 giugno 2008, n. 35866. Sulla difficoltà di controllare il requisito in esame, ed il rischio di abusi che ne deriva, v. R. Orlandi, *Questioni attuali*, cit., p. 136 s.

(32) Delle quali i dati in questione consentono di stabilire le modalità (si veda l'art. 3 d.lgs. 30 maggio 2008 n. 109), senza però rivelarne i contenuti: ragione per cui sarebbe illogico includere la loro acquisizione nell'ambito delle intercettazioni, come invece dispone il discutibile disegno di legge S 1611 in materia di intercettazioni, giustamente criticato, sotto questo profilo, da V. Grevi, *Le intercettazioni come mero «mezzo di ricerca» di riscontri probatori?*, in *Cass. pen*. 2009, p. 850.

(33) Si pensi agli indirizzi *ip*, che permettono di determinare i tempi e la fonte degli ingressi nei sistemi, essenziali per risalire ai *computers* da cui gli ingressi hanno avuto origine: v. O.S. Kerr, *Digital evidence*, cit., p. 283 s.

fornitori di servizi informatici con decreto «motivato» del pubblico ministero. Nonostante che la norma non lo espliciti, è ragionevole pensare che la motivazione debba investire la probabilità di rinvenire prove del reato (34), ed inoltre che il provvedimento di apprensione dei dati sia impugnabile nelle stesse forme dei sequestri delle altre prove digitali (35). Lo conferma il fatto che l'art. 254 *bis* c.p.p., introdotto dalla l. n. 48 del 2008, prevede la possibilità di sequestrare i dati detenuti dai fornitori, «compresi quelli di traffico»: tale ultima disposizione, pur senza incidere sui termini di conservazione stabiliti dall'art. 132 codice della privacy, ha l'effetto di ricomprendere le operazioni in esame nell'orbita dei mezzi di ricerca di tutte le altre prove digitali.

La legge non commina nessuna inutilizzabilità nel caso in cui i requisiti previsti non fossero rispettati: nulla vieterebbe, ad esempio, di acquisire in dibattimento le prove digitali reperite a seguito di una perquisizione informatica ordinata direttamente dalla polizia pur in assenza di urgenza, oppure non convalidata dal pubblico ministero (36).

Questo regime di facile ingresso nei sistemi informatici, mirato a favorire la repressione penale anche a costo della riservatezza, è ineccepibile dal punto di vista del rispetto degli artt. 14 e 15 Cost.: quando le prove digitali sono situate in un domicilio o quando consistono in forme di corrispondenza la loro acquisizione avviene sulla base di un atto motivato dell'autorità giudiziaria, nei casi e nei modi legalmente prestabiliti.

Né la disciplina in esame appare criticabile sotto il profilo della sua opportunità. L'universalità delle prove digitali sconsiglia di limitarne la reperibilità solo in rapporto ad un elenco prestabilito di reati, come invece è previsto per le intercettazioni. Si aggiunga che queste ultime hanno ad oggetto dati comunicativi in via di formazione al momento stesso della loro captazione, e vanno necessariamente eseguite in segreto, per evitare di pregiudicarne l'effetto. Le prove digitali, al contrario, anche quando contengono comunicazioni – si pensi alla corrispondenza inoltrata per via telematica (37) – sono già cristallizzate nel loro apporto informativo. Questa è la ragione per cui, come si vedrà, vanno ricercate tramite un'indagine per-

---

(34) È naturale che tale probabilità non sia, invece, richiesta quando l'istanza proviene dal difensore dell'indagato, il quale «può richiedere direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391 *quater* del codice di procedura penale».

(35) Ritengono, al contrario, che l'acquisizione in base all'art. 132 codice della *privacy* non sia impugnabile S. Aterno e A. Cisterna, *Il legislatore interviene ancora sul data retention, ma non è finita*, in *Dir. pen. proc*. 2009, p. 289 s.

(36) Così C. Conti, *L'attuazione della direttiva*, cit., p. 26, anche se in riferimento ai soli dati di traffico. V. pure, prima dell'entrata in vigore della l. n. 48 del 2008, F. Ruggieri, *Profili processuali*, cit., p. 161.

(37) Sequestrabile in base all'art. 254 c.p.p., e quindi non sottoposta al regime delle intercettazioni: cfr. L. Luparia, *La ratifica della Convenzione cybercrime del Consiglio d'Europa. I profili processuali*, in *Dir. pen. proc*. 2008, p. 721.

cepibile da tutti i presenti, compreso il difensore dell'indagato (38): un'attività che non necessita, per questo suo carattere pubblico, dei più severi requisiti richiesti per le intercettazioni.

4.2. – Se appare sconsigliabile difendere la privacy in via preventiva, restringendo le modalità di accesso ai sistemi informatici da parte degli organi inquirenti, in quali limiti una protezione è conseguibile attraverso la disciplina della conservazione delle prove digitali?

Quest'ultima forma di salvaguardia deve esplicarsi sul duplice fronte della loro detenzione da parte dei fornitori dei servizi informatici e da parte dell'autorità giudiziaria. Si può già anticipare come la tutela appaia, nel complesso, eccessiva dal primo punto di vista, ed insufficiente dal secondo.

Quanto alle prove digitali presso i fornitori, le barriere per la riservatezza sono rappresentate dalle modalità di trattamento dei dati attinenti al traffico informatico e dai termini della loro conservazione.

Le regole di trattamento stabilite dal Garante per la privacy (39) sono senz'altro rigorose: esse consentono l'accesso ai dati solo a personale qualificato, tramite sistemi di autenticazione informatica e di registrazione degli ingressi. Sono, però, allo stato piuttosto costose da adottare, e non stupisce che la loro attuazione sia stata reiteratamente prorogata dal Garante.

La disciplina dei termini di conservazione dei dati, dal canto suo, appare eccessivamente sbilanciata a favore della tutela della riservatezza. I termini vigenti – dodici mesi dalla ricezione dei dati, ed inoltre ulteriori novanta giorni, prorogabili fino a sei mesi, per i dati oggetto della speciale procedura di congelamento introdotta dalla l. n. 48 del 2008 (40) – valgono indiscriminatamente per tutti i reati, e potrebbero risultare, in concreto, troppo ristretti (41), finendo con l'essere aggirati. Non si dimentichi che nessuna norma processuale vieta di acquisire i dati conservati oltre i termini prescritti (42). Divieti probatori non appaiono ricavabili neppure dalla generica inutilizzabilità stabilita dall'art. 11 comma 2 codice della privacy, che si origina a seguito della «violazione della disciplina rilevante in materia di trattamento dei dati personali»: nell'ambito di quest'ultima non si possono certo ricomprendere le regole di ammissione delle prove (43). Sarebbe stato preferibile

---

(38) V. *infra*, § 5.2.

(39) Si veda il provvedimento del 17 gennaio 2008, poi modificato dal provvedimento del 24 luglio 2008.

(40) Cfr. i commi 4 *ter-quinquies* dell'art. 132 codice della *privacy*, i quali hanno introdotto una normativa che non brilla per precisione: si vedano le critiche di F. Cerqua, *Il difficile equilibrio tra la protezione dei dati personali e le indagini informatiche*, in Aa.Vv., *Sistema penale*, cit., p. 236 s., e di L. Luparia, *La ratifica*, cit., p. 722 s.

(41) Così C. Conti, *L'attuazione della direttiva*, cit., p. 16 s.

(42) In senso contrario v. C. Conti, *L'attuazione della direttiva*, cit., p. 26.

(43) Cfr. C. Conti, *Accertamento del fatto e inutilizzabilità nel processo penale*, Padova 2007, p. 120 s.

prevedere termini più ampi perlomeno in rapporto ai reati di maggiore gravità, e comunque non scendere al di sotto dei ventiquattro mesi consentiti dalla direttiva europea attuata dalle prescrizioni in esame (44).

La riservatezza appare eccessivamente pregiudicata, per converso, sul fronte della detenzione delle prove digitali da parte degli organi inquirenti. Ciò è dovuto al fatto che in giurisprudenza si tende a differenziare il regime di conservazione delle prove digitali originali sequestrate insieme ai loro supporti materiali da quello delle eventuali copie, conservate su altri supporti. Non si dubita che gli originali vadano restituiti ai legittimi proprietari ai sensi dell'art. 262 c.p.p., al più tardi dopo il passaggio in giudicato della sentenza (45). Una volta riottenuti gli originali, però, l'indagato non avrebbe il diritto di entrare nel possesso anche delle copie (46).

