

LA PROVA INFORMATICA AL VAGLIO DEL
GIUDICE, TRA CATTIVA SCIENZA E CATTIVI
SCIENZIATI *

Alessandra Sanna **



THE DIGITAL EVIDENCE UNDER THE SCRUTINY OF THE JUDGE,
BETWEEN BAD SCIENCE AND BAD SCIENTISTS

The massive use of digital evidence in modern criminal proceedings carries two types of risks. The first concerns the protection of individual rights to the extent required by the Constitution. Procedural rules designed to govern traditional evidence are ineffective against the intrusive ability of digital evidence on the sphere of privacy. The second type of risk concerns the reliability of the evidence and the protection of the defensive guarantees. The genuineness of the digital evidence is compromised if investigators do not observe the best practices. On the other hand, the defense attorney is not allowed to intervene when evidence is collected. The remedy against these risks is the role of gatekeeper exercised by the judge against the bad science and the bad scientists.

KEYWORDS Digital evidence – Privacy – Defensive guarantees

SOMMARIO 1. Premessa: la pervasività della prova digitale. – 2. Pericoli e strategie di contenimento: a) il *vulnus* ai diritti individuali. – 3. b) l'inattendibilità della conoscenza e gli ostacoli al diritto di difesa.

1. Premessa: la pervasività della prova digitale

Nella sistematica, oramai precaria, del codice di rito il termine prova rimanda al dibattimento, sede privilegiata per la formazione delle conoscenze idonee a fondare la decisione nel merito.

Così il tema della prova informatica si lega indissolubilmente alle modalità di ingresso, acquisizione e valutazione in giudizio del dato digitale.

La natura digitale è, infatti, il tratto distintivo della categoria probatoria in discorso, specie del *genus* prova scientifica, caratterizzata da contenuti espressi, non già

* È il testo, corredato da note bibliografiche, dell'intervento svolto in data 18 marzo 2022, nell'ambito del Corso di perfezionamento *post-lauream* «Internet tra diritto penale e processo», organizzato dal Dipartimento di Scienze giuridiche dell'Università di Firenze

** Professore associato di diritto processuale penale nell'Università di Firenze

in forma analogica, ovvero tramite grandezze fisiche poste in progressione continua, ma attraverso sequenze numeriche binarie, i bit, trasfigurate in segnali elettronici¹.

Un modo diverso di rappresentare la realtà divenuto gradualmente pervasivo e forse dominante grazie all'evoluzione tumultuosa dell'informatica e dell'avvento di Internet. Gran parte delle nostre vite si svolge oramai nell'universo parallelo del cyberspazio: tramite l'accesso compulsivo ai nostri *device* mobili, rapporti di lavoro e sociali, informazione, istruzione, acquisti transitano nel *web* sotto forma di segnali digitali e lì disseminano tracce digitali, in una misura che probabilmente sfugge alla nostra consapevolezza. Si dice che le società di *Big data*, attraverso la manipolazione algoritmica dei nostri dati conoscano meglio di noi stessi le nostre opinioni, attitudini, personalità². Allo stesso modo gli inseparabili *smartphones*, propaggine elettronica dell'*homo technologicus*, sono depositari delle nostre vite³.

Ovvio che il fenomeno dovesse ripercuotersi sul terreno del processo penale, di per sé specchio della società. Il trasloco di parte consistente dell'esistenza umana nei gangli dei circuiti informatici e nell'universo *web* determina l'incremento esponenziale delle situazioni in cui le tracce digitali assumono rilevanza ai fini del processo.

Le prove informatiche non sono solo utili per la repressione dei reati informatici, cioè i reati commessi contro o attraverso un sistema informatico, ma forniscono conoscenze determinanti ai fini dell'accertamento di qualunque reato e possiedono, quindi, un ambito potenzialmente illimitato⁴. La prova dell'illecito finisce sempre più per

¹ I dati informatici consistono in “*zeroes and ones of electricity*”, senza possibilità di discriminare valori intermedi tra le due cifre consecutive: v. S. ATERNO, *Acquisizione e analisi della prova informatica*, in *Dir. pen. proc.*, 2008, n. 6, *Dossier, La prova scientifica nel processo penale*, p. 61.

² Le c.d. identità digitali costituiscono merce preziosa, analizzate attraverso algoritmi servono a prevedere e persino ad indirizzare i comportamenti a fini di *marketing* o a scopi elettorali. Non stupisce quindi che esse siano preda di apprensione occulta e sistematica ad opera dei colossi digitali: per una più estesa riflessione al riguardo, cfr., volendo, A. SANNA, *L'irriducibile atipicità delle intercettazioni tramite virus informatico*, in *Le indagini atipiche*, a cura di A. SCALFATI, Seconda edizione, 2019, p. 602.

³ Si osserva come l'insieme di informazioni affidate a nostri *smartphones* finisce per comporre «una dimensione che spesso teniamo nascosta persino alle persone più care»: così A. CAPONE, *Intercettazioni e Costituzione, problemi vecchi e nuovi*, in *Cass. pen.*, 2017, p. 1263.

⁴ Lo si desume dall'art. 4 § 2 c della Convenzione di Budapest, che invita gli Stati contraenti ad apprestare un'apposita disciplina finalizzata a “*la collecte des preuves électroniques de toute infractions pénales*”: così M. DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, p. 283. Sulla progressiva espansione delle indagini informatiche in ogni ambito dell'accertamento penale, dai *computer crimes*, agli illeciti commessi soltanto occasionalmente con lo strumento informatico (c.d. *old wine in new bottles*), fino ai reati comuni: L. LUPÁRIA, *Processo penale e tecnologia informatica*, in *Dir. internet*, 2008, n. 3, p. 221.

annidarsi nel *computer* o in un *server* altrove dislocato, mentre l'uso della prova digitale può giovare non solo in prospettiva accusatoria, ma pure in chiave difensiva⁵.

2. Pericoli e strategie di contenimento: a) il *vulnus* ai diritti individuali

L'irrompere massiccio della prova digitale nelle aule di giustizia comporta due principali ordini di rischi. Il primo riguarda la tutela dei diritti individuali nella misura richiesta dalla Costituzione.

Tra le tradizionali forme di comunicazione a distanza e quelle informatiche odierne vi è un macroscopico divario: le prime, ancorate a luogo e tempo definiti, sono destinate a rivestire una valenza residuale nella sfera dei rapporti intersoggettivi, le seconde, svincolate da limiti spazio-temporali, possiedono un'incontenibile forza espansiva, sì da divenire assorbenti nel perimetro delle relazioni umane.

La metamorfosi si riflette sul piano giuridico: in particolare la sfera delle prerogative tutelate dall'art. 15 Cost. compie un salto qualitativo⁶. Svincolato dalla dimensione fisica l'esercizio del diritto di comunicazione diviene sempre più centrale e partecipe del nucleo incompressibile della dignità umana, così da esigere uno speculare incremento delle garanzie poste a salvaguardarne libertà e riservatezza. È la "tutela progressiva" dei diritti⁷, a cui legislatore è chiamato non solo davanti all'affacciarsi di nuovi diritti di libertà, ma pure qualora l'inedito atteggiarsi di quelli conosciuti comprometta l'efficacia delle tutele esistenti.

L'affanno del legislatore processuale qui è tangibile: c'è qualcosa che stona nell'equivalenza codicistica tra intercettazioni tra presenti, compiute tramite la tradizionale microspia e le captazioni fornite dal temibile *trojan virus* (art. 266 comma 2 c.p.p.)⁸. Il fattore di crisi è dato dalla natura mobile del dispositivo bersaglio: l'attivazione da remoto del microfono di uno *smartphone* trasforma l'apparecchio in una

⁵ Si pensi all'ipotesi di un alibi "informatico" rappresentato, ad esempio, dall'invio di una e-mail all'ora del fatto contestato ma da un luogo diverso rispetto a quello di commissione del reato: cfr. sul punto, L. MARAFIOTI, *Digital evidence e processo penale*, in *Cass. pen.*, 2011, p. 4509.

⁶ Muta la «proiezione spirituale» dell'individuo che tradizionalmente delimita e dà corpo alla tutela fornita dall'art. 15 Cost.: v. F. CAPRIOLI, *Colloqui riservati e prova penale*, Torino, Giappichelli, 2000, p. 56.

⁷ L'espressione è di R. ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. proc. pen.*, 2014, pp. 1133 ss.

⁸ Più in generale non convince l'artificiosa partizione legislativa intesa a ricondurre ciascuna delle poliedriche attività consentite dal *malware* sotto l'egida del mezzo probatorio affine: cfr., fra gli altri, A. CAMON, *Cavalli di Troja in Cassazione*, in *Arch. nuova proc. pen.*, 2017, p. 94; E.M. MANCUSO, *L'acquisizione di contenuti e-mail*, in *Le indagini atipiche*, cit., p. 502.

microspia capace di ascoltare ogni “sospiro” del soggetto sotto controllo. Vi è un inevitabile eccesso di ingerenza quando l’apprensione sonora finisce per sfuggire a limiti spazio-temporali e accompagna ogni momento della vita della persona sottoposta a controllo. Saltano le categorie di riferimento: qualora l’attività di captazione segua tutti gli spostamenti del possessore del dispositivo, diventa privo di significato discorrere, come fa l’articolo 266 comma 2, c.p.p. di una determinata categoria di soggetti “presenti”. La cimice informatica estende il proprio raggio d’azione ad una folla indeterminata e indeterminabile di persone, spesso estranei ai fatti oggetto di indagine, “che in qualunque luogo conversano, non necessariamente col possessore del cellulare”⁹.

Il nodo si ripropone con riguardo alla captazione tramite *trojan* delle comunicazioni digitali in transito racchiuse in e-mail o scambiate tramite una comune applicazione di messaggistica (*WhatsApp* o affini): qui secondo la chiave di lettura prevalente l’attività di indagine si risolverebbe in una tecnica intercettativa, rientrando come tale nell’ambito della disciplina *ex artt.* 266 e ss. c.p.p.¹⁰

Ma il ragionamento non suona persuasivo perché è basato, in definitiva, sulla convinzione che l’efficacia delle tutele normative, ossia la loro capacità di fornire un bilanciamento accettabile degli interessi in gioco, si misuri a prescindere dal grado di sacrificio imposto al diritto considerato. Non è così: più cresce il tasso di aggressività dell’intervento statale sulla sfera dell’individuo tanto più occorre limitarne l’esercizio¹¹. Un conto è sottoporre a controllo un’utenza telefonica fissa, altro è inoculare il *trojan virus* all’interno di uno *smartphone*. Qualora l’illimitata forza pervasiva del *virus* informatico si eserciti sull’intera sfera delle comunicazioni *web*, si produce un effetto annichilente sul diritto tutelato dall’art. 15 Cost., cui invano si pretende di fare schermo con gli articoli 266 e ss. c.p.p., concepiti in un’era tecnologica ormai remota e, quindi, minati da sopraggiunta obsolescenza¹².

⁹ A. CAPONE, *op cit.*, p. 1263.

¹⁰ E, in particolare, qualora abbia ad oggetto dati dinamici comunicativi, nell’area dell’art. 266-*bis* c.p.p.: così R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma*, in *Riv. it. dir. proc. pen.* 2018, p. 538. Si ragiona sul presupposto che la bontà dell’assetto codicistico prescinda dal tipo di tecnologia di volta in volta impiegata: G. LASAGNI, *L’uso di captatori informatici (trojans) nelle intercettazioni tra presenti*, in *Dir. pen. cont.*, ed. *on-line* del 7 ottobre 2017, p. 11.

¹¹ Ad incrinarsi è *in primis* la linea di equilibrio tracciata dal codice tra le esigenze di investigazione e la salvaguardia del diritto coperto dall’art. 15 Cost.: a fronte dell’elevata carica lesiva del mezzo d’indagine, la previsione dei casi, ossia l’area delle captazioni occulte, e dei presupposti che ne legittimano l’impiego non appare rispettosa del principio di proporzionalità: per un approfondimento sul punto cfr., volendo, A. SANNA, *L’irriducibile atipicità delle intercettazioni tramite virus informatico*, cit., pp. 605 ss.

¹² Ritengono che l’assetto complessivo della disciplina sulle intercettazioni “vecchio stile” risulti inadeguato a regolare il nuovo strumento d’indagine: F. CAPRIOLI, *Il captatore informatico come*

La questione classificatoria si ripropone con maggior forza rispetto all'acquisizione occulta tramite attività da remoto di dati statici conservati nei sistemi informatici. Simili attività non sono inquadrabili nello schema tipico della perquisizione: né in quello della perquisizione "ordinaria" (*ex artt. 247-252 c.p.p.*), né in quello della perquisizione "informatica" (*ex art. 247 comma 1-bis c.p.p.*) per il loro essere, appunto, occulte, ovvero svolte all'insaputa della persona che ha la disponibilità dell'oggetto da perquisire, destinate a protrarsi nel tempo, nonché funzionali all'acquisizione indiscriminata di dati (notizie di reato comprese) anziché alla ricerca selettiva di prove in ordine a un addebito preesistente¹³.

Fallito, dunque, il tentativo di ricondurre le attività di ricerca descritte sotto l'egida del mezzo probatorio affine disciplinato dal codice¹⁴, i diritti fondamentali coinvolti restano senza presidio. Ne deriva una breccia nel dettato costituzionale e sovraordinato, a cui la giurisprudenza vorrebbe porre rimedio attraverso il ricorso al meccanismo preordinato all'ingresso in giudizio della prova atipica *ex art. 189 c.p.p.* Così il reperto digitale scovato nel computer tramite il *trojan* inoculato nell'apparecchio è pacificamente ammissibile: benché sfuggente alla sequenza perquisizione-sequestro informatico, sarebbe classificabile come "mezzo di ricerca della prova atipico"¹⁵.

La ricostruzione sconta un vizio di fondo: l'operatività dell'art. 189 c.p.p. implica in capo al giudice un potere istruttorio, ovvero di ammissione della prova, che sarà poi assunta secondo modalità che, nel silenzio della legge, saranno determinate con l'ausilio delle parti¹⁶.

strumento di ricerca della prova in Italia, in *Rev. bras. dir. proc. pen.*, 2017, p. 494 e L. PARLATO, *Problemi irrisolti: le perquisizioni on line*, in *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di G. GIOSTRA - R. ORLANDI, Giapichelli, Torino, 2018, p. 308.

¹³ Emerge qui l'originario *imprinting* del *malware*, nato come strumento in uso alle attività di *intelligence* e, perciò, impiegato in chiave di prevenzione del crimine. Si constata, peraltro – e l'asserto non può che inquietare – come la capacità di prevenzione risulti più efficace, non già con la raccolta mirata, quanto piuttosto con l'acquisizione indiscriminata e automatica di dati, strumentale alla loro analisi tramite elaboratori dalla grande potenza di calcolo: così R. BRIGHI, *Funzionamento e potenzialità investigative del malware*, in *Nuove norme in tema di intercettazioni. Tutela della riservatezza*, cit., pp. 211-212.

¹⁴ V., sul punto, E.M. MANCUSO, *L'acquisizione di contenuti e-mail*, in *Le indagini atipiche*, cit., pp. 523 ss.

¹⁵ L'indirizzo è inaugurato da Cass., Sez. V, 14 ottobre 2009, n. 16556, Virruso, in *CED*, n. 246954, con riferimento alle attività di *on-line search*, inclusive di prelievo e copia di documenti memorizzati nell'*hard disk* di un computer. Nel medesimo solco, più di recente: Cass., Sez. V, 30 maggio 2017, Occhionero, in *Giur. it.*, 2017, p. 2498.

¹⁶ Merita, peraltro, interrogarsi sulla compatibilità tra il meccanismo del contraddittorio *ex ante*, dettato dall'art.189 c.p.p. in riferimento alla sede dibattimentale, e la fase investigativa, in seno al quale

Ma qualora la prova incida sui diritti definiti inviolabili dalla Costituzione (artt. 13, 14 e 15 Cost.) ovvero sul diritto alla riservatezza nel significato accolto dall'art. 8 CEDU, in assenza di un intervento legislativo che determini in quali casi, con quali modi e con quali garanzie i diritti di cui si tratta possono essere violati, manca alla radice un atto di investitura del potere istruttorio in capo al giudice. Sicché, come hanno sottolineato le Sezioni unite nella sentenza Prisco, l'art. 189 c.p.p. «presuppone logicamente la formazione lecita della prova, e soltanto in questo caso la rende ammissibile»¹⁷. E nel medesimo solco si sono poste le Sezioni unite Scurato¹⁸: dinanzi all'impossibilità, nel silenzio della legge, di circoscrivere il raggio di azione del *trojan virus* entro confini compatibili con gli artt. 14 e 15 Cost. si configurava un divieto d'uso del mezzo di indagine destinato a coprire l'intera area dei procedimenti ordinari¹⁹. E poiché il legislatore è in seguito intervenuto solo per disciplinare un circoscritto uso del *trojan*, quelli residui, tuttora sottratti alla previsione di legge, sono da ritenersi inammissibili. Tale almeno il corollario in un sistema governato dal canone di stretta legalità.

Non mancano, quindi, gli strumenti normativi capaci di sorreggere il giudice nel prezioso ruolo di *gatekeeper* dei valori del processo rispetto alla “cattiva scienza” informatica²⁰, da intendersi anche nel significato di scienza che, svincolata dal canone della legalità, finisce per travolgere i diritti fondamentali delle persone coinvolte.

L'importanza del ruolo è viceversa trascurata o malamente intesa nella prassi, in omaggio alla bulimia investigativa intrinseca alla natura dei mezzi di ricerca informatici, che si rivela assai duttile alle attività delle agenzie di *intelligence*, ma incompatibile con il rigore delle forme processuali.

manca fisiologicamente la possibilità di un confronto dialettico sulle modalità di acquisizione probatoria: cfr. sul punto: E.M. MANCUSO, *Le perquisizioni on-line*, in *JusOnline*, 2017, n. 3, p. 428.

¹⁷ Cass., Sez. un., 28 marzo 2006, Prisco, in *Dir. pen. proc.*, 2006, p. 1349, in materia di ammissibilità dei risultati di video-riprese svolte all'interno dei c.d. *privés* di una discoteca.

¹⁸ Cfr. Cass., Sez. un., 28 aprile 2016, Scurato, in *Cass. pen.*, 2016, p. 3536, in cui la Corte negò l'ammissibilità delle intercettazioni c.d. ambientali svolte tramite *trojan virus*, all'epoca prive di apposita disciplina. Interpreta la pronuncia *de qua* come espressione del divieto di mezzi probatori atipici limitativi di diritti fondamentali: M. TROGU, *Intrusioni segrete nel domicilio informatico*, in *Le indagini atipiche*, cit. p. 582.

¹⁹ Dinanzi al rischio di incidere sui diritti fondamentali al di fuori dei confini tracciati dalla legge, la Corte “bandisce dal processo gli strumenti investigativi le cui potenzialità intrusive non siano determinabili a priori”: così F. CAPRIOLI, *Il “captatore informatico” come strumento di ricerca della prova in Italia*, cit., p. 501.

²⁰ Cfr. F. CAPRIOLI, *La scienza “cattiva maestra”: le insidie della prova scientifica nel processo penale*, in *Cass. pen.*, 2008, p. 3525, il quale impiega la formula per alludere all'impiego nel processo di “strumenti tecnico-scientifici che non garantiscono in sé e per sé, a prescindere dall'applicazione che se ne faccia nel caso concreto, un margine sufficiente di affidabilità e attendibilità”.

3. b) l'inattendibilità della conoscenza e gli ostacoli al diritto di difesa

Il secondo ordine di rischi che solleva il protagonismo della prova digitale sulla scena del processo riguarda i profili dell'attendibilità dei risultati conoscitivi e della tutela delle garanzie difensive.

La prova informatica si forma perlopiù nella fase delle indagini: qui si svolgono le apprensioni da remoto tramite *virus* e la sequenza ispezione-perquisizione-sequestro informatici, al cui interno trova spazio l'accertamento tecnico inteso a formare la copia clone²¹. Dati e documenti così raccolti, una volta ammessi al dibattimento, saranno sottoposti al contraddittorio c.d. argomentativo sui risultati dell'attività di indagine già svolta, che dovrà auspicabilmente avvalersi dell'apporto di periti e consulenti tecnici²².

Si osservi per inciso, che se il momento genetico della prova informatica si colloca fuori dall'alveo dibattimentale, l'incremento statistico del suo uso processuale coopera nel determinare la perdita di centralità del dibattimento nonché la crisi dell'assetto del sistema processuale tendenzialmente accusatorio voluto dal codice del 1988. La prova narrativa diventa sempre più residuale e con essa sfuma l'importanza del valore poetico del contraddittorio.

Per altro verso, la formazione della prova in fase d'indagine e la sottrazione al contraddittorio pieno che ne deriva si risolvono in gravi controindicazioni in punto di attendibilità dell'elemento conoscitivo e di tutela delle garanzie difensive. Tanto più che la intrinseca volatilità, modificabilità e alterabilità del dato digitale impongono la rigorosa osservanza delle migliori pratiche elaborate dalla comunità scientifica e l'aderenza alle regole dettate dal legislatore in attuazione della Convenzione di Budapest (l. 18 marzo 2008 n. 48).

Occorre infatti fare i conti con le caratteristiche della prova digitale: dematerializzazione del supporto, fragilità del dato²³, imputabilità ad un determinato autore, rapporti originale/copia clone.

²¹ Ben evidenzia il peculiare atteggiarsi di ispezione e perquisizione aventi ad oggetto dati informatici: P. FELICIONI, *Le ispezioni e perquisizioni di dati e sistemi*, in AA.VV., *Cybercrime. Diritto e procedura penale dell'informatica*, Milano, 2019, pp. 1377 ss.

²² Il contraddittorio postumo, inteso a sondare l'idoneità del *modus operandi* degli investigatori, assume una valenza imprescindibile al fine di sopperire al *gap* conoscitivo del giudice rispetto ai soggetti "esperti": L. MARAFIOTI, *Digital evidence e processo penale*, cit., p. 4512.

²³ Cfr., fra gli altri, L. LUPÁRIA, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa: i profili processuali*, in *Dir. pen. proc.*, 2008, p. 719 e P. TONINI, *Documento informatico e giusto processo*, ivi, 2009, p. 404.

Se ciascuno di questi tratti distintivi pone altrettante questioni sul piano processuale²⁴, le maggiori implicazioni in punto di uso e valutazione del dato informatico discendono dalle modalità seguite per l'apprensione dell'elemento di prova e l'incorporamento in un supporto materiale.

L'operazione comunemente eseguita dagli investigatori, di regola funzionari di polizia giudiziaria, è la copiatura mediante *bit-stream image* (procedura che consente un duplicato esatto dell'*hard disk* originario)²⁵, alla quale allude l'art. 354, comma 2, c.p.p. allorché menziona la "duplicazione su adeguati supporti" mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità. Sono le *best practices* in materia a suggerire di formare secondo queste modalità una "copia-clone" del contenuto del *computer*, sulla quale poter poi compiere le necessarie elaborazioni ed analisi, senza il rischio di alterare la prima "fotografia" del contenuto digitale.

Ne deriva che le attività di ricerca probatoria in un contesto informatico servono di regola ad assicurare al processo veri e propri documenti. Benché il documento digitale possieda caratteristiche esclusive, ovvero la scorporabilità del contenuto dal supporto su cui è stato *ab origine* registrato, (senza che ciò comporti la perdita delle proprie caratteristiche), esso è pur sempre una prova documentale, dove la *res* è costituita dal supporto magnetico, mentre i bit (o segnali digitali) ivi incorporati rappresentano fatti, cose o persone, come recita l'art. 234 c.p.p.²⁶

Il documento digitale è, peraltro, uno strumento conoscitivo particolarmente insidioso. Sono elevatissimi i rischi che le prove digitali siano contraffatte o manipolate, volontariamente oppure a causa dell'impiego delle tecniche sbagliate. È perciò indispensabile proteggere quella che gli studiosi anglosassoni definiscono la «catena di custodia»

²⁴ Così dall'immaterialità discende l'alta probabilità che le prove digitali di un reato si trovino dislocate in luoghi tra loro distanti, racchiuse in *server* o computer situati in sedi remote. Di qui la necessità di individuare la competenza degli organi inquirenti in modo da evitare la sovrapposizione di più procedimenti aventi il medesimo oggetto. E la questione si pone anche con riferimento ai rapporti con le autorità straniere, sui quali la l. 18 marzo 2008 n. 48 attuativa della Convenzione di Budapest ha mancato di intervenire: lo evidenzia M. DANIELE, *La prova digitale nel processo penale*, cit., p. 285. Alle lacune tenterà di rimediare il secondo Protocollo addizionale alla Convenzione di Budapest, in corso di elaborazione: il testo circolante punta, in specie, ad incrementare le procedure di cooperazione rafforzata tra le autorità degli Stati: cfr., in argomento, S. TOGNAZZI, *Criminalità informatica e cooperazione internazionale: verso il secondo Protocollo addizionale alla Convenzione di Budapest*, in *Dir. pen. proc.*, 2021, pp. 1031 ss.

²⁵ La *bit stream* o *mirror image* del disco fisso è un esatto duplicato non solo dei file, ma di ogni bit del disco fisso: cfr. P. FELICIONI, *Le ispezioni e perquisizioni di dati e sistemi*, cit., p. 1419.

²⁶ Per simile inquadramento, v. F. ZACCHÈ, *La prova documentale*, in *Trattato di procedura penale*, vol. XIX, diretto da G. UBERTIS e G.P. VOENA, Milano, 2012, p. 34.

(*chain of custody*): le prove digitali devono rimanere integre in tutti i loro passaggi dal sistema informatico di origine alla disponibilità da parte del giudice del dibattimento²⁷.

Occorre quindi porre in campo strategie contro le distorsioni indotte nel sistema dall'uso non appropriato della scienza (c.d. profilassi cognitiva): qui il ruolo di *gatekeeper* del giudice deve rivolgersi non già contro la cattiva scienza, ma contro i “cattivi scienziati”²⁸. In gioco è l'attendibilità dell'accertamento, la vanificazione della pretesa punitiva come pure la perdita di prove a difesa decisive per la sorte dell'imputato.

Ma quali sono le strategie capaci di contrastare simili esiti?

Il rimedio ideale per garantire l'autenticità dello strumento informatico sarebbe che il legislatore potesse prestabilire una specifica tecnica di acquisizione dalle prove digitali, da osservare a pena di inammissibilità e/o inutilizzabilità del risultato. Questa strada non è però percorribile: allo stato dell'arte non esiste un metodo di raccolta delle prove digitali in grado di imporsi su tutti gli altri, così la scelta della tecnica da impiegare dipende dalla situazione che si presenta in concreto agli investigatori. Una normativa che ancorasse ad un metodo specifico, storicamente determinato, l'operato degli investigatori fisserebbe regole destinate ad essere inevitabilmente superate da una repentina evoluzione scientifico-tecnologica.

Di qui l'impostazione accolta dalla l. n. 48 del 2008, dove non si prescrive una metodologia legale di raccolta delle prove digitali, ma ci si limita a fissare gli obiettivi che gli organi inquirenti devono perseguire, attraverso l'impiego dei protocolli scientifici accreditati sul piano internazionale²⁹.

L'opzione, se da un lato implica l'intervento degli esperti in tutte le fasi nell'*iter* probatorio, dall'altro determina l'assenza di sanzioni processuali qualora la raccolta e l'analisi del dato digitale si discosti dalle migliori pratiche o, in altri termini, quando

²⁷ Il rispetto della catena di custodia consente, da un lato di evidenziare (*chain of custody process*), dall'altro di documentare i passaggi indispensabili all'autenticazione dell'elemento di prova (*chain of custody document*): per la duplice finalità della metodologia cfr. A. CHELO, *Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria*, Padova, 2014, p. 21.

²⁸ Occorre, in altri termini, valutare se il perito o il consulente o, in generale, l'incaricato di svolgere l'accertamento tecnico “abbia fatto un uso corretto della sua scienza (in sé buona)”: F. CAPRIOLI, *La scienza “cattiva maestra”: le insidie della prova scientifica nel processo penale*, cit., p. 3530.

²⁹ Così gli artt. 244, comma 2, 247 comma 1-*bis*, 254 comma 2, 259 comma 2, 352 comma 1-*bis* e 354 comma 2 c.p.p. richiedono l'uso di “misure tecniche” capaci di “assicurare la conservazione” e di “impedire l'alterazione dei dati originali”. Si osserva, peraltro, come manchi nella prassi la condivisione di *standard* e metodologie, sostituita dal fiorire di protocolli operativi differenti, elaborati in autonomia da ciascun organismo inquirente (carabinieri, polizia di stato, guardia di finanza) e perfino all'interno dello stesso corpo di polizia in ragione della sede territoriale: L. LUPÁRIA, *La disciplina processuale e le garanzie difensive*, in *Investigazione penale e tecnologia informatica*, a cura di L. LUPÁRIA-G. ZICCARDI, Milano, 2007, pp. 192-193.

l'esperto si atteggi a cattivo scienziato³⁰. Dinanzi al principio di tassatività delle invalidità non sono configurabili né regole di esclusione, che impedirebbero l'ammissione della prova³¹, né di inutilizzabilità dirette ad inibire l'uso della prova mal formata³².

Un'altra strategia rivolta a preservare l'autenticità della prova consisterebbe nel garantire il contraddittorio tecnico, con coinvolgimento di difensore e consulenti, in fase di assunzione del dato digitale. Qui la soluzione si scontra con il granitico indirizzo della giurisprudenza, stando alla quale 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 stabilite dall'art. 360 c.p.p. per gli accertamenti non ripetibili, ovvero il preavviso alla difesa in ordine al compimento delle operazioni, la possibilità di parteciparvi con un consulente tecnico e il diritto all'instaurazione dell'incidente probatorio³³.

Questa posizione, nella sua intransigenza, non è condivisibile: è ormai consapevolezza comune che le procedure di copia delle prove informatiche, anche quando non riguardano un oggetto esposto a deterioramento, potrebbero comportare un'alterazione

³⁰ Cfr. in tal senso: M. DANIELE, *Prova scientifica e regole di esclusione*, in *Prova scientifica e processo penale*, a cura di G. CANZIO- L. LUPÁRIA, Padova, 2017, p. 506.

³¹ In particolare, è da escludere l'inammissibilità tramite il filtro *ex art.* 189 c.p.p., per la semplice ragione che le prove informatiche di cui si discorre trovano un'apposita disciplina all'interno del codice. Né suona convincente la soluzione che invoca lo sbarramento *ex art.* 190 c.p.p., e in specie del parametro della rilevanza, da intendersi nel significato di idoneità della tecnica scientifica adottata, sicché risulterebbe irrilevante e, quindi, inammissibile la prova formata secondo tecniche non conformi ai protocolli scientifici generalmente riconosciuti: cfr. in tal senso, M. CAIANIELLO, *L'ammissione della prova scientifica nel processo italiano*, in *Prova scientifica e processo penale*, cit., p. 206. Se, da un lato, in tal modo si consentirebbe al giudice di anticipare indebitamente il proprio convincimento (così O. DOMINIONI, *La prova penale scientifica*, Milano, 2005, pp. 220 ss.), dall'altro, il carattere specialistico del *modus operandi* investigativo è tale da consentirne di regola solo una verifica *ex post*: cfr. M. DANIELE, *Prova scientifica e regole di esclusione*, cit., p. 507.

³² Tale l'approdo pressoché univoco della giurisprudenza: cfr., fra le altre: Cass., sez. V, 10 maggio 2017, La Rosa, in *CED*, n. 270139 e Cass., sez. V, 21 marzo 2016, Branchi, in *CED*, n. 266477. Ritengono viceversa nell'ipotesi operante l'inutilizzabilità, che interverrebbe a presidio delle "forme essenziali" dell'atto, intaccate dalla scorrettezza della metodologia impiegata: C. CONTI, *La prova informatica e il mancato rispetto della best practice: lineamenti sistematici sulle conseguenze processuali*, in *Cyber-crime. Diritto e procedura penale dell'informatica*, cit., p. 1334 e, in senso analogo, L. MARAFIOTTI, *Digital evidence e processo penale*, cit., pp. 4521 ss.

³³ Stando alla giurisprudenza l'attività di estrazione di una copia di *file* da un *computer* oggetto di sequestro non comporta attività valutativa su base tecnico-scientifica e "non determina alcuna alterazione dello stato delle cose, tale da recare pregiudizio alla genuinità del contributo conoscitivo nella prospettiva dibattimentale", sicché sarebbe sempre assicurata la futura riproducibilità di informazioni identiche a quelle contenute nell'originale: cfr. Cass., sez. I, 5 marzo 2009, n. 14511, Aversano Stabile, in *Cass. pen.*, 2010, p. 1522. Nel medesimo solco: Cass. 30 aprile 2009, C. R., in *CED*, n. 244454 e, più di recente, Cass., sez. III, 8 luglio 2015, n. 29061, in *Guida dir.*, 2015, n. 32, p. 91.

irreversibile dell'elemento appreso. L'ipotesi è riconducibile alla fattispecie *ex art. 117 disp. att. c.p.p.* ed esige, quindi, il rispetto delle forme *ex art. 360 c.p.p.*

Se, in astratto, la possibilità di formare plurimi duplicati sembrerebbe elidere ogni rischio di irripetibilità dell'attività svolta, le criticità si collocano a monte, ossia al momento della "fotografia digitale" del contenuto racchiuso nel dispositivo. È in questa fase che potrebbe concretizzarsi il rischio di una modificazione irreparabile del dato, dinanzi al quale dovranno adottarsi le opportune cautele volte a preservare la genuinità della conoscenza³⁴. Allo scopo l'*iter* da privilegiare consiste nel sequestro del contenitore informatico, seguito dall'estrazione del relativo contenuto con l'osservanza delle garanzie proprie degli accertamenti tecnici irripetibili.

Si osservi come lo svolgimento del contraddittorio nel momento genetico della prova non solo giovi all'attendibilità del risultato conoscitivo, ma salvaguarda anche la tenuta dell'ipotesi accusatoria perché pone il dato acquisito al riparo dalle probabili confutazioni sulla correttezza del metodo che potranno essere avanzate nel futuro giudizio dal consulente tecnico della difesa.

Di contro, nella prospettiva dell'imputato, l'intervento difensivo *ab inizio* è cruciale: un difensore che assista al compimento dell'atto, benché di regola privo di cognizioni specifiche in materia, avrà l'opportunità di confrontarsi con il proprio consulente in ordine al *modus operandi* degli investigatori per poi contestare in dibattimento l'eventuale scorrettezza delle tecniche impiegate³⁵.

Un altro fondamentale strumento di contrasto alla scienza malamente applicata è infatti il contraddittorio "sulla prova" da esercitarsi in giudizio, che si manifesta come argomentazione critica delle prove digitali assunte nella fase investigativa. Qui riveste un preminente rilievo l'esposizione dei risultati dell'indagine informatica ad opera del perito o del consulente tecnico, che sarà veicolata attraverso l'esame e il controesame, sì da consentire alla difesa di sondare la competenza specifica dell'esperto, l'impiego in concreto delle *best practices* in materia nonché l'osservanza della catena di custodia delle prove digitali.

³⁴ In altri termini, "l'irripetibilità delle operazioni di copia o apprensione dei dati digitali deve essere verificata caso per caso in relazione alle modalità con cui viene svolta": cfr. in tal senso, P. FELICIONI, *Le ispezioni e perquisizioni di dati e sistemi*, cit., p.1421.

³⁵ Da questo punto di vista, è senz'altro censurabile l'indirizzo 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. Asserto smentito dalla l. n. 48 del 2008 che, nel ricondurre le perquisizioni informatiche all'interno del *genus* perquisizioni, riconosce al difensore il diritto di assistere benché senza preavviso: cfr. M. DANIELE, *La prova digitale nel processo penale*, cit., p. 296.

Occorre, peraltro, che si pongano le condizioni perché il controllo differito sulla metodica di riproduzione digitale possa agevolmente esplicarsi. Qui si registra un'ingiustificata latitanza del legislatore, colmabile attraverso la prescrizione di forme di documentazione audiovisiva di tutte le operazioni svolte dagli investigatori³⁶, nonché dell'uso di programmi informatici diversi da quelli coperti da licenza, il quali occultano i loro "codici sorgente", vale a dire le fondamenta che li sorreggono e ne condizionano il funzionamento.

Solo nel rigoroso rispetto di queste condizioni potrebbe configurarsi un onere probatorio in capo alla parte che lamenti la non genuinità del documento digitale, altrimenti, qualora non vi sia trasparenza nell'operato investigativo, l'inattendibilità della prova dovrebbe ritenersi intrinseca³⁷.

Infine, un ulteriore baluardo contro i cattivi scienziati digitali si erge in sede di valutazione. Tutti gli errori tecnici commessi in sede di raccolta ed evidenziati dal contraddittorio argomentativo, pur non sanzionati con l'inutilizzabilità, sono destinati a pesare sul vaglio giudiziale di affidabilità della prova, fino a determinare esiti assolutori.

Lo dimostra una nota vicenda processuale, in cui la Cassazione decretò che le risultanze di indagini – in quel caso genetiche – compiute in violazione delle regole consacrate dai protocolli internazionali erano da ritenersi inaffidabili e prive di autonomia valenza dimostrativa³⁸. Si coglie qui un esempio del superamento del c.d. paradosso della prova scientifica, allusivo alla difficoltà del giudice di compiere un controllo effettivo sui risultati dell'indagine tecnico-scientifica, finendo per rimettere nelle mani dell'esperto la responsabilità della decisione.

Sullo sfondo si staglia un formidabile problema etico e politico di responsabilità del giudicante³⁹, destinato in prospettiva ad amplificarsi dinanzi al futuribile impiego dei *software* di intelligenza artificiale – specie di prova informatica⁴⁰ – come forma di ausilio delle decisioni.

³⁶ Cfr., in tal senso, F. CAPRIOLI, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, cit., p. 3530.

³⁷ Critica l'indirizzo giurisprudenziale che addossa all'imputato l'onere di dimostrare l'avvenuta modifica del dato informatico qualora non sia stata seguita la *best practice* nella fase di raccolta della *digital evidence*: L. MARAFIOTI, *Digital evidence e processo penale*, cit., p. 4521, il quale vi ravvisa una vera e propria *probatio diabolica*, "posto che il dato originario, dopo la modifica, risulta perlopiù irrecuperabile".

³⁸ Cfr. Cass., sez. V, 25 marzo 2015, Sollecito-Knox, in *Foro it.*, 2016, p. 447.

³⁹ V. F. CAPRIOLI, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, cit., p. 3524.

⁴⁰ Cfr., in tal senso, M. GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, p. 61.

Sembra insomma che la giurisdizione sia chiamata ad una sfida non più procrastinabile: l'elaborazione di una cultura dei criteri, ovvero di un codice per valutare il tasso di scientificità della tecnica probatoria adottata, capace di affrancare il giudice dal sapere monopolistico dell'esperto e porlo nelle condizioni di esercitare l'indispensabile ruolo di guardiano contro la cattiva scienza e i cattivi scienziati.