LA CATENA DI CUSTODIA DEL MATERIALE INFORMATICO: SOLUZIONI A CONFRONTO

Laura Bartoli*
Scuola di Giurisprudenza, Università di Bologna

Resumen

«La cadena de custodia de la evidencia informática: comparando soluciones». El artículo describe la normativa vigente relativa a la cadena de custodia de la evidencia digital, comparando las soluciones italianas con las adoptadas en otros países.

Palabras clave: cadena de custodia, evidencia informática, informática forense, derecho processal penal.

Abstract

«Chain of Custody of Digital Evidence: Comparing Solutions». The essay describes the current regulation concerning the chain of custody of digital evidence, comparing the Italian solutions with those adopted in other countries.

Keywords: Chain of Custody, Digital Dvidence, ICT and Law, Criminal Procedure.

Anales de la Facultad de Derecho, 33; diciembre 2016, pp. 145-162; ISSN: e-2530-8319

1. INTRODUZIONE

La prova informatica, da scorcio avveniristico, è ormai divenuta la quotidianità del processo penale. Del resto, sono poche le attività umane a non lasciare una scia di tracce digitali: analizzate, possono avvalorare o smentire un numero sempre maggiore di ricostruzioni. I dati sono così divenuti uno strumento straordinariamente utile per qualunque indagine —anche la più lontana dall'area del *cybercrime*[1]— ma assieme ai vantaggi sono giunte sfide inedite: dobbiamo fare i conti con elementi difficili da incasellare, che sfuggono alla tradizionale bipartizione tra prove fisiche e prove dichiarative[2]. Nella nostra ottica, non interessa infatti il dispositivo —un hard disk, un telefono, una chiavetta USB— ma il suo contenuto: le informazioni, indipendenti tanto dal supporto che le ospita quanto dalla loro rappresentazione[3]. A questo s'aggiunge la loro natura precaria: esse sono facilmente alterabili; anche l'operazione apparentemente più banale può provocare modifiche o perdite, minando alla base la credibilità di quanto raccolto[4]. L'esigenza che sorge, insomma, è quella di tutelare in maniera efficace l'integrità del materiale, tenendolo al riparo da contaminazioni.

Nell'ordinamento che per primo si è posto il problema, quello statunitense, l'insieme di precauzioni messo a punto per raggiungere l'obiettivo è identificato in

---

* Dottoranda di ricerca in Procedura Penale; si ringrazia il professor Cesare Maioli per il supporto e gli utili confronti.

[1] A questo proposito v. Umberg-Warden, *Digital Evidence and Investigatory Protocols*, in *Digital Evidence and Electronic Signature Law Review,* 4/2014, p. 136: «the collection of digital evidence is the «rule rather than the exception» in current investigations»; Daniele, *La prova digitale nel processo penale*, in *Rivista di diritto processuale*, 2011, p. 283; Orlandi, *Questioni attuali in tema di processo penale e informatica*, in *Rivista di diritto processuale,* 2009, p. 129; Caccavella, *Le perizie informatiche,* in Aterno-Mazzotta, *La perizia e la consulenza tecnica*, Padova, CEDAM, 2006, p. 195; Meyers-Rogers, *Computer Forensics: The Need for Standardisation and Certification,* in *International Journal of Digital Evidence,* 3/2004.

[2] È pur vero che un file può contenere una dichiarazione, ma qui interessa l'oggetto digitale in quanto tale —per intenderci, una successione di bit— non la sua rappresentazione. Sul punto, v. Kerr, *Digital Evidence and the New Criminal Procedure*, in *Columbia Law Review,* 2005, p. 279 e ss.

[3] Per una rapida descrizione dei dati, anche nelle loro caratteristiche tecniche, v. Caccavella, *Le perizie informatiche*, cit., p. 196 e ss.; Aterno, *Acquisizione e analisi della prova informatica,* in *Dossier: La prova scientifica nel processo penale - Diritto penale e processo,* 2008, pp. 61-62.