Tale interpretazione trascura il fatto che non è in gioco solo il diritto di proprietà, a tutelare il quale sarebbe sufficiente la restituzione degli originali, ma anche la riservatezza. Le copie, in rapporto quest'ultima, sono pericolose tanto quanto gli originali, poiché contengono la medesima massa di informazioni. Se rimanessero indefinitamente a disposizione dell'autorità giudiziaria, aumenterebbe il rischio della loro apprensione da parte di terzi. Questo è il motivo per cui va preferita la lettura in base alla quale l'interesse in capo alla difesa ad impugnare i provvedimenti di sequestro dei dati digitali continua a sussistere anche dopo la restituzione degli originali (47).

5. – L'immaterialità delle prove digitali ne determina anche un'altra caratteristica: la loro congenita modificabilità. I dati contenuti in un sistema informatico sono facilmente alterabili da parte di chiunque ne venga in contatto. Sono altissimi i rischi che le prove digitali siano contraffatte o manipolate, volontariamente oppure a causa dell'impiego delle tecniche sbagliate (48).

Si capisce pertanto perché, affinché le prove digitali possano generare informazioni decisive in giudizio, è essenziale garantirne l'autenticità. A tale fine è necessario proteggere quella che gli studiosi anglosassoni definiscono la «catena di custodia» (*chain of custody*): le prove digitali devono rimanere integre in tutti i loro

---

(44) Art. 6 direttiva 2006/24/CE.

(45) Con possibilità per il pubblico ministero di riesaminare gli originali qualora vi fosse la necessità di svolgere ulteriori indagini impraticabili sulle copie: v. Cass., Sez. VI, 26 giugno 2009, n. 26699.

(46) Così Cass., Sez. un., 24 aprile 2008, n. 18253, poco prima dell'entrata in vigore della l. n. 48 del 2008.

(47) Cfr. S. Carnevale, *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare*, in *Dir. pen. proc*. 2009, p. 481; P. Tonini, *Documento informatico*, cit., p. 405.

(48) Si vedano, tra i molti, L. Luparia, *La disciplina processuale*, cit., p. 147 s.; P. Tonini, *Documento informatico*, cit., p. 404.

passaggi dal sistema informatico di origine alla disponibilità da parte del giudice del dibattimento (49).

Esistono dei possibili rimedi alla contaminazione delle prove digitali? È un pericolo che il legislatore non può permettersi di ignorare, a pena della vanificazione della pretesa punitiva, oppure della perdita di prove a difesa magari decisive per la sorte dell'imputato.

5.1. – Un primo antidoto è rappresentato dall'impiego delle metodologie di individuazione e di apprensione delle prove digitali in assoluto ritenute migliori dalla tecnica informatica.

Sotto questo profilo, l'ideale sarebbe che il legislatore potesse prestabilire una specifica tecnica di acquisizione dalle prove digitali, da osservare scrupolosamente a pena di inutilizzabilità ogni volta in cui un reato lasciasse tracce in un sistema informatico. Il metodo prescelto diventerebbe la «regola d'oro» (50) della formazione delle prove digitali, come l'esame incrociato lo è per l'assunzione delle prove dichiarative.

Al momento, però, purtroppo questa strada non è percorribile. L'informatica è una scienza relativamente giovane, e non si può dire che ad oggi esista un metodo di raccolta delle prove digitali in grado di imporsi su tutti gli altri (51). Gli esperti in materia suggeriscono perlopiù un approccio pragmatico: la scelta della tecnica da impiegare dipende dalla situazione che si presenta in concreto agli investigatori (52). Una normativa che cristallizzasse un metodo piuttosto che un altro sarebbe a rischio di immediata obsolescenza, in quanto fisserebbe regole che potrebbero essere velocemente superate dell'evoluzione.

Appare, quindi, giustificabile l'approccio della l. n. 48 del 2008, la quale non ha delineato una tecnica precisa di raccolta delle prove digitali, ma si è limitata a fissare gli obiettivi che gli organi inquirenti devono perseguire, in accordo con le *best practices* adottate a livello internazionale (53). Si tratta di due indicazioni di fondo che vanno osservate in rapporto a qualunque attività di raccolta delle prove digitali, nonostante che il legislatore non abbia interpolato tutti gli articoli del codice rilevanti in materia.

---

(49) Queste problematiche sono approfondite da E. Casey, *Digital evidence and computer crime*, 2ª ed., London 2004, p. 169 s.

(50) L'espressione è di P. Ferrua, *La regola d'oro del processo accusatorio: l'irrilevanza probatoria delle contestazioni*, in Aa.Vv., *Il giusto processo, tra contraddittorio e diritto al silenzio*, a cura di R.E. Kostoris, Torino 2002, p. 11 s.

(51) Per una rassegna v. E. Casey, *Digital evidence*, cit., p. 193 s. Nella dottrina italiana, G. Ziccardi, *Le tecniche informatico-giuridiche di investigazione digitale*, in L. Luparia, G. Ziccardi, *Investigazione penale*, cit., p. 3 s.

(52) V. A. Grillo, U.E. Moscato, *Riflessioni sulla prova informatica*, in *Cass. pen*. 2010, p. 375 s.

(53) Cfr. G. Ziccardi, *L'ingresso della* computer forensics *nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in Aa.Vv., *Sistema penale*, cit., p. 165 s.

a) Le operazioni di individuazione e di apprensione delle prove digitali – che il legislatore, come si diceva, ricomprende nelle ispezioni, nelle perquisizioni e nei sequestri – vanno svolte impiegando «misure tecniche» in grado di «assicurare la conservazione» e di «impedire l'alterazione» dei dati originali (54).

b) I sequestri tramite copia delle prove digitali devono avvenire su «adeguati supporti», tramite tecniche che assicurino «la conformità della copia all'originale e la sua immodificabilità» (55). La scelta se sequestrare i dati originali o se copiarli, giustamente, non è effettuata in astratto dal legislatore, ma è lasciata agli operatori, sulla base della situazione specifica (56).

Se si ritiene condivisibile la scelta di non precostituire un metodo di conduzione delle indagini informatiche, si devono però accettare pure i corollari che ne discendono.

Una prima conseguenza è che la raccolta delle prove digitali rientra nella classe degli accertamenti tecnici. Di qui la necessità di integrare le norme in tema di ispezioni, di perquisizioni e di sequestri con quelle che prescrivono l'intervento di appositi esperti in tutti gli stadi del procedimento: in sede di indagini di polizia (57), quando il pubblico ministero assume la direzione delle investigazioni (58), ed anche in dibattimento, dove il giudice può valutare l'operato degli investigatori attraverso il canale della perizia (59). Il che porta inevitabilmente al sostanziale monopolio degli esperti nella gestione e nella valutazione delle prove digitali, come del resto avviene in ordine ad ogni altra indagine scientifica immessa nel processo penale.

Mancando un preciso metodo di raccolta delle prove digitali consacrato dal legislatore, inoltre, è inevitabile che manchino pure le relative sanzioni. Non sono configurabili nullità di ordine generale o inutilizzabilità quando le indagini informatiche non sono svolte da esperti, o quando vengono impiegati metodi che non appaiono in grado di assicurare gli obiettivi perseguiti dal legislatore (60). Affermare il contrario (61) significherebbe ricavare divieti probatori basati sulla sola le-

---

(54) Art. 244 comma 2 c.p.p.; v. anche gli artt. 247 comma 1 *bis*, 254 comma 2, 259 comma 2, 352 comma 1 *bis* e 354 comma 2 c.p.p.

(55) Art. 260 comma 2 c.p.p.; v. anche gli artt. 254 *bis* e 354 comma 2 c.p.p. Una tecnica di copia in grado di assicurare questo risultato, anche se non sempre praticabile in concreto, è quella della *bitstream image*, su cui v. L. Luparia, *La ratifica*, cit., p. 719 s.

(56) Cfr. S. Aterno, *Art. 8*, cit., p. 209 s.

(57) Art. 348 comma 4 c.p.p.

(58) Artt. 359 e 360 c.p.p.

(59) Artt. 220 s., 468, 501 c.p.p.

(60) Così G. Braghò, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in Aa.Vv., *Sistema penale*, cit., p. 190 s. Ammette l'assenza di chiare previsioni di inutilizzabilità anche A. Monti, *La nuova disciplina del sequestro informatico*, in Aa.Vv., *Sistema penale*, cit., p. 217. In giurisprudenza v. già Trib. Bologna, 22 dicembre 2005, in *Dir. internet*, 2006, p. 153 s.

(61) Ritiene configurabile una nullità intermedia A. Vitale, *La nuova disciplina delle ispe-*

sione dell'interesse tutelato dalla legge (62), ma privi, in realtà, di un'espressa copertura normativa (63).

L'assenza di regole di esclusione della prova digitale non comporta la totale arbitrarietà dell'indagine informatica. Tutti gli errori tecnici commessi in sede di raccolta, pur non sanzionati con l'inutilizzabilità, sono destinati a pesare al momento della valutazione della prova. In quest'ultima sede il giudice ha la possibilità, grazie agli apporti dei periti e dei consulenti tecnici, di testare le tecniche informatiche impiegate, e di verificare se la catena di custodia delle prove digitali si sia spezzata (64).

5.2. – L'altro antidoto alla modificabilità delle prove digitali è rappresentato dall'attuazione del contraddittorio tecnico nella loro raccolta. È controverso, tuttavia, il modo in cui realizzare quest'ultimo: sono ipotizzabili almeno tre scenari interpretativi, variabili a seconda del bilanciamento tra le esigenze dell'accusa e i diritti della difesa che si ritenga preferibile.

a) *Negazione del contraddittorio tecnico*. È ricorrente l'affermazione giurisprudenziale secondo cui le operazioni di sequestro tramite copia delle prove digitali costituirebbero in ogni caso accertamenti tecnici ripetibili *ex* art. 359 c.p.p., da svolgere pertanto senza le garanzie fissate dall'art. 360 c.p.p. per gli accertamenti non ripetibili: il preavviso alla difesa in ordine al compimento delle operazioni, la possibilità di parteciparvi con un proprio esperto e il diritto all'instaurazione dell'incidente probatorio (65).

Questa asserzione, nella sua assolutezza, non è conciliabile con il carattere della modificabilità della prova digitale. Qualunque ingresso in un sistema informatico, anche se effettuato con le metodiche più avanzate, può alterare i dati in esso contenuti, generando mutazioni che, anche se minimali, rischiano di risultare de-

---

zioni e delle perquisizioni in ambiente informatico o telematico, in *Dir. internet* 2008, p. 509 s. Parla, invece, di inutilizzabilità E. Lorenzetto, *Le attività urgenti di investigazione informatica e telematica*, in Aa.Vv., *Sistema penale*, cit., p. 162 s.; analogamente, prima della l. n. 48 del 2008, L. Luparia, *La disciplina processuale*, cit., p. 196 s.

(62) Secondo l'impostazione di N. Galantini, *L'inutilizzabilità della prova nel processo penale*, Milano 1992, p. 139 s.

(63) Per la necessità che le inutilizzabilità siano esplicitamente costruite dalla legge processuale nella forma dei divieti di acquisizione v. F. Cordero, *Procedura penale*, 8ª ed., Milano 2006, p. 616 s.

(64) Cfr. G. Braghò, *L'ispezione*, cit., p. 188 s.

(65) Cfr. Cass., Sez. I, 5 marzo 2009, n. 14511, secondo cui l'attività di copia non comporterebbe «alcuna attività di carattere valutativo su base tecnico-scientifica», né determinerebbe «alcuna alterazione dello stato delle cose, tale da recare un pregiudizio alla genuinità del contributo conoscitivo in prospettiva dibattimentale»: sarebbe assicurata «in ogni caso, la riproducibilità di informazioni identiche a quelle contenute nell'originale»; negli stessi termini Cass., Sez. un., 25 febbraio 2010, n. 15208. V. pure Id., Sez. I, 30 aprile 2009, n. 23035; Id., Sez. I, 1º aprile 2009, n. 16942; Id., Sez. II, 31 marzo 2009, n. 18581; Id., Sez. I, 11 marzo 2009, n. 12472; Id., Sez. I, 26 febbraio 2009, n. 15153; Id., Sez. I, 26 febbraio 2009, n. 11863.

cisive se riguardano circostanze fattuali rilevanti ai fini dell'affermazione della responsabilità dell'imputato (66).

Vale a dire che le procedure di copia delle prove digitali, anche quando non riguardano dati in procinto di modificarsi – condizione che già da sola consentirebbe l'esperibilità della procedura degli accertamenti tecnici non ripetibili – potrebbero risultare tali da mutare irreversibilmente l'oggetto su cui cadono, integrando la fattispecie dell'art. 117 disp. att. c.p.p., e legittimando comunque l'impiego dell'art. 360 c.p.p.

Ancora più criticabile è la statuizione della Corte di cassazione in forza della quale l'esame di un sistema informatico non di pertinenza dell'indagato, svolto in via d'urgenza dalla polizia in base all'art. 354 comma 2 c.p.p., non sarebbe garantito dal diritto di assistere in capo al difensore (67).

È una lettura che va decisamente respinta, in quanto contrasta con la scelta della l. n. 48 del 2008 di includere le investigazioni informatiche nei contenitori normativi delle ispezioni, dei perquisizioni e dei sequestri: mezzi di ricerca della prova in rapporto ai quali il difensore, pur non avendo il diritto di essere preavvisato, ha in ogni caso il diritto di assistere (68), stabilito a pena di nullità intermedia (69).

L'importanza di questo diritto è cruciale: assistendo al compimento dell'atto, un difensore anche privo di cognizioni in materia avrebbe maggiori possibilità di informare il proprio consulente in ordine alle operazioni svolte dagli investigatori, in modo da contestare più efficacemente in dibattimento le tecniche impiegate.

Ciò non comporta che il diritto all'assistenza vada esteso in modo indiscriminato: esso non arriva a ricomprendere il diritto ad ottenere l'interruzione dell'attività di indagine qualora il difensore non fosse immediatamente reperibile (70). Al contempo, però, non va sistematicamente azzerato sulla base della sola urgenza dell'operazione (71).

Dalla configurazione legislativa delle indagini informatiche derivano precise ripercussioni anche ai fini della qualificazione giuridica di quelle operazioni di perquisizione occulta dei *personal computers* previste dall'art. 19 della Convenzione

---

(66) V., *ex plurimis*, L. Luparia, *La disciplina processuale*, cit., p. 151 s., e 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 s.

(67) Così Cass., Sez. I, 25 febbraio 2009, n. 11503; v. pure Id., Sez. III, 2 luglio 2009, n. 38087; Id., Sez. I, 30 aprile 2009, n. 23035; Id., Sez. I, 1º aprile 2009, n. 16942.

(68) Si vedano l'art. 356 c.p.p. riguardo alle indagini della polizia, e gli artt. 364 comma 5 e 365 c.p.p. quanto alle indagini del pubblico ministero.

(69) Per violazione di una norma attinente all'assistenza dell'imputato: cfr. gli artt. 178 lett. *c* e 180 c.p.p.

(70) In questo senso si veda Cass., Sez. fer., 25 luglio 2006, n. 27372.

(71) Non sorge nessuna nullità, invece, se il difensore, ritualmente avvisato, non si presenta: cfr. Cass., Sez. VI, 22 ottobre 2008, n. 13523.

di Budapest, possibili grazie all'impiego di appositi programmi in grado di introdursi nei sistemi informatici e di carpirne i contenuti (72).

Attività del genere rientrerebbero nel paradigma delle intercettazioni delineato dall'art. 266 *bis* c.p.p., seguendone la relativa disciplina, solo qualora riguardassero comunicazioni o conversazioni in corso mediante i sistemi informatici sotto controllo (73).

L'apprensione segreta dei dati digitali statici contenuti in un *computer* e non destinati ad essere condivisi con altre persone non trova, invece, legittimazione in nessuna norma (74). Non si tratterebbe di una perquisizione, la quale, stando alle indicazioni del codice, dovrebbe essere compiuta da esseri umani di fronte ai presenti ed al difensore, e non da invisibili dispositivi elettronici. Né integrerebbe una prova atipica, dato che l'art. 189 c.p.p. non può essere impiegato per aggirare la regolamentazione dei mezzi di ricerca della prova disciplinati dalla legge (75). Va considerata, dunque, un'attività di indagine irrituale, come tale giuridicamente improduttiva di effetti (76).

b) *Abuso del contraddittorio tecnico.* Muovendo dalla natura congenitamente non ripetibile delle indagini informatiche, altri affermano che, ai fini della piena realizzazione del contraddittorio tecnico, la raccolta delle prove digitali andrebbe svolta, almeno di regola, sulla base della procedura dell'art. 360 c.p.p. (77).

Questo secondo scenario interpretativo, speculare a quello appena considerato, è ineccepibile dal punto di vista dei presupposti teorici da cui muove. Proprio l'agevole modificabilità delle prove digitali, tuttavia, lo rende sconsigliabile. Le tracce più significative ai fini dell'accertamento della responsabilità, spesso, sono anche quelle nell'immediata disponibilità dell'indagato: si pensi alle prove situate nel suo *personal computer* o in dispositivi informatici di cui egli potrebbe facilmente entrare in possesso. Considerato che le prove digitali possono essere eliminate molto più rapidamente delle prove fisiche, è troppo alto il pericolo che, grazie al preavviso al difensore, l'indagato cancelli gli elementi a suo carico o, comunque, ne comprometta il valore conoscitivo.

c) *Graduazione del contraddittorio tecnico.* Nell'intento di contemperare le

---

(72) Sull'adozione di questa forma di perquisizione nell'ordinamento tedesco, e sulla declaratoria di incostituzionalità da parte della Corte costituzionale federale il 27 febbraio 2008 v. C. Sarzana di S. Ippolito, *Informatica*, cit., p. 680 s.

(73) Così S. Marcolini, *Le cosiddette perquisizioni on line (o perquisizioni elettroniche)*, in *Cass. pen.* 2010, p. 2859 s.

(74) Cfr. S. Aterno, *Art. 8*, cit., p. 213 s.

(75) «Non può considerarsi 'non disciplinata dalla legge' la prova basata su un'attività che la legge vieta»: Cass., Sez. un., 28 marzo 2006, n. 26795.

(76) Nel senso, invece, dell'inutilizzabilità di questa attività, la quale discenderebbe dal suo contrasto con il diritto alla riservatezza, tutelato dall'art. 8 C.e.d.u. e, come tale, dotato di rango costituzionale in forza dell'art. 117 Cost., v. S. Marcolini, *Le cosiddette perquisizioni*, cit., p. 2866 s.

(77) In questo senso v. P. Tonini, *Documento informatico*, cit., p. 405 s.; cfr. pure A. Ester Ricci, Digital evidence *e irripetibilità delle operazioni acquisitive*, in *Dir. pen. proc*. 2010, p. 345 s.

esigenze difensive con quelle dell'accusa, il contraddittorio tecnico, in questa materia, deve essere graduato.

Quando hanno ad oggetto dati nella potenziale disponibilità dell'indagato, le indagini informatiche vanno svolte assicurando l'effetto sorpresa tipico delle ispezioni, delle perquisizioni e dei sequestri: il difensore ha il diritto di assistervi senza però essere preavvisato.

In questa situazione il contraddittorio tecnico non può che essere posticipato in dibattimento, laddove la difesa ha la facoltà di contestare le procedure di raccolta e la genuinità dei dati digitali, anche tramite l'ausilio di propri esperti. Essenziale, a tal fine, è la documentazione audiovisiva integrale di tutte le operazioni svolte dagli organi inquirenti: tale adempimento, sebbene non sia previsto a pena di inutilizzabilità – e sotto questo profilo la l. n. 48 del 2008 appare criticabile – è indispensabile per rafforzare il peso conoscitivo delle prove digitali reperite. Allo stesso tempo, in giudizio la difesa può escutere con l'esame incrociato i tecnici che si sono occupati della raccolta dei dati, anche qualora si trattasse degli stessi poliziotti.

La più garantita procedura degli accertamenti tecnici non ripetibili va osservata – anche se si tratta di un dovere privo di sanzione – quando, in rapporto al caso concreto, il pericolo della distruzione delle prove non sussiste. Il caso paradigmatico è quello delle operazioni di copia delle prove originali già sequestrate dagli organi inquirenti, e reperibili presso l'ufficio del pubblico ministero (art. 260 comma 2 c.p.p.). Venendo meno il rischio dell'alterazione dei dati, è opportuno che il contraddittorio tecnico si riespanda nella sua pienezza. Non è necessario, peraltro, che le operazioni in esame avvengano in dibattimento, come sostenuto in giurisprudenza (78): diversamente la difesa non avrebbe la possibilità di estrarre ed esaminare una sua copia prima del giudizio, in tempo utile per apprestare al meglio la propria strategia.

MARCELLO DANIELE
Professore associato
nell'Università di Padova

(78) Cfr. Cass., Sez. III, 9 giugno 2009, n. 28524, secondo la quale si tratterebbe, in questa ipotesi, non della «semplice visione della cosa sequestrata che può essere effettuata fuori del contraddittorio alla sola presenza del custode», ma di un'«un'attività che deve essere necessariamente espletata nel dibattimento nel contraddittorio delle parti e sotto la direzione del giudice».