Capitolo I

Digital evidence e categorie probatorie

SOMMARIO: 1. Progresso tecnologico, metodi di conoscenza e "nuove" tipologie probatorie. – 2. La specificità della prova informatica. Dematerializzazione e dispersione dell'elemento di prova. – 3. *Computer forensics* e prova tecnico-scientifica. – 4. L'inquadramento sistematico della prova informatica tra mezzi di prova tipici ed innominati. – 5. *Digital evidence* e prova documentale.

1. *Progresso tecnologico, metodi di conoscenza e "nuove" tipologie probatorie*

La tecnologia trova, da sempre, applicazione nel processo penale in funzione di ausilio per l'accertamento di fatti di reato [1]. Dai nuovi ambiti scientifici si attinge per creare nuove tipologie di prova e nuovi strumenti investigativi [2]. Ma nessun settore appare tanto fecondo quanto quello informatico e telematico [3].

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 [4].

---

[1] Cfr., *ex multis*, G. DI CHIARA, *Il canto delle sirene. Processo penale e modernità scientifico-tecnologica: prova dichiarativa e diagnostica della verità*, in *Criminalia*, 2007, p. 19 ss.

[2] V. S. MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.*, 2015, p. 760 ss.

[3] Tanto che è stata, addirittura, preconizzata un'era ove qualsiasi fonte di prova sarà digitale. Cfr. G. ZICCARDI, *Informatica giuridica.* Privacy, *sicurezza informatica,* computer forensics *e investigazioni digitali*, vol. II, Giuffrè, Milano, 2012, p. 296.

[4] Cfr., da ultimo, R.E. KOSTORIS, *Il nuovo "pacchetto" antiterrorismo, tra prevenzione, contra-*

In effetti, il campo delle scienze informatiche e telematiche applicate al processo penale è angolo visuale privilegiato per fornire risposta all'interrogativo, di prepotente attualità, se l'interazione fra processo e scienza abbia mutato il sapere giuridico processuale, oltre che dal punto di vista quantitativo, anche sotto il profilo qualitativo. Vale a dire, se, per un verso, possa dirsi cambiato il diritto delle prove penali, nonché, per altro verso, sia mutato «nei suoi tratti essenziali il metodo investigativo e, con esso, il "codice genetico" del sapere processuale» [5].

Del resto, se «in forza delle prove è la multiforme vita umana, individuale e sociale, che balza nel processo; il loro contenuto si plasma secondo le infinite contingenze di questa» [6], non deve sorprendere che le cognizioni informatiche rivestano un ruolo di primo piano nell'accertamento penale dell'era digitale. Di qui, l'ineludibile esigenza, per gli organi investigativi, di ricercare elementi di prova tra i dati contenuti in sistemi informatici o telematici [7].

Il tema della prova informatica si è, per tale via, legato indissolubilmente a quello delle indagini preliminari, tanto da indurre alcuni autori a prendere atto dell'esistenza di una nuova tipologia d'indagine, definita in senso lato informatica [8], in una duplice accezione: qualora l'attività investigativa sia diretta «all'identificazione dell'autore di crimini informatici (cioè principalmente quelli previsti dalla L. 23 dicembre 1993, n. 547), come pure se si utilizzano tecnologie informatiche e telematiche nello svolgimento delle investigazioni sui reati comuni» [9].

Gli accennati mutamenti nelle tecniche d'indagine sono, in parte, frutto dell'utilizzo della tecnologia informatica a scopi criminali. In questa prospettiva, le indagini informatiche hanno rappresentato la risposta dello Stato alle

---

sto in rete e centralizzazione delle indagini, in R.E. KOSTORIS-F. VIGANÒ (a cura di), *Il nuovo "pacchetto" antiterrorismo*, Giappichelli, Torino, 2015, p. XVI.

[5] V., sia pure in prospettiva più ampia, S. LORUSSO, *Investigazioni scientifiche, verità processuale ed etica degli esperti*, in *Dir. pen. proc.*, 2010, p. 1346.

[6] La citazione è di E. FLORIAN, *Delle prove penali*, Vallardi, Milano, 1921, pp. 8-9.

[7] 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. Anche G. PIERRO, *Introduzione allo studio dei mezzi di ricerca della prova informatica*, in *Dir. pen. proc.*, 2011, p. 1516, evidenzia i riflessi processual-penalistici della rivoluzione digitale.

[8] Sulle più recenti tendenze delle indagini informatiche, v., da ultimo, A. SCALFATI, *Un ciclo giudiziario "travolgente"*, in *Proc. pen. giust.*, n. 4, 2016, pp. 114-115; S. SIGNORATO, *Tipologie e caratteristiche delle* cyber-investigations *in un mondo globalizzato*, in *Dir. pen. cont.*, n. 3, 2016, p. 190 ss.

[9] Così P. GUALTIERI, *Prova informatica e diritto di difesa*, in *Dir. pen. proc.*, 2008, *Dossier prova scientifica*, p. 70.

difficoltà di accertamento sorte in relazione a reati perpetrati mediante l'utilizzo di sistemi informatici o telematici [10].

Eppure, sarebbe del tutto miope circoscrivere l'ambito delle indagini informatiche al solo accertamento dei *computer crimes* [11]. A ben vedere, l'espansione incontrollata della *Information and Communication Technology* [12] – si pensi all'impiego diffuso di *social network* e *smartphone* – impone, oramai, l'acquisizione, l'analisi e la gestione di dati digitali nella stragrande maggioranza delle indagini in ambito penale.

Ed in effetti, al giorno d'oggi, nel corso delle indagini preliminari [13], vengono quotidianamente impiegate conoscenze del particolare ambito scientifico noto come *computer forensics*, o informatica forense [14], vale a dire quel settore di ricerca che studia «le problematiche tecniche e giuridiche correlate alle investigazioni sui dati digitali» [15].

---

[10] La dottrina nordamericana ha operato una tripartizione dei *cyber crimes* a seconda del collegamento del *computer* con il fatto criminoso: l'attrezzatura informatica può essere il *target* dell'azione criminosa (si pensi, nel nostro sistema, alla fattispecie di cui all'art. 615-*ter* c.p., rubricata "Accesso abusivo ad un sistema informatico e telematico"); oppure, può essere il *tool* mediante il quale l'azione viene realizzata; da ultimo, il *computer* può essere un mero *container* di prove. Cfr. THOMAS K. CLANCY, *Cyber Crime and Digital Evidence: Materials and Cases*, LexisNexis, New Providence, NJ, 2011, *ebook*.

[11] V., sul punto, F. RUGGIERI, *Profili processuali nelle investigazioni informatiche*, in L. PICOTTI (a cura di), *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.

[12] Cfr., in proposito, D. CURTOTTI, *Le ragioni di un confronto di idee*, in *Arch. pen.*, 2013, p. 765, nonché G. ZICCARDI, *Le tecniche informatico-giuridiche di investigazione digitale*, in L. LUPARIA-G. ZICCARDI, *Investigazione penale e tecnologia informatica*, cit., pp. 3-4.

[13] Cfr. V. PISANI, *La crisi delle garanzie difensive nell'attività atipica della polizia giudiziaria. Profili sistematici e prassi giurisprudenziali*, Giuffrè, Milano, 2016, p. 215 ss.

[14] Per una approfondita analisi degli aspetti tecnici del tema, v. AA.VV., Computer Forensics *e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Experta, Forlì, 2011, *passim*, nonché G. ZICCARDI, *Informatica giuridica*, cit., p. 291 ss.

[15] La definizione è di A. GRILLO-U.E. MOSCATO, *Riflessioni sulla prova informatica*, in *Cass. pen.*, 2011, p. 371, mentre G. ZICCARDI, *Informatica giuridica*, cit., pp. 296-297 la definisce come «quella scienza che studia il valore che un dato correlato ad un sistema informatico o telematico può avere in un ambito sociale, giuridico o legale […]», laddove per valore si intende la «capacità di resistenza ad eventuali contestazioni e capacità di convincimento del giudice, delle parti processuali o di altri soggetti […] in ordine alla genuinità, non ripudiabilità, imputabilità e integrità del dato stesso e dei fatti dallo stesso dimostrati». V. anche M. MEYERS-M. ROGERS, *Computer Forensics: The Need for Standardization and Certification*, in *2 Int. J. Dig. Evidence*, 2004, p. 4 ss.

Chiara la differenza ontologica, con riguardo all'oggetto, rispetto alle tradizionali metodologie d'indagine. Le informazioni rilevanti ai fini investigativi sono, nel caso della *computer forensics*, conservate e trasmesse in un linguaggio diverso, ovverosia quello digitale. Seppure i dati digitali, nel loro contenuto informativo, possono essere immediatamente percepiti da colui che viene in contatto con essi, ciò non significa che siano dotati di una materialità immediatamente percepibile. Essi vivono, piuttosto, quali frammenti di elettricità veicolati attraverso contenitori, dai quali il dato può essere estratto mediante complesse operazioni tecniche.

Diretto al recupero, a fini giudiziari, di simili dati, il metodo [16] seguito dagli esperti di *computer forensics* si esplica, in via di prima approssimazione, in quattro fasi [17] – raccolta, esame, analisi e presentazione – fondate su principi informatici [18]. Com'è agevole avvertire, sorgono numerosi interrogativi allorquando tale metodo, applicato per reperire, analizzare e conservare informazioni di cruciale importanza per l'accertamento di fatti di reato, viene posto a raffronto con la tradizionale epistemologia processual-penalistica [19].

---

[16] Inteso quale «protocollo di operazioni per ottenere un risultato». Cfr. P. FERRUA, *Metodo scientifico e processo penale*, in *Dir. pen. proc.*, 2008, *Dossier prova scientifica*, p. 12.

[17] Queste fasi della *computer forensics*, individuate dallo statunitense *National Institute for Standard and Technology*, sono richiamate da G. VACIAGO, Digital Evidence. *I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Giappichelli, Torino, 2012, p. 7. Non vi è, comunque, concordia su tali *step*. Quelli identificati P. PERRI, Computer forensics *(indagini informatiche)*, in AA.VV., *Dig. pen.*, IV ed., Utet, Torino, 2011, p. 101, tutto sommato analoghi, consistono, ad esempio, in identificazione, conservazione, analisi e presentazione.

[18] È opportuno anticipare che il legislatore, allorquando ha inserito le attività di *digital forensics* nel codice di rito, non ha indicato in dettaglio la metodologia da utilizzare ma ha concentrato la propria attenzione sul risultato dell'attività. 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. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul* cybercrime *(L. 18 marzo 2008, n. 48)*, Giuffrè, Milano, 2009, p. 166.

[19] Si è evidenziato come logica informatica (nonché, più in generale, scientifica) e logica del diritto siano diverse: nella prima, «lo sviluppo e l'impiego degli strumenti informatici si attesta su un carattere di ipoteticità, deduttività e monologicità, facendo sì che i vari ragionamenti condotti si fondino su premesse convenzionalmente stabilite e presupposte a priori»; mentre la seconda è una «logica retorica di tipo argomentativo e dialogico sulla base di veri propri ragionamenti di tipo endossale». Così A. TESTAGUZZA, Digital forensics. *Informatica giuridica e processo penale*, Cedam-Wolters Kluwer, Milano, 2014, p. 1. Più in generale, sulla tensione tra logica scientifica, da un lato, ispirata dalla precarietà delle proprie teorie e caratterizzata dalla rapida evoluzione, e, dall'altro, logica penale, le cui regole sono tendenzialmente immutabili e ricollegate al fine primario della ricostruzione di una vicenda in termini di sufficiente certezza, v. E. APRILE, *Le indagini tecnico-scientifiche: problematiche giuridiche sulla formazione della prova penale*, in *Cass. pen.*, 2003, p. 4034.

In questa prospettiva, è ben presto parsa ineludibile la necessità, puntualmente registrata in numerosi contributi scientifici, di una compiuta regolamentazione del fenomeno, nonché del correlativo inquadramento dogmatico.

Il primo e fondamentale piano di ricerca attiene, dunque, alle modalità di intreccio tra informatica forense, da un lato, ed istituti probatori e garanzie del processo penale, dall'altro. Attività ricostruttiva ulteriormente complicata dalla circostanza che le attività di *computer forensics* nascono parametrate e finalisticamente orientate all'ammissibilità della prova nel sistema in cui tale scienza nasce, vale a dire quello nordamericano [20]; sistema che, come noto, è sotto molti profili difficilmente sovrapponibile a quello italiano.

A completare il quadro, deve segnalarsi, altresì, che la *computer forensics* è scienza in costante mutamento. Con lo sviluppo tecnologico, sono cambiati ad impressionante velocità anche i luoghi ove reperire gli elementi di prova, tanto che alla nozione di *computer forensics* alcuni hanno sostituito quella, omnicomprensiva rispetto al dato digitale, di *digital forensics* [21].

Infatti, al giorno d'oggi, elementi utili all'accertamento, conservati in formato digitale, si ritrovano in numerosi dispositivi di utilizzo quotidiano, dal *personal computer* al *server* aziendale, dalla memoria di un lettore di *file* musicali ad una *pen-drive*. Tutti strumenti sconosciuti all'epoca di redazione dell'attuale codice di rito e, per di più, notevolmente diversi l'uno dall'altro, quanto a modalità di accesso e di recupero del loro contenuto.

Tuttavia, l'evoluzione legislativa non ha seguito di pari passo quella tecnologica. La prima innovazione codicistica frutto dell'incontro tra macchina giudiziale e tecnologia informatica e telematica risale al 1993; segnatamente, il riferimento è alla creazione dell'art. 266-*bis* c.p.p., relativo all'intercettazione di comunicazioni informatiche o telematiche, all'interno del Libro III sulle prove. Tale modifica, però, è rimasta a lungo isolata: si è dovuto attendere ben quindici anni, allorché la L. n. 48/2008 [22] ha provveduto ad un più generale, sia pur lacunoso, tentativo di sistemazione della materia mediante una serie di interpolazioni *ad hoc*.

---

[20] V. G. ZICCARDI, *Le tecniche informatico-giuridiche di investigazione digitale*, cit., p. 17.

[21] Cfr. A. GHIRARDINI-G. FAGGIOLI, *Digital Forensics*, Apogeo, Milano, 2013, *passim*. Per una panoramica sulle molteplici categorie della *digital forensics*, tra cui *computer media analysis* e *media forensics*, cfr. A. TESTAGUZZA, Digital forensics. *Informatica giuridica e processo penale*, cit., p. 2, nonché G. MAINO, *Nuove sfide per l'informatica forense*, in M. ANDRETTA-D. FONDAROLI-G. GRUPPIONI (a cura di), *Dai "casi freddi" ai "casi caldi". Le indagini storiche e forensi fra saperi giuridici e investigazioni scientifiche* (Atti del Convegno), Wolters Kluwer, Milano, 2014, p. 151 ss.

[22] L. 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*, in *G.U.*, 4 aprile 2008, n. 80.

Simili mutamenti appaiono comunque significativi, giacché, da un lato, evidenziano la scarsa attenzione riservata dal legislatore al fenomeno, sensibile testimonianza di una malriposta fiducia nella capacità di adattamento a fenomeni nuovi degli istituti già previsti in tema di prova [23]; dall'altro lato, confermano l'indissolubile endiadi fra dato digitale ed indagini preliminari.

In realtà, nell'arco di tempo segnalato, intervallato da sporadiche modifiche legislative, le indagini informatiche hanno affrontato, nella prassi, una evoluzione costante [24]. Alle prime, pionieristiche indagini aventi ad oggetto *floppy disk* si sono, in seguito, sostituite attività sempre più complesse, che reclamano competenze tecniche specifiche e sofisticate, fino alle recentissime ipotesi di analisi dei dati contenuti in un sistema di *cloud computing* [25].

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 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) da reperire. Il che è diretta conseguenza, soprattutto, delle caratteristiche intrinseche del dato digitale.

2. *La specificità della prova informatica. Dematerializzazione e dispersione dell'elemento di prova*

In assenza di una precisa nozione di risultanza frutto dell'analisi ed elaborazione di strumenti informatici e telematici, quest'ultima è stata oggetto di diverse ricostruzioni dogmatiche, le quali hanno portato ad una pletora di definizioni.

---

[23] Secondo 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. 343, il ritardo del legislatore deve attribuirsi, altresì, all'erronea convinzione che la prova digitale fosse strumento conoscitivo rilevante solo per l'accertamento dei *computer crimes* di cui alla L. n. 547/93.

[24] 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.

[25] 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, nonché 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. Sulle problematiche relative alla raccolta transfrontaliera della prova digitale, con precipuo riguardo al *cloud computing*, v. F. SIRACUSANO, *La prova informatica transnazionale: un difficile "connubio" tra innovazione e tradizione*, in *Proc. pen. giust.*, 2017, p. 178 ss.

Alcuni autori hanno utilizzato la dizione di matrice statunitense *digital evidence*, intendendola quale contenitore ove ricomprendere qualsiasi «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» [26].

L'espressione *digital evidence* è stata tradotta, talvolta, come "prova digitale", facendo leva sull'essenza del dato, frutto di una manipolazione elettronica di numeri [27]. Mentre altri studiosi, proprio a causa della «strutturale ed intrinseca immaterialità dell'elemento di prova», hanno ritenuto più corretta la locuzione "prova di natura digitale" [28].

In dottrina, si sono anche utilizzate, spesso come sinonimi di *digital evidence* [29], le locuzioni "prova informatica" [30] e "prova elettronica" [31], quali corri-

---

[26] Così L. MARAFIOTI, *Digital evidence* e processo penale, in *Cass. pen.*, 2011, p. 4509. La definizione riecheggia quella di E. CASEY, *Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet*, Elsevier, London, 2004, p. 12, secondo cui può definirsi *digital evidence* qualsiasi dato conservato o trasmesso mediante un *computer* che possa supportare o confutare la tesi circa l'avvenuta commissione di un crimine, o che attenga ad elementi rilevanti quali il movente o l'alibi. Chiara, in quest'ultima definizione, la prospettiva finalistica relativa all'utilizzazione del dato a fini procedimentali. Definizione simile è stata, altresì, recepita in ambito europeo, ove nell'ambito del progetto CyberCrime@IPA è stata stilata una *Electronic Evidence Guide*, la quale identifica la prova informatica come «l'insieme dei dati e delle informazioni che derivano da dispositivi elettronici come i *computer* e le relative periferiche, le reti di *computer*, i telefoni cellulari, le fotocamere digitali o altri dispositivi mobili, i dispositivi di archiviazione dati, nonché da *internet*, [ovvero] informazioni generate, memorizzate o trasmesse mediante dispositivi elettronici che possono essere utilizzate in giudizio». Ne riferisce E. COLOMBO, *Una novità dall'Unione Europea per la lotta ai* Cybercrimes*: una* Electronic Evidence Guide, in *Cass. pen.*, 2014, p. 374 ss.

[27] Così M. DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, p. 283; v. anche ID., *Caratteristiche della prova digitale*, in F. RUGGIERI-L. PICOTTI (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica: aspetti sostanziali e processuali*, Giappichelli, Torino, 2011, p. 204. 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 "meta-territorio", dove sembrerebbe perdere consistenza la naturale propensione dell'uomo di rapportarsi al mondo "reale" con l'uso dei cinque sensi». S. ATERNO, *Le investigazioni informatiche e l'acquisizione della prova digitale*, in *Giur. merito*, 2013, p. 955, parla di prove digitali forensi. In giurisprudenza, la locuzione è utilizzata da Cass., Sez. V, 31 marzo 2015, Asciore e al., *inedita*.

[28] Cfr. F.M. MOLINARI, *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen.*, 2013, p. 1261.

[29] Lo sottolinea G. DI PAOLO, voce *Prova informatica (diritto processuale penale)*, in *Enc. dir.*, Annali, VI, Giuffrè, Milano, 2013, p. 736. Si è, tuttavia, esattamente osservato che le espressioni *digital evidence*, da tradurre con prova digitale o prova di natura digitale, ed *electronic evidence* non sono sinonimi, giacché quest'ultima comprende anche fonti di natura analogica, che ben possono essere digitalizzate ma non nascono in tale formato. Cfr., a tal riguardo, S. MASON, *Electronic Evidence: Disclosure, Discovery and Admissibility*, LexisNexis, Londra, 2007, p. 22.

spettivi della diversa espressione anglofona *electronic evidence*. Con tale locuzione, si intende un'informazione generata, conservata o trasmessa attraverso apparecchiature elettroniche che possa essere utilizzata di fronte ad un giudice [32].

Sul punto occorre intendersi fin da subito. Ben può utilizzarsi la formula *digital evidence*, o prova digitale, quale recipiente ove includere ogni forma di utilizzo a fini procedimentali, in senso lato, di dati originariamente contenuti in supporti informatici o telematici, oppure ancora trasmessi in modalità digitale. A patto, però, di tenere a mente che si tratta di un fenomeno con diverse sfaccettature, che mal si presta a inquadramenti a priori ed è difficilmente conciliabile con le tradizionali distinzioni in tema di prova.

Più in particolare, la natura multiforme del dato digitale sconsiglia generalizzazioni aprioristiche. Già si è accennato alla difficoltà ricostruttiva di un *iter* di reperimento dell'informazione digitale, giacché esso muta a seconda del contenitore dell'informazione. Ebbene, i problemi classificatori sussistono anche con riferimento al risultato di prova ottenuto, diversamente classificabile a seconda del grado di aderenza all'oggetto di prova.

Con riguardo a tale ultimo aspetto, appare arduo teorizzare in via generale un inquadramento della *digital evidence* nella conseueta bipartizione tra prove rappresentative-dirette e prove critiche-indirette [33]. Difatti, la natura informatica del dato da cui trarre il risultato probatorio può vertere sia direttamente

---

[30] Cfr. G. PIERRO, *op. cit.*, p. 1516 ss. La dicitura prova informatica è stata, altresì, utilizzata dalla giurisprudenza fin dalle prime manifestazioni del dato digitale nelle aule di giustizia: cfr. Cass., Sez. I, 19 gennaio 2000, Pellegrino, *inedita*, dove con quella dicitura si indicano alcuni «dischetti» (*floppy disk*); la pronuncia riveste interesse anche nella parte in cui include i medesimi *floppy disk* all'interno delle prove documentali. La locuzione prova informatica è poi tornata in auge più di recente, allorché è stata utilizzata al fine di indicare gli esami compiuti su un *computer* (Cass., Sez. fer., 6 settembre 2012, Franchini, *inedita*), nonché un *file* ed una ripresa tratta da un sistema di videosorveglianza e rinvenuta in un *hard disk* (Cass., Sez. II, 4 giugno 2015, Scanu e al., in *C.E.D. Cass.*, rv. 264286).

[31] V. R. KOSTORIS, *Ricerca e formazione della prova elettronica: qualche considerazione introduttiva*, in F. RUGGIERI-L. PICOTTI (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica: aspetti sostanziali e processuali*, Giappichelli, Torino, 2011, p. 179 ss. La locuzione "prova elettronica" è utilizzata dalla Relazione di accompagnamento al d.d.l. n. 2807, in occasione dei lavori preparatori della futura L. n. 48/2008. Nella giurisprudenza, si ritrova un isolato, sia pur recente, utilizzo dell'espressione in Cass., 7 gennaio 2015, Boselli, in *C.E.D. Cass.*, rv. 262084.

[32] Questa la definizione adottata dalla *International Organization on Computer Evidence* nel 2000. La richiama G. VACIAGO, *op. cit.*, p. 1. Tale locuzione, tuttavia, appare troppo ampia, giacché appare destinata a ricondurre alle prove di fonte digitali anche tutte le ipotesi di prova digitale creata in ambito endoprocedimentale. Sul punto, v. *infra*, in questo paragrafo.

[33] V., per tutti, P. FERRUA, *La prova nel processo penale: profili generali*, in P. FERRUA-E. MARZADURI-G. SPANGHER (a cura di), *La prova penale*, Giappichelli, Torino, 2013, p. 11, anche per i riferimenti dottrinali citati in nota 19.

sul *thema probandum* sia su un fatto secondario da cui risalire al fatto principale [34]: quale esempio del primo tipo v'è l'immagine pedopornografica in formato digitale il cui possesso è contestato all'imputato; quale esempio del secondo tipo possono addursi i *file* di *log* [35] circa l'avvenuto accesso ad un *social network* per mezzo di un *computer* localizzato sulla *scena criminis* ove è stato commesso un omicidio nella medesima finestra temporale [36].

Se la ricerca di un minimo comun denominatore fra le diverse ipotesi di *digital evidence* non trova approdi con riferimento al risultato di prova, le cose stanno diversamente allorché l'attenzione si sposta sull'elemento di prova. Ed invero, l'unica *reductio ad unum* possibile della categoria qui analizzata pare attenere alla natura dell'elemento di prova, e precisamente alla peculiare natura del dato.

In effetti, ciò che accomuna tutte le definizioni di *digital evidence* fornite è proprio la fondamentale caratteristica del dato da cui trarre l'informazione probatoria: la sua materialità non immediatamente percepibile [37]. E gran parte delle criticità del fenomeno della prova digitale e delle indagini informatiche e telematiche nascono proprio dalla circostanza che gli elementi ricercati dagli organi investigativi consistono in «*zeroes and ones of electricity*» [38].

---

[34] Talvolta il collegamento tra dato digitale e oggetto di prova è estremamente labile: ad esempio, è stato valutato quale elemento di riscontro ad una ipotesi di cessione di materiale pedo-pornografico la presenza, sul *personal computer* in ipotesi utilizzato per la condotta contestata, di programmi quali *AutohideIP*, *MooD*, *Antirecovery* e *Codissey Freeraser*, volti a mascherare l'indirizzo *Internet Protocol* e a «distruggere ogni dato recuperabile nell'*hard disk* senza toccare i *file* esistenti»: una vicenda simile si rinviene in Cass., Sez. III, 7 novembre 2013, n. 11535, *inedita*.

[35] Si tratta di quei *file*, solitamente generati automaticamente dagli apparati informatici e telematici, che memorizzano in maniera sequenziale e cronologica le attività compiute da un utente e che, pertanto, consentono successivamente di ripercorrerne le tracce. Cfr. G. VACIAGO, *op. cit.*, p. 24 ss. Anche la Cassazione si è occupata del tema, in una ipotesi di accesso abusivo a sistemi informatici: «è sempre il server *web* violato che conserva le informazioni dell'accesso o della permanenza del *client*, mantenendo la traccia sul proprio *file log* di tutte le attività compiute a partire dall'accesso sino alla sua uscita dal sistema; tra queste vi è il numero *IP* del *client*, la sua *login*, la data dell'accesso e le pagine visitate» (Cass., Sez. I, 27 maggio 2013, confl. comp. in proc. Martini, in *Cass. pen.*, 2014, p. 1706, con nota di S. Aterno).

[36] Il caso si è realmente verificato: ne dà atto Cass., Sez. I, 5 febbraio 2014, Angelillo, *inedita*.

[37] Come precisato in dottrina, il tradizionale assunto circa l'immaterialità delle prove digitali non deve essere inteso nel senso che le medesime siano prive di fisicità: si tratta, viceversa, di «impulsi elettrici che rispondono ad una sequenza numerica prestabilita e che, convogliati in un supporto informatico dotato di una memoria, originano informazioni intellegibili». Così M. DANIELE, *La prova digitale nel processo penale*, cit., p. 284.

[38] L'espressione è di O. KERR, *Digital Evidence and the New Criminal Procedure*, in *105 Colum. L. Rev.*, 2005, p. 291. Del resto, si tratta di trasformazioni avvertibili più in generale nell'intero sistema penale: «il concetto di azione penalmente rilevante subisce nella realtà virtuale una accentuata modificazione fino a sfumare in impulsi elettronici; l'*input* rivolto al computer

Tali caratteri sono stati, altresì, ben evidenziati dalla giurisprudenza. Invero, la Corte di Cassazione, in un apprezzabile sforzo definitorio volto all'identificazione della nozione di sistema informatico, ha chiarito come quest'ultimo alluda ad «una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche», caratterizzate, a loro volta, dalla «registrazione (o "memorizzazione"), per mezzo di impulsi elettronici, su supporti adeguati, di "dati" di rappresentazioni elementari di un fatto, effettuata attraverso simboli (*bit*) numerici ("codice"), in combinazioni diverse: tali dati, elaborati automaticamente dalla macchina, generano le informazioni […]»[39], costituite da «un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente»[40].

L'impalpabilità di questi dati conferisce i caratteri di volatilità e fragilità al-

da un atto umano consapevole e volontario si traduce in un trasferimento sotto forma di energie o *bit* della volontà dall'operatore all'elaboratore elettronico, il quale procede automaticamente alle operazioni di codificazione, di decodificazione, di trattamento, di trasmissione o di memorizzazione di informazioni». E ancora: «nel *cyberspace* i criteri tradizionali per collocare le condotte umane nel tempo e nello spazio entrano in crisi, in quanto viene in considerazione una dimensione "smaterializzata" (dei dati e delle informazioni raccolti e scambiati in un contesto virtuale senza contatto diretto o intervento fisico su di essi) ed una complessiva "delocalizzazione" delle risorse e dei contenuti (situabili in una sorte di meta-territorio)». Così, con chiarezza, Cass., Sez. Un., 26 marzo 2015, confl. comp. in proc. Rocco, in *Dir. pen. proc.*, 2015, p. 1291 ss., con nota di R. Flor, nonché: *ivi*, 2016, p. 80 ss., con nota di E. Anselmi; in *Cass. pen.*, 2015, p. 3501 ss., con nota di M.L. Sciuba; in *Giust. pen.*, 2015, n. 7, III, p. 402 ss., con nota di A. Leopizzi; in *Proc. pen. giust*., n. 4, 2015, p. 38 ss., con nota di P. Maggio; in *Riv. pen.*, 2016, p. 563 ss., con nota di D. Giannelli.

Nella dottrina processual-civilistica si è ben chiarito come «il "segno digitale" consiste essenzialmente in sequenze di simboli binari, chiamati *bit*, attraverso i quali può essere codificata e memorizzata dall'elaboratore qualsiasi informazione costituita da testi, suoni, immagini. Di per sé, quindi il contenuto rappresentativo dei dati informatici è di fatto inaccessibile ad un comunicante umano: perché avvenga il processo comunicativo è infatti necessaria l'intermediazione della macchina che, eseguendo determinati programmi (c.d. *software*), nella fase di *input* configura il messaggio in forma digitale, per renderlo poi fruibile dall'utente, decodificandolo, mediante appositi dispositivi di *output* (*monitor*, stampante, altoparlanti)». Così F. ROTA, *I documenti*, in M. TARUFFO (a cura di), *La prova nel processo civile*, Giuffrè, Milano, 2012, p. 729.

[39] Così Cass., Sez. VI, 4 ottobre 1999, Piersanti, in *Cass. pen.*, 1999, p. 2990 ss., con note di L. Cuomo e S. Aterno, definizione poi richiamata da numerosissime sentenze dei giudici di legittimità, anche successivamente alla ratifica della Convenzione di Budapest, secondo cui costituiscono un sistema informatico «qualsiasi apparecchiature o gruppi di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica dei dati». Cfr., da ultimo, Cass., Sez. Un., 26 marzo 2015, Rocco, cit., in cui si rinviene anche l'interessante affermazione per cui un «dispositivo elettronico assurge al rango di sistema informatico o telematico se si caratterizza per l'installazione di un *software* che ne sovrintende il funzionamento, per la capacità di utilizzare periferiche o dispositivi esterni, per l'interconnessione con altri apparecchi e per la molteplicità dei dati oggetto di trattamento».

[40] Cass., Sez. II, 10 aprile 2013, Allegro, *inedita*.

la prova digitale [41]. A titolo d'esempio, un *file* comune, quale una immagine in formato *jpg*, comprende circa un milione di *bit* [42]; la modifica di uno solo di essi può comportare un mutamento 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 la rilevanza probatoria.

Ne consegue che l'esigenza di tutelare la genuinità della prova – ineludibile per l'intero sistema processuale – si ripropone, nella fattispecie, con rinnovato vigore.

Proprio la preoccupazione [43] di evitare la dispersione dell'elemento di prova informatico pare aver guidato il legislatore allorquando questi, con la L. n. 48/2008, nel modificare numerose disposizioni codicistiche relative alla ricerca della prova e all'attività di polizia giudiziaria, ha inserito una serie di disposizioni attente, più che al metodo da utilizzare per acquisire l'informazione utile a fini probatori, alla finalità di tutelare la conservazione e di impedire l'alterazione dei dati originali [44]. In altre parole, concentrando la propria attenzione sulla natura alterabile e fragile della fonte di prova digitale.

Appaiono, altresì, frutto della presa di coscienza dell'intrinseca volatilità del dato informatico le particolari cautele imposte in caso di duplicazione del dato ai sensi dell'art. 260 c.p.p. Una prescrizione, quest'ultima, che pare una sorta di "traduzione" informatica della consueta estrazione di copia dei documenti cartacei, nonché della riproduzione delle *res* facilmente alterabili già prevista anteriormente alla riforma; ulteriore conferma, allora, della natura deteriorabile (e falsificabile) del dato.

---

[41] Cfr. F. SIRACUSANO, *La prova informatica transnazionale*, cit., p. 179.

[42] V. S. ATERNO, *Acquisizione 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 2*n* valori differenti. Una sequenza di 8 *bit* corrisponde a un *byte*. Cfr. anche G. PIERRO, *op. cit.*, p. 1516.

[43] Tanto che alcuni Autori hanno teorizzato una sorta di «principio di cautela» nel trattamento del dato informatico. Cfr. G. ZICCARDI, *L'ingresso della* computer forensics *nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, cit., p. 177.

[44] In particolare, clausole siffatte si rinvengono negli artt. 244, comma 2, 247, comma 1-*bis*, 254, comma 1, 260, comma 2, 352, comma 1-*bis*, 354, comma 2, c.p.p. Cfr. G. ZICCARDI, *L'ingresso della* computer forensics *nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, cit., p. 166 ss. L'Autore evidenzia che le nuove disposizioni sono diretta emanazione dei principali concetti di *computer forensics*, vale a dire valore e resistenza dei dati, intesi quali capacità di convincimento del giudice e di resistenza a contestazioni delle parti processuali.

Discorso analogo vale per la regola di comportamento imposta dall'art. 354 c.p.p., secondo cui, alle prese con sistemi informatici o telematici, gli ufficiali e gli agenti di polizia giudiziaria debbono, in primo luogo, assicurare – ed assicurarsi – l'informazione probatoria, provvedendo all'immediata duplicazione del dato su adeguati supporti. Si tratta, anche in questo caso, di una disposizione legata a doppio filo alle peculiarità della fonte di prova in oggetto.

Ciò premesso, pare comunque necessaria qualche annotazione ulteriore al fine di delimitare l'indagine circa l'utilizzo a fini probatori di dati digitali.

In primo luogo, deve rilevarsi che, in senso stretto, può parlarsi di *digital evidence* solo in riferimento a materiale probatorio digitale a genesi extraprocedimentale [45]. Ciò, sia che l'informazione venga creata dall'utente sia che il dato venga generato da una operazione automatica dell'elaboratore [46].

Insomma, la peculiare natura dell'incorporamento dell'informazione – a base digitale – non è, da sola, tale da far propendere per l'inclusione di uno strumento nel novero delle prove digitali.

Al riguardo, è stata teorizzata una distinzione tra prove digitali extraprocedimentali ed endoprocedimentali [47]. Nel primo caso, oggetto dell'attività è un dato digitale, nella sua forma statica (si pensi al *file* conservato in una memoria) oppure dinamica (ad esempio, un flusso di comunicazioni tra più sistemi informatici); nel secondo, invece, lo strumento informatico o telematico è utilizzato dagli attori processuali nell'ambito delle loro funzioni, quali la redazione di un'informativa da parte della polizia giudiziaria, oppure di una sentenza da parte del giudice, a mezzo di strumentazione informatica, ad esempio tramite un *personal computer* [48], o ancora per la ricostruzione di un accadimento

---

[45] Cfr., in proposito, G. DI PAOLO, *op. cit.*, p. 738.

[46] Si pensi al trasferimento su un *computer* di una immagine fotografica, scattata con uno *smartphone*, in formato *jpg*. Il salvataggio è frutto di una scelta dell'utente; allo stesso tempo, però, automaticamente nella memoria digitale verranno conservate automaticamente numerose informazioni, quali, a titolo d'esempio, la data in cui l'immagine è stata scattata e la data di salvataggio sull'*hard disk*. Informazioni, queste, che potrebbero risultare di grande utilità ai fini dell'accertamento della commissione di un reato.

[47] V., ancora, G. DI PAOLO, *op. cit.*, pp. 740-741 e, specialmente, nota 34. La distinzione proposta riecheggia quella di matrice statunitense tra *computer-derived* e *computer-generated evidence*: nella prima, lo strumento informatico è l'oggetto dell'attenzione investigativa; nella seconda, è il soggetto dell'operazione dimostrativa, ovvero lo strumento utilizzato dalle parti in funzione ausiliaria per la ricostruzione di un fatto. Cfr., a tale riguardo, L. LUPARIA, *Processo penale e tecnologia informatica*, in *Dir. internet*, 2008, p. 224.

[48] Appaiono rientrare in questa categoria anche quei casi in cui «il sistema informatico sia il mezzo dell'operazione probatoria, e precisamente il *medium* per la raccolta di dichiarazioni procedimentali», come avviene nel caso di esame a distanza previsto dall'art. 147-*bis*, commi 2-5, disp. att. c.p.p. Cfr. G. DI PAOLO, *op. cit.*, p. 742. Sulla tecnologia digitale come nuovo mezzo di formazione della prova dichiarativa v. M. DANIELE, *La formazione digitale delle prove*, Giappichelli, Torino, 2012, p. 7 ss.

a fini probatori [49]. Poiché in tali ultimi casi gli atti descritti nulla hanno a che vedere con l'acquisizione, la gestione e l'analisi di dati informatici, quest'ultima categoria esorbita dall'indagine che si sta conducendo; appare più adeguata, al riguardo, la locuzione "documentazione informatica di atti procedimentali" [50].

Più problematica l'inclusione nel novero delle *digital evidence* di quelle ipotesi di strumenti probatori in cui «l'utilizzo della tecnologia informatica, pur costituendo una componente essenziale (e qualificante) dell'atto di indagine, non abbia di mira una realtà digitale» [51].

In effetti, la distinzione potrebbe apparire arbitraria, giacché, effettivamente, anche in simili casi il frutto dell'attività investigativa è rappresentato da dati digitali. In tali ipotesi, come si è rilevato, dirimente risulterebbe il bersaglio dell'azione investigativa [52]. Qualora quest'ultimo non sia rappresentato da un dato digitale, l'utilizzo di strumenti tecnologici per la ricerca del dato – paradigmatico l'esempio delle video-registrazioni – sarebbe soltanto un mero accidente frutto del ventaglio di possibilità tecnologiche offerte agli investigatori.

Tuttavia, se la distinzione appena accennata è agevole in astratto, in concreto potrebbe risultare ostico distinguere i mezzi di ricerca della prova digitale da quelli tradizionali. Tanto che i confini tra gli istituti volti a disciplinare gli uni e gli altri vengono, talvolta, persino a confondersi.

Un esempio paradigmatico di quanto appena rilevato si rinviene con riferimento all'apprensione in tempo reale di dati informatici. Come noto, le coordinate in ordine alla captazione di conversazioni telefoniche sono dettate dagli artt. 266 e ss. c.p.p.; per le intercettazioni telematiche una disciplina, parzialmente diversa, è prevista dagli art. 266-*bis* e 268, commi 3-*bis*, 6 e 7, c.p.p. Quale discrimine tra i due istituti, il legislatore ha concentrato l'attenzione sul mezzo attraverso il quale avvengono le comunicazioni: quelle mediante telefono (e altre forme di telecomunicazione) ricadono nell'ambito applicativo dell'art. 266 c.p.p.; quelle relative a flussi di comunicazioni tra sistemi informatici o telematici nell'art. 266-*bis* c.p.p.

Ebbene, lo sviluppo tecnologico ha fatto sì che l'intero sistema di telefonia,

---

[49] Su questa peculiare forma di *computer-generated evidence*, v., ampiamente, F. SBISÀ, *Le* computer-generated evidence *da strumento a prova tecnico-scientifica nel processo penale statunitense*, in C. CONTI (a cura di), *Scienza e processo penale. Nuove frontiere e vecchi pregiudizi*, cit., p. 423 ss.

[50] Si segue, qui, l'insegnamento sempre attuale, sia pure originariamente offerto con riferimento ai tradizionali documenti analogici, da E. FLORIAN, *op. cit.*, pp. 60-61.

[51] Così G. DI PAOLO, *op. cit.*, pp. 741-742. Si pensi, a titolo d'esempio, alle videoregistrazioni mediante strumenti informatici o telematici o al monitoraggio a mezzo *G.P.S.*

[52] La tesi è di G. DI PAOLO, *op. loc. ult. cit.*

mobile e fissa, sia, oramai, un vero e proprio sistema telematico, come espressamente riconosciuto anche dalle Sezioni Unite della Corte di Cassazione [53].

Dunque, a voler seguire pedissequamente il criterio discretivo in base alla natura del dato appreso (digitale o meno), ciò comporterebbe una radicale 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., giacché tutte le captazioni di comunicazioni vocali, anche quelle a mezzo del telefono, dovrebbero ormai ricondursi *tout court* all'art. 266-*bis* c.p.p. Dunque, l'art. 266 c.p.p. diverrebbe lettera morta: conseguenza, questa, evidentemente inaccettabile.

Si tornerà sul punto, ma già ora appare chiaro quanto sia insidioso e complesso il terreno sul quale l'interprete è chiamato ad operare: una rilettura del sistema che tenga conto delle peculiarità delle "nuove" prove di recente emersione, contemperando le tradizionali ricostruzioni degli istituti in tema di prova con i caratteri peculiari della fonte di prova in esame.

3. Computer forensics *e prova tecnico-scientifica*

Secondo un indirizzo dottrinale, la prova digitale rappresenterebbe «un sottotipo di recente emersione [della prova scientifica], a causa dell'alto grado di tecnicismo richiesto per trasformare le informazioni originariamente contenute in macchinari alquanto complessi in dati intellegibili da un giudice» [54].

In effetti, in quanto prova tecnica, fondata sull'applicazione, a fini forensi, della scienza informatica, appare in via di prima approssimazione corretto ricomprendere la *digital evidence* nel novero delle prove scientifiche [55]. Difatti,

---

[53] Cass., Sez. Un., 23 febbraio 2000, D'Amuri, in *Cass. pen.*, 2000, p. 2595 ss., con nota di G. Melillo, nonché *ivi*, 2000, p. 3245 ss., con nota di L. Filippi.

[54] In questa prospettiva, L. MARAFIOTI, Digital evidence *e processo penale*, cit., p. 4510. *Contra*, F.M. MOLINARI, *Le attività investigative inerenti alla prova di natura digitale*, cit., p. 1261. Secondo F. NOVARIO, *Le prove informatiche*, in P. FERRUA-E. MARZADURI-G. SPANGHER (a cura di), *La prova penale*, cit., p. 123, le prove informatiche sono riconducibili «alla categoria delle prove tecniche o scientifiche, quali prove derivate dall'impiego di tecnologie informatiche». Anche S. LORUSSO, *La prova scientifica*, in AA.VV., *Prova penale e metodo scientifico*, Utet, Torino, 2009, p. 26, ricomprende la *digital evidence* tra il catalogo di strumenti tecnico-scientifici utili alla ricerca di materiale cognitivo, portandola quale esempio di sapere scientifico impiegato ai fini dell'accertamento giurisdizionale.

[55] Secondo la dottrina più accreditata, è scientifica la prova che, «partendo da un fatto dimostrato, utilizza una legge scientifica per accertare l'esistenza di un ulteriore fatto da provare». Così P. TONINI, *La prova scientifica: considerazioni introduttive*, in *Dir. pen. proc.*, 2008, *Dossier prova scientifica*, p. 8. Per dirla con le parole della giurisprudenza di legittimità, la prova è scientifica «quando l'inferenza probatoria che è alla base dell'accertamento del fatto non può essere articolata sulla base delle conoscenze ordinarie, del sapere diffuso»; in tali casi, «il sapere scien-

l'intera attività che si svolge negli ambiti dell'informatica forense «esula dalle competenze dell'uomo medio»[56] ed implica necessariamente precise conoscenze tecniche ad elevata specializzazione.

Il tema dell'intreccio tra *scientific evidence* e *digital evidence* è, tuttavia, alquanto delicato e merita qualche precisazione in più.

Come noto, prova scientifica è espressione «ellittica», giacché «designa un complesso fenomeno, articolato e diversificato in molteplici forme di manifestazione»[57]. Parametrata sul dibattimento, la scientificità della prova è data dall'utilizzo di determinati strumenti conoscitivi nei momenti di ammissione, assunzione e valutazione della prova[58]. Mentre, con riferimento alla *digital evidence*, l'impiego di attrezzatura tecnica ad elevata specializzazione è essenziale già in un momento anteriore, vale a dire per l'identificazione del dato probatorio in fase investigativa e per la sua apprensione all'interno del procedimento, nonché, successivamente, per l'analisi del dato.

Con riferimento alla valenza euristica del metodo scientifico, l'utilizzo di strumentazione tecnica fin dalla fase di raccolta del dato non deve, però, far equivocare il valore probatorio della *digital evidence*, nel senso di una perfetta equivalenza tra prova digitale e prova perfetta. Come la dottrina occupatasi dell'argomento ha chiarito, non esiste, invero, alcun metodo scientifico che possa

---

tifico costituisce un indispensabile strumento al servizio del giudice di merito: si tratta di tentare di metabolizzare la complessità e di pervenire, così, ad una spiegazione degli accadimenti che risulti infine comprensibile per tutti, ostensibile». Così Cass., Sez IV, 17 settembre 2010, Cozzini, in *Dir. pen. proc.*, 2011, p. 1341 ss., con nota di P. Tonini, nonché in *Cass. pen.*, 2011, p. 1713 ss., con nota di R. Bartoli. Per gli sviluppi giurisprudenziali successivi alla sentenza Cozzini, cfr. D. VICOLI, *Riflessioni sulla prova scientifica: regole inferenziali, rapporti con il sapere comune, criteri di affidabilità*, in *Riv. it. med. leg.*, 2013, p. 1243.

[56] Così, correttamente, P. PERRI, *op. cit.*, p. 98.

[57] L'espressione è di O. DOMINIONI, *La prova penale scientifica*, Giuffrè, Milano, 2005, p. 12. In tema, v. anche ID., voce *Prova scientifica (diritto processuale penale)*, in *Enc. dir.*, Annali, II, Giuffrè, Milano, 2008, p. 977 ss.; ID., *L'esperienza italiana di impiego della prova scientifica nel processo penale*, in M. BERTOLINO-G. UBERTIS, *Prova scientifica, ragionamento probatorio e decisione giudiziale* (Atti del Convegno), Jovene, Napoli, 2015, p. 37 ss.; ID., *L'esperienza italiana di impiego della prova scientifica nel processo penale*, in *Dir. pen. proc.*, 2015, p. 601 ss.; P. GIARRETTA, *Alcune considerazioni generali sulla nozione di prova scientifica*, *ivi*, p. 85 ss.; F. GIUNTA, *Questioni scientifiche e prova scientifica tra categorie sostanziali e regole di giudizio*, *ivi*, p. 55 ss.; G. PANSINI, *Le prove deboli nel processo penale italiano*, Giappichelli, Torino, 2015, p. 103 ss.; S. RENZETTI, *La prova scientifica nel processo penale: problemi e prospettive*, in *Riv. dir. proc.*, 2015, p. 399 ss.; P.P. RIVELLO, *La prova scientifica*, Giuffrè, Milano, 2014, p. 57 ss.; ID., *Il processo e la scienza*, in *Riv. it. dir. proc. pen.*, 2010, p. 1715 ss.; G. SPANGHER, *Brevi riflessioni sparse in tema di prova tecnica*, in C. CONTI (a cura di), *Scienza e processo penale. Nuove frontiere e vecchi pregiudizi*, cit., p. 27; G. UBERTIS, *La prova scientifica e la nottola di Minerva*, in L. DE CATALDO NEUBURGER (a cura di). *La prova scientifica nel processo penale*, Cedam, Padova, 2007, p. 83 ss.

[58] Cfr., ancora, O. DOMINIONI, *La prova penale scientifica*, cit., p. 12.

portare ad approdi certi, potendosi al più ragionare in termini di alta probabilità delle conclusioni [59]. Il che appare tanto più vero con riguardo al tema che ci occupa, a causa dei già accennati peculiari caratteri propri del dato che custodisce l'informazione probatoria, e che lo rendono quanto mai sfuggente.

Segnatamente, il riferimento è al «peccato originale» [60] del dato digitale come fonte di prova. Anche qualora il dato sia, di per sé, prova dell'avvenuta integrazione della fattispecie criminosa – si pensi al già proposto esempio del *file* rinvenuto su un *hard disk* che raffigura materiale pornografico realizzato utilizzando minori – sarà alquanto difficile [61] l'ulteriore passaggio all'attribuzione del fatto al suo autore [62]; insomma, a voler seguire le tradizionali classificazioni probatorie, il dato digitale rischia di essere prova generica più spesso che prova specifica [63].

Più in generale, anche con riferimento alla *digital evidence* si ripropongono questioni già affrontate sul terreno del rapporto tra processo e *novel science*, con particolare riguardo alla collocazione della prova nell'ambito del sistema codicistico, nonché alla capacità dimostrativa della prova scientifica, all'attendibilità dell'esperto e al rischio di una sopravvalutazione del contributo cognitivo offerto da quest'ultimo.

Il parallellismo tra *scientific evidence* e *digital evidence* è approdo sicuro da cui iniziare la ricerca, giacché i criteri stabiliti con riferimento alla prima dalla giurisprudenza di legittimità sono in grado di fornire utili chiavi di lettura – sia pure con i doverosi adattamenti – anche avuto riguardo alla seconda.

Il riferimento è, soprattutto, alla valutazione, imposta al giudicante, circa l'autorità scientifica dell'esperto e circa la generale accettazione, nella comunità scientifica, degli enunciati proposti [64]. L'applicazione di tali canoni alla *digi-*

---

[59] Sul carattere congetturale di qualsiasi teoria scientifica, *ex multis*, cfr. S. LORUSSO, *La prova scientifica*, cit., p. 5 ss.

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

[61] Si può ipotizzare il caso in cui nei metadati di un *file* ne è indicato l'autore; ma anche in tal caso occorrerebbe verificare la veridicità di tale informazione.

[62] Cfr., sul punto, A. BARILI, *Accertamenti informatici*, in R. VALLI (a cura di), *Le indagini scientifiche nel procedimento penale*, Giuffrè, Milano, 2013, p. 598.

[63] V., per tutti, E. FLORIAN, *op. cit.*, p. 145, il quale identifica la prova generica in quella che «riguarda l'avvenimento del delitto nella sua consistenza obiettiva, nel suo effetto materiale»; prova specifica quella «rivolta a ricercare e individuare l'autore od i partecipi del delitto». Con specifico riguardo alla prova digitale, cfr. L. LUPARIA, Computer crimes *e procedimento penale*, in G. GARUTI (a cura di), *Modelli differenziati di accertamento*, in *Trattato di procedura penale*, diretto da G. Spangher, Utet, Torino, 2011, p. 375.

[64] Una traccia chiara di tali criteri si rinviene in Cass., Sez IV, 17 settembre 2010, Cozzini, cit. Per un'ipotesi recente relativa alla prova del *DNA*, v. Cass., 18 aprile 2013, Stasi, in *C.E.D. Cass.*, rv. 258321. Chiara l'influenza sui giudici di legittimità della giurisprudenza nordamericana e, in particolare, dei noti criteri dettati nella sentenza emessa dalla Corte Suprema degli Stati

tal evidence incontra un primo scoglio nella contingenza che la *computer forensics* è ambito scientifico di recente nascita [65]; non sempre vi è, dunque, concordia sulle modalità operative [66]. Cionondimeno, il criterio della necessità di una generale accettazione della comunità scientifica in relazione alle attività dell'esperto informatico fornisce qualche indicazione utile sulle modalità pratiche che l'attività del *computer forenser* deve seguire, con particolare riguardo al punto più delicato della stessa, vale a dire la scelta del *software* da utilizzare per le ricerche.

L'alternativa, a tal proposito, 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 secondi è possibile risalire al codice sorgente, sicché solo in quest'ultimo caso il funzionamento del *software* è assoggettabile a controllo: il che li rende di gran lunga preferibili.

Depone, altresì, a favore dell'utilizzo di *software open source* la possibilità di esaminare il formato dei *file* utilizzati, la facoltà per il tecnico di accludere l'intero programma ai risultati della propria attività, nonché la disponibilità del programma per lunghi periodi di tempo [67].

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: 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*. È immediatamente evidente che, in tale sistema, la nozione di accettazione generale non è pre-condizione necessaria e sufficiente. Infatti, il giudice assume il ruolo di *gatekeeper* della prova scientifica, dovendo valutare discrezionalmente l'affidabilità e dovendo controllare la validità dei *methods and procedures* che presiedono alla formazione della stessa; sarà il medesimo a dover garantire l'affidabilità dell'*expert witness* sul piano del fondamento scientifico, nonché sul piano dell'utilità ai fini della decisione della controversia. In dottrina, per un commento a tale pronuncia, v. M. TARUFFO, *Le prove scientifiche nella recente esperienza statunitense*, in *Riv. trim. dir. proc. civ.*, 1996, p. 219; per una recente applicazione dei principi in parola nel nostro ordinamento, v. Cass., Sez. I, 26 febbraio 2014, Busco, in *Dir. pen. proc.*, 2015, p. 415 ss., con nota di C. MANCINI, *Processo di via Poma: l'applicazione dei criteri Daubert rende la motivazione esente da vizi*.

[65] Cfr. M. MATTIUCCI, *Le indagini su reperti invisibili*. High Tech Crime, in D. CURTOTTI-L. SARAVO (a cura di), *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienze*, Giappichelli, Torino, 2013, p. 710.

[66] V. A.E. RICCI, Digital evidence*, sapere tecnico-scientifico e verità giudiziale*, cit., p. 348, la quale dà atto della molteplicità degli approcci operativi sul dato. Al fine di arginare il problema in parola, alcuni Stati si sono risolti ad adottare dei veri e propri manuali per le investigazioni digitali, contenenti regole e procedure da seguire una volta entrati in contatto con un dato digitale: è il caso, ad esempio, del manuale, edito dal Dipartimento di giustizia statunitense, intitolato *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. Ne riferisce P. PERRI, *op. cit.*, p. 96.

[67] Cfr. A. GRILLO-U.E. MOSCATO, *op. cit.*, p. 372 ss. Gli Autori sottolineano come solo il

Tuttavia, 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» [68]. 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.

Eppure, con riguardo all'attività dell'esperto, un'applicazione dei criteri teorizzati con riferimento alla prova scientifica anche alla *digital evidence* consiglierebbe un maggiore controllo sull'attività dell'esperto e, in ultimo, consentirebbe un più facile esercizio dei poteri valutativi in capo al giudice.

In diversificata prospettiva, sebbene l'applicazione di alcuni criteri teorizzati nell'ambito delle prove tecnico-scientifiche alla prova digitale sia auspicabile e foriera di esiti positivi a livello pratico, la riconducibilità della *digital evidence* nel novero di queste ultime non fornisce, cionondimeno, indicazioni precise, a livello teorico, quanto alla collocazione sistematica delle risultanze informatiche nel sistema processuale penale, con particolare riferimento alla loro tipicità o atipicità.

Anzi, l'inquadramento della *digital evidence* nel più ampio campo della prova scientifica rischia di ingenerare perniciosi equivoci, con particolare riguardo all'assimilabilità al regime previsto dall'art. 189 c.p.p., quale disposizione idonea a ricomprendere ogni ipotesi di nuova prova scientifica [69].

4. *L'inquadramento sistematico della prova informatica tra mezzi di prova tipici ed innominati*

Agli albori della *digital evidence*, se ne era sostenuta la riconducibilità *tout court* alla disciplina di cui all'art. 189 c.p.p. [70].

---

software open source risponda ai tradizionali criteri seguiti dalla giurisprudenza statunitense per l'ammissione della prova scientifica.

[68] La curiosa affermazione si rinviene in Cass., Sez. fer., 6 settembre 2012, Franchini, cit.

[69] V., a tal riguardo, P. MOSCARINI, *Lo statuto della "prova scientifica" nel processo penale*, in *Dir. pen. proc.*, 2015, p. 656. Critico sull'applicabilità dell'art. 189 c.p.p. è G. UBERTIS, *Il giudice, la scienza, la prova*, in *Cass. pen.*, 2011, p. 4111 ss. V. anche ID., *Prova scientifica e giustizia penale*, in *Riv. it. dir. proc. pen.*, 2016, p. 1192 ss.

[70] Cfr. P. GUALTIERI, *Prova informatica e diritto di difesa*, cit., p. 70. Una ipotesi di analisi forense ricondotta all'art. 189 c.p.p. si rinviene in G. NICOSIA-D.E. CACCAVELLA, *Indagini della difesa e alibi informatico: utilizzo di nuove metodiche investigative, problemi applicativi ed intro-*

L'equivoco appare frutto di quanto espressamente affermato nella Relazione al progetto preliminare del codice di procedura penale. Invero, la previsione di cui all'art. 189 c.p.p. sarebbe fondata proprio sulla necessità di rispondere alle sfide imposte dal «continuo sviluppo tecnologico che estende le frontiere dell'investigazione» [71]. Constatazione che, a prima vista, parrebbe attagliarsi perfettamente al tema in analisi.

In realtà, deve fin d'ora rilevarsi come la peculiarità della fonte di prova – vale a dire, la sua natura digitale – non fornisce elementi decisivi in ordine alla tipicità di quegli atti «mediante il quale l'oggetto di prova è rivelato e consegnato al processo» [72].

Inoltre, invocare oggi il contenitore della prova atipica quale *sedes materiae* della prova informatica appare, a seguito delle modifiche operate dalla L. n. 48/2008, anacronistico, giacché numerosi istituti, già presenti nel codice di rito, sono stati rimodellati al fine di essere adattati alle problematiche attinenti la fonte di prova digitale [73].

Più in generale, già anteriormente alla riforma si era dubitato che il contenitore della prova atipica fosse idoneo a ricomprendere ogni ipotesi di prova digitale e, più in generale, di *scientific evidence* [74]. Ciò, in primo luogo, sul presupposto che quest'ultima spesso non integra tanto una prova priva di disciplina espressa nella legge, quanto, piuttosto, una diversa forma di manifestazione di istituti codicistici già a lungo sperimentati [75]. Il che ha trovato conferma nella modifica volta a disegnare particolari modalità operative di acquisizione del dato allorché esso sia contenuto su supporti informatici [76].

---

duzione nel giudizio, in *Dir. internet*, 2007, p. 521. In generale, sull'istituto della prova atipica, *ex multis*, v. G.F. RICCI, *Le prove atipiche*, Giuffrè, Milano, 1999, *passim*.

[71] Così la *Relazione al progetto preliminare del codice di procedura penale*, citata in G. CONSO-V. GREVI-G. NEPPI MODONA, *Il nuovo codice di procedura penale. Dalla legge delega ai decreti delegati*. Vol IV, *Il progetto preliminare del 1988*, Cedam, Padova, 1990, p. 553.

[72] Si richiama, qui, la nota definizione di mezzi di prova offerta da E. FLORIAN, *op. cit.*, p. 137.

[73] Secondo E.M. MANCUSO, *L'acquisizione di contenuti* e-mail, in A. SCALFATI (a cura di), *Le indagini atipiche*, Giappichelli, Torino, 2014, p. 54, a convincere il legislatore sarebbe stato «l'iniziale adattamento degli istituti esistenti alle peculiarità mostrate dalla prova digitale, in sede applicativa».

[74] 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.

[75] In questo senso, proprio con riferimento alla prova digitale, v. L. MARAFIOTI, Digital evidence *e processo penale*, cit., p. 4511.

[76] In realtà, in tale ultima ipotesi, anche prima della L. n. 48/2008, quantomeno con riferimento alle ispezioni, perquisizioni e sequestri di materiale informatico, non si era in presenza di una atipicità probatoria come tradizionalmente intesa, nelle sue consuete accezioni di prova innominata (mezzo di prova del tutto nuovo o comunque non disciplinato dalla legge), prova irri-

In secondo luogo, si è rilevato che, al fine di consentire l'ingresso di strumenti tecnico-scientifici nel processo, risulterebbero sufficienti gli istituti della perizia e della consulenza tecnica, i quali – già da soli – sarebbero in grado di attrarre all'interno del proprio ambito operativo ogni forma di sapere tecnico impiegato ai fini processuali.

Con riguardo a tale ultimo profilo, deve rilevarsi che il discrimine tra prova atipica, per cui è richiesto uno specifico vaglio d'affidabilità, e gli strumenti deputati dal codice a consentire l'ingresso di tecniche scientifiche è stato individuato, dalla giurisprudenza di legittimità [77], nella novità ed autonomia delle leggi scientifiche applicate. Laddove queste ultime si fondino su legge di collaudata esperienza, proprie di altre scienze universalmente riconosciute, non è necessario che l'ammissione della prova sia preceduta dall'audizione delle parti e non deve essere scomodato il concetto di atipicità probatoria.

Applicando tali considerazioni al tema che ci occupa, seppure la *computer forensics* è scienza di recente formazione, essa si fonda su regole essenzialmente di tipo informatico e matematico [78]; regole proprie, dunque, di discipline universalmente riconosciute. Potrebbe, quindi, ritenersi che ogni ipotesi di risultanza digitale trovi viatico per l'ingresso nel materiale probatorio attraverso gli istituti della consulenza tecnica e della perizia.

Sarebbe, tuttavia, assai frettoloso concludere nel senso che l'art. 189 c.p.p. non conservi spazi applicativi con riferimento al dato digitale. Difatti, la già

---

tuale (ove si utilizza un mezzo di prova con modalità diverse da quelle previste) oppure prova anomala, vale a dire l'utilizzo di un mezzo di prova per ottenere il risultato di un altro, tipico mezzo di prova); ciò che cambiava era l'oggetto materiale dell'attività investigativa, vale a dire dati informatici. Il problema riguardava, allora, piuttosto, la capacità espansiva degli istituti già previsti con riguardo all'apprensione di dati digitali. Sull'atipicità probatoria, cfr., da ultimo, V. BOZIO, *La prova atipica*, in P. FERRUA-E. MARZADURI-G. SPANGHER (a cura di), *La prova penale*, cit., p. 62 ss., anche per i riferimenti bibliografici.

[77] Cfr., *ex multis*, Cass., Sez. I, 21 maggio 2008, Franzoni, in *Cass. pen.*, 2009, p. 1840 ss., con nota di F. Caprioli, relativa alla *Blood Pattern Analysis* (B.P.A.). In dottrina, sul tema della B.P.A., v. anche S. CAPITANI, *Il caso Cogne*, in C. CONTI (a cura di), *Processo mediatico e processo penale. Per un'analisi critica dei casi più discussi da Cogne a Garlasco*, Giuffrè, Milano, 2016, p. 25 ss.

[78] F. NOVARIO, *Le prove informatiche*, cit., pp. 122-123, evidenzia che «il fulcro dell'informatica è la tecnologia del calcolatore, che elabora informazioni espresse in numeri binari e può pertanto definirsi digitale. È composto da due elementi: il *software* e l'*hardware*. Quest'ultimo è l'anima meccanica che consente l'elaborazione dei dati, tramite il microprocessore, e la loro memorizzazione, tramite memorie volatili (*RAM*) e non volatili (*ROM* e *Hard disk*). L'*hardware* esegue istruzioni che gli vengono impartite tramite algoritmi, precise e univoche specificazioni di azioni eseguibili da un elaboratore. Il *software* è composto da combinazioni di algoritmi che consentono al calcolatore di giungere da un *input* determinato ad un *output* determinabile. I programmi informatici […] sono un testo, sequenza di caratteri alfanumerici, che conferisce algoritmi al processore del *computer*, consentendo agli utenti di fruire dei dati, anche attraverso reti di calcolatori: ad esempio *Internet*».

accennata peculiare natura del dato digitale comporta una innegabile difficoltà di tipizzazione e una scarsa compatibilità con uno schema probatorio rigido.

Sul punto, appare opportuna, in via preliminare, una considerazione. A prima vista, il congegno di cui all'art. 189 c.p.p. appare radicalmente incompatibile con lo svolgimento di una attività investigativa sul dato digitale che, per essere proficua, deve restare segreta: impossibile, infatti, instaurare il preventivo confronto tra le parti sull'ammissibilità della prova e sulle modalità di assunzione previsto dalla suddetta disposizione.

Eppure, la giurisprudenza ha ritenuto compreso nell'ampio contenitore di cui all'art. 189 c.p.p. qualsiasi strumento d'indagine che si discosti dal paradigma legale[79], qualunque sia la natura del dato da apprendere; dunque, anche quello informatico.

Pienamente legittimo, allora, in astratto, immaginare attività investigative su dati digitali da ricomprendere nel paradigma della prova atipica. Difatti, se è vero che, a seguito della L. n. 48/2008, gran parte delle verifiche sul dato digitale sono ora ricomprese all'interno delle tradizionali attività d'indagine, è altrettanto vero che lo sviluppo della scienza informatica fornisce l'occasione agli investigatori di coniare sempre nuove modalità di ricerca delle informazioni rilevanti.

Dal quadro sin qui delineato traspare una prima conseguenza: la natura digitale dell'informazione da apprendere al procedimento non appare, di per sé, tale da consentire una classificazione preventiva della fonte di prova. Il che impone di verificare, caso per caso, se lo strumento probatorio relativo al dato digitale utilizzato nel caso di specie sia estraneo o meno – e, se sì, sotto quale profilo: fonte di convincimento del tutto nuova, oppure diverse modalità operative di mezzo già noto – al catalogo legale; e ciò, soprattutto, con riferimento ai mezzi di ricerca della prova digitale.

Sotto diverso profilo, il problema relativo alla collocazione degli strumenti per reperire *digital evidence* tra i mezzi di ricerca tipici o innominati rischia, altresì, di essere foriero di equivoci. Il discorso classificatorio sulla *digital evidence* potrebbe, infatti, celare il vero nodo problematico delle nuove attività d'indagine sul dato informatico: vale a dire, il conflitto latente fra diritti fon-

---

[79] Cfr., *ex multis*. Cass., Sez. V, 27 febbraio 2002, Bresciani, in *Cass pen.*, 2002, p. 3049 ss., con nota di A. Laronga, con riguardo al monitoraggio tramite *GPS*. È interessante notare che tale pronuncia richiama l'art. 266-*bis* c.p.p. come esempio di adeguamento del codice di rito ai nuovi ritrovati della tecnica che il legislatore potrebbe, in futuro, seguire anche con riferimento alla localizzazione a distanza. Il richiamo serve, nell'economia del *dictum*, a differenziare quegli strumenti per cui il legislatore ha previsto un'assimilazione alle intercettazioni di cui all'art. 266 c.p.p. quanto a presupposti e modalità, quale appunto le intercettazioni telematiche, e i mezzi atipici di ricerca della prova, quali il monitoraggio *GPS*, per i quali non è richiesto decreto motivato dell'autorità giudiziaria.

damentali e accertamento investigativo, nonché, più in generale, fra tutela dell'individuo e ricerca della verità. Problema che, mutuato sul terreno della *digital evidence*, attiene in buona sostanza a come conciliare duttilità dei modi e delle tecniche di apprensione richiesti dalla natura del dato e individuazione del percorso legale formalizzato.

In quest'ottica, il richiamo all'art. 189 c.p.p. non può certo elidere il doveroso controllo circa la rispondenza dello strumento investigativo utilizzato con i diritti della persona; anzi, proprio il riferimento alla libertà morale della persona contenuto nella summenzionata disposizione deve orientare il giudice al fine della scelta tra ammissione o meno delle risultanze.

Di più. L'incidenza sui diritti fondamentali degli strumenti di ricerca della prova digitale, soprattutto con riguardo alla *online search* sul *personal computer* [80], richiama esigenze di legalità – compromissione nei soli casi e modi previsti dalla legge – poco compatibili con la prova atipica, ove lo schema acquisitivo è, per definizione, sottratto alle disposizioni normative e rimesso al confronto delle parti ed alla decisione del giudice.

Eppure, non sempre la giurisprudenza ha mostrato di comprendere l'invasività nella sfera personale di alcuni nuovi strumenti di indagine. Appare, invero, che i giudici di legittimità tengano in maggior conto il principio di non dispersione della prova [81] piuttosto che la tutela di un rapporto, quello tra individuo e attrezzatura informatica, che coinvolge e necessariamente implica diritti inviolabili quali la libertà personale, la libertà di domicilio, anche nella sua particolare accezione di domicilio informatico, nonché la libertà e la segretezza della corrispondenza. E tracce lampanti di quanto appena rilevato si rinvengono in quell'orientamento giurisprudenziale che ha identificato nell'utilizzo di *malware* a fini investigativi un mezzo di ricerca atipico della prova digitale [82].

L'utilizzo di *virus* informatici per finalità di accertamento appare fenomeno degno di attenzione anche perché ulteriore testimonianza delle difficoltà classificatorie dei mezzi di ricerca della prova digitale. Ed invero, agli albori dell'impiego di un *malware* da parte della pubblica accusa, era affermazione ricorrente nell'ambito di diversi uffici del Pubblico ministero quella secondo cui l'ingresso dei *file* recuperati dal programma nell'ambito del procedimento sarebbe dovuto avvenire mediante l'istituto della prova documentale ai sensi dell'art. 234 c.p.p. [83]; il che porta a indirizzare la ricerca proprio verso tale istituto.

---

[80] Sul punto, v. *infra*, cap. II, § 5.

[81] Cfr. P. GUALTIERI, *Prova informatica e diritto di difesa*, cit., p. 70.

[82] Cass., Sez. V, 14 ottobre 2009, Virruso, in *C.E.D. Cass.*, rv. 246954.

[83] Cfr. Cass., Sez. V, 14 ottobre 2009, Virruso, cit.