[4] Sul piano tecnico, è sorprendente osservare quanto le procedure d'analisi cambino a seconda dello stato in cui si trova il dispositivo: se acceso o spento; v. Umberg-Warden, *Digital Evidence and Investigatory Protocols,* cit. p. 129. Più in generale, sulla 'volatilità' dell'elemento digitale v. Di Paolo, *Prova informatica*, in *Enciclopedia del Diritto*, *Annali VI*, Milano, Giuffrè, 2014, p. 738 e ss.; Daniele, *La prova digitale nel processo penale*, cit., p. 283; Conti, *Il volto attuale dell'inutilizzabilità: derive sostanzialistiche e bussola della* legalità, in *Diritto penale e processo*, 2010, p. 790 e ss.; Lorenzetto, *Le attività urgenti di investigazione informatica e telematica*, in *Sistema penale e criminalità informatica*, a cura di Luparia, Milano, Giuffrè, 2009, p. 135; Aterno, *Acquisizione e analisi della prova informatica*, cit., p. 62; Luparia, *La ricerca della prova digitale tra esigenze cognitive e valori costituzionali*, in Luparia-Ziccardi, *Investigazione penale e tecnologia informatica*, Milano, Giuffrè, 2007, p. 147-149.

un istituto: la catena di custodia. È la risposta collaudata dalla prassi per soddisfare una regola del diritto delle prove: la parte interessata all'acquisizione di un oggetto deve presentare elementi sufficienti a far ritenere che corrisponda a quanto si sostiene che sia[5]. L'assetto non è stato concepito pensando al mondo impalpabile dei dati: è lo stesso testo a suggerirlo; l'onere grava infatti sulle parti per ogni prova precostituita di cui si chiede l'ammissione. Quando il problema s'è posto in ambito informatico, la garanzia si è semplicemente estesa: per fugare dubbi sull'integrità del materiale, dunque, è necessario tenere una documentazione scrupolosa[6]. All'operatore si chiede di registrare ogni passaggio di mano con precisione: occorre sapere, per ciascun elemento, come è stato raccolto, dove, da chi, quando, con quali modalità. Il percorso del dato dev'essere limpido e consequenziale, privo di lacune. Così facendo, diventa almeno più facile individuare le fonti di pericolo, evidenziare i passaggi più incerti, sfidare la narrazione. Tutto ciò sarebbe ancora insufficiente se non si adottassero procedure tecniche adeguate, tali da non compromettere il materiale che si va cercando; continuità e integrità sono infatti simbionti: la prima serve a poco senza elementi tecnici a protezione della seconda, così come dimostrare la genuinità è operazione assai più semplice se si conoscono nel dettaglio gli snodi del percorso[7].

A partire da questo assetto, l'espressione 'catena di custodia' ha avuto successo e il suo uso s'è rapidamente esteso a diversi ordinamenti, ma dietro alla stessa etichetta non sempre sta la stessa nozione. In alcuni paesi dell'America latina, per esempio, si tratta sì d'un istituto disciplinato da cima a fondo dai codici[8], diversamente dagli Stati Uniti in cui codificata è una regola sull'onere della prova, non il concreto modo per soddisfarla. Nelle leggi europee, invece, si cercherebbe invano un

[5] Il testo originale della Federal Rule of Evidence n. 901 recita: «To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is»; www.law.cornell.edu.

[6] Rispetto a questa materia, il requisito è stato allargato anche al processo civile. Se in ambito penale l'esigenza di un controllo sull'identità dei singoli elementi è sempre stata avvertita, nel civile è invece una novità che dipende dal diverso formato in cui si producono ormai gran parte dei materiali rilevanti. L'informatizzazione ha soppiantato il cartaceo e di conseguenza si è posta l'identica questione di autenticità cui si è fatto fronte, anche in questo caso, con la catena di custodia; v. Arkfeld, *Arkfeld's Best Practices for ESI Pretrial Discovery*, Phoenix, Law Partner Publishing, 2013, § 3.9.

[7] Sul piano concettuale, tuttavia, è bene distinguere: non è detto che a una catena di custodia impeccabile corrisponda un elemento inalterato; specularmente, anche osservando scrupolosamente i migliori standard tecnici potrebbero esserci vuoti di documentazione. Sul punto, v. Ziccardi, *La procedura di analisi della fonte di prova digitale,* in Luparia-Ziccardi, *Investigazione penale e tecnologia informatica*, cit., p. 65; Romero Guerra-Cruz Gómez, *50 preguntas sobre la cadena de custodia federal*, Instituto Nacional de Ciencas Penales, www.inacipe.gob.mx, p. 19.

[8] Per esempio, un intero capitolo del Código de Procedimiento Penal colombiano è dedicato alla catena di custodia (art. 254 s.) cui s'aggiunge la Resolucion 6394/2004, che prevede istruzioni operative stringenti e modelli cui gli agenti devono attenersi. Ugualmente, l'ordinamento messicano disciplina l'istituto nel Código Federal de Procedimientos Penales (art. 123 Bis s.), integrando la disciplina con l'Acuerdo A/002/2010; al gradino inferiore si colloca invece la normativa statale. Anche il legislatore venezuelano ha introdotto il dispositivo con una riforma del 2009, completando il dettato dell'art. 187 mediante l'adozione di un manuale.

corrispettivo letterale: lo stesso risultato è infatti perseguito in modo strutturalmente diverso. Le cautele necessarie a preservare i reperti sono distribuite di volta in volta tra i diversi atti d'indagine, e lo stesso stile dà forma alla disciplina in materia di materiale informatico: lavorando sull'esistente, i legislatori hanno innestato una serie di previsioni specifiche sul tronco originario[9]. La 'catena di custodia' sarà quindi una categoria descrittiva preziosa, utile nella misura in cui designa in sole tre parole tutti i frammenti dedicati alla tutela dell'integrità degli elementi di prova.

Tenendo presente il panorama più largo, ci accosteremo soltanto a quanto riguarda il materiale digitale: a causa della singolare natura dei dati, sono diverse le disposizioni che si distaccano dal quadro generale. Ci dedicheremo a queste e, nel farlo, seguiremo la falsariga dell'ordinamento italiano: ratificando la Convenzione di Budapest sulla criminalità informatica[10], il legislatore ha inserito nel codice di procedura penale una serie di aggiornamenti che analizzeremo di seguito, confrontandoli con quelli adottati in altri sistemi —in particolare quello francese. Non si tratterà d'una comparazione completa, esaustiva in ogni aspetto: si cercherà piuttosto di trarre spunti di riflessione dalle diverse soluzioni normative messe all'opera in diversi ordinamenti.

Per dare un ordine al discorso, spezzeremo in diversi archi il tragitto degli elementi digitali: la ricerca, la raccolta, la custodia e l'analisi. Ragioneremo poi intorno al rapporto tra le norme processuali e le migliori pratiche elaborate in seno alla scienza informatica.

2. RICERCA

Sin dal primo contatto degli investigatori con il materiale informatico, il legislatore si mostra prudente: del resto, come s'accennava, anche la semplice osservazione di un sistema può causare modifiche, sovrascritture o la perdita di dati volatili.

Le modalità d'intervento possibili sono diverse, ciascuna corredata da un insieme di obblighi; prima di avanzare qualche osservazione giova, forse ripercorrere la disciplina. Iniziamo dall'ispezione di sistemi informatici e telematici (art. 244): vi si può accedere per accertare tracce e altri effetti materiali del reato «adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione». La medesima formula torna in materia di perquisizioni (art. 247), ma

[9] In Italia, la tecnica fu criticata: la si ritenne un'occasione mancata per disciplinare l'indagine digitale in maniera organica; per tutti, v. Luparia, *La ratifica della convenzione cybercrime del Consiglio d'Europa-I profili processuali*, in *Diritto penale e processo,* 6/2008, p. 719.

[10] L. 18 marzo 2008, n. 48, che ratifica la Convenzione del Consiglio d'Europa sulla criminalità informatica fatta a Budapest il 23 novembre 2001. Per alcuni commenti alla legge, v. Picotti-Luparia, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa,* in *Diritto penale e processo,* 2008, p. 696 e ss.; Luparia, *Sistema penale e criminalità informatica*, Milano, Giuffrè, 2009; Corasaniti-Corrias Lucente, *Cybercrime, responsabilità degli utenti, prova digitale*, Padova, Cedam, 2009.

il mezzo ha un perimetro differente: è finalizzato alla ricerca di dati, informazioni, programmi informatici o tracce comunque pertinenti al reato ospitati da un sistema informatico o telematico, ancorché protetto da misure di sicurezza[11].

La previsione più articolata è quella che riguarda gli accertamenti urgenti (art. 354): nei casi d'emergenza, gli ufficiali di polizia giudiziaria possono prendere diversi provvedimenti rispetto ai dati, alle informazioni, ai programmi informatici o ai sistemi informatici o telematici. In primo luogo adottano le misure o impartiscono le prescrizioni necessarie ad impedire l'alterazione dei dati o l'accesso ai sistemi. Ove possibile, procedono a immediata duplicazione su supporti adeguati, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità.

Del riepilogo svolto sin qui, colpisce subito la ripetitività; in fondo le esigenze si riducono a due: stabilire le cautele nell'accesso alle informazioni e nella loro duplicazione[12]. Anziché far riecheggiare le stesse formule, poteva essere più efficiente stabilirle una volta per tutte come regole valide per ciascun soggetto, a qualunque titolo coinvolto nell'indagine digitale. La ridondanza, tuttavia, sarebbe una semplice questione di stile se si agisse con precisione: interventi così mirati presuppongono un legislatore sorvegliato, puntuale. Non sono mancate, invece, le sbavature e la disciplina degli accertamenti tecnici del pubblico ministero (art. 359), non interpolata, non presenta disposizioni specifiche. Non si tratta però d'un vizio capitale: da un lato, la lacuna sembra facile da colmare in via interpretativa: se si è inteso tutelare l'integrità di un elemento di prova particolarmente fragile, sarebbe irragionevole differenziare lo standard tecnico a seconda del soggetto che lo maneggia o del mezzo prescelto[13]. Dall'altro, la dimenticanza sembra essere priva di conseguenze pratiche: come vedremo oltre, la violazione delle prescrizioni elencate non sbarra l'accesso del materiale a processo né ne impedisce l'utilizzo; il mancato aggiornamento non comporta quindi un diverso regime.

Al netto della sovrabbondanza, il minimo comun denominatore delle norme citate è la conservazione dell'originale: in effetti, se il materiale fosse ben raccolto e preservato, basterebbe duplicarlo e riprodurre l'analisi; chiunque potrebbe controllare la correttezza di ogni snodo: con la stessa base di partenza si dovrebbero ottenere i medesimi risultati[14]. La legge pone quindi un obbligo che si presenta, a seconda delle formulazioni, in due sfumature. Se da un lato si richiede di «proteggere

---

[11] Nonostante la differenza che le disposizioni tracciano tra ispezione e perquisizione, è il caso di notare come il confine tra i due atti sfumi, in campo informatico, fin quasi a farsi evanescente: v. Costabile, Computer forensics *e informatica investigativa alla luce della Legge n. 48 del 2008*, in *Ciberspazio e diritto*, 2010, p. 480; Aterno, *Modifiche al titolo III del libro terzo del codice di procedura penale*, in *Cybercrime, responsabilità degli enti e prova digitale*, cit., p. 203 e ss.

[12] Categorie che, svecchiando un poco il linguaggio, potrebbero ben essere sostituite a quelle sin qui descritte. Su questo punto si veda la stessa relazione esplicativa alla convenzione di Budapest, disponibile al sito www.coe.int.

[13] In senso analogo v. Lorenzetto, *Le attività urgenti di investigazione informatica e telematica,* cit., p. 141 e ss.

[14] L'assunto è condiviso anche dalla letteratura scientifica di riferimento: è infatti buona norma lavorare su un'apposita copia del materiale, lasciando intatto un originale; v. Raghavan, *Digital*

adeguatamente i dati originali»[15], altrove s'impone di «assicurare la conservazione dei dati originali e [di] impedirne l'alterazione»[16]. L'obiettivo è il medesimo e la sfasatura tra le due espressioni può sembrare irrisoria, ma la seconda pone, in realtà, un comando cui è a volte impossibile obbedire: preservare tutto senza modificare nulla. Per copiare il contenuto della memoria da un computer acceso, per esempio, occorre eseguire un programma che andrà necessariamente a sovrascrivere parte del materiale. Si tratta senza dubbio di una modifica —alcuni dati volatili andranno persi— ma rimane da chiedersi che impatto abbia questa variazione sull'affidabilità del risultato. Gran parte degl'interventi che permettono di estrarre i dati, insomma, quasi sicuramente altereranno il sistema, ma ciò non significa che il valore del dato sia sempre, irrimediabilmente compromesso. Per questo il canone dell'adeguatezza sembra essere quello più utile e onesto[17]: qui dovrebbe fermarsi l'asticella anche nell'interpretare la formula più rigida.

La tutela del materiale di prima mano è dunque una priorità per l'ordinamento italiano; le cose vanno diversamente in Francia, dove la protezione dell'originale è ben lontana dall'essere un valore assoluto. Una volta assicurate alla giustizia, infatti, le informazioni possono essere definitivamente cancellate se la loro detenzione o il loro uso è illegale o pericoloso per la sicurezza di persone o beni[18]. Nel caso in cui i dati provengono da un fornitore di servizi[19], inoltre, è sufficiente conservarne la stampa: la copia integrale della versione digitale su un idoneo supporto non è un dovere, ma una semplice ipotesi alternativa[20]. Si tratta d'una impostazione decisamente distante da quella sin qui illustrata, che si riflette pure in scelte operative differenti: nessuna prescrizione tecnica è dettata all'inquirente —sia egli agente di polizia, pubblico ministero o giudice istruttore. Mancano disposizioni specifiche, ma questo non significa che non sia prevista alcuna cautela; restano le garanzie che presiedono allo svolgimento dell'atto d'indagine con cui si procede: la perquisizione, che deve avvenire in presenza della persona al domicilio della quale ha luogo. Nel caso in cui questa non possa presidiare, l'ufficiale di polizia giudiziaria o il giudice istruttore che procede ha l'obbligo d'invitarla a designare un rappresentante a sua scelta; se nemmeno questa via è percorribile, si procederà in presenza di due testimoni scelti tra persone che non siano soggette alla loro autorità amministrativa[21]. In ogni caso, qualcuno dev'essere in grado di riferire su quanto è avvenuto, e ciò è

forensic research: current state of art, in *CSI transactions on ICT*, 1/2013, p. 91; Mason, *International Electronic Evidence*, British Institute of International and Comparative Law, 2008, p. xlviii.

[15] Art. 254-*bis*.

[16] Artt. 244, 247, 354.

[17] Cfr. Casey, *What does forensically sound really mean?*, in *Digital Investigation*, 4/2007, p. 49.

[18] Art. L56, art. L97 Code de procédure pénale.

[19] La categoria individuata dall'art. R15-33-68 è assai ampia: si estende dalle agenzie di viaggio alle assicurazioni, dai gestori della distribuzione energetica alle imprese di trasporto collettivo. A norma degli articoli L60-2, L77-1-2 e L99-4, a questi enti pubblici o privati è possibile richiedere la messa a disposizione dei dati in loro possesso.

[20] Art. R15-33-74 Code de procédure pénale.

[21] Art. L57, art. L96 Code de procédure pénale.

previsto a pena di nullità dell'atto[22]: la catena di custodia, così, può essere stabilita mediante la ricostruzione che i presenti saranno in grado di offrire.

L'idea che ne emerge, in sostanza, è quella di non lasciare che la polizia o il giudice istruttore agiscano in solitudine, e la soluzione ha i suoi pregi. Lo spettatore ha il compito di vigilare su ciò che accade e potrà quindi denunciare le eventuali irregolarità: al termine delle operazioni deve sottoscrivere il verbale o sarà annotato il rifiuto. L'equilibrio francese, tuttavia, presuppone un obiettivo diverso da quello che muove il legislatore italiano: più che la contaminazione dell'elemento, il rischio che sembra essere scongiurato è quello di manovre arbitrarie da parte degli agenti. L'astante controlla, ma è assai improbabile che sia sufficientemente preparato per cogliere le imprecisioni tecniche, le scelte capaci di compromettere l'integrità del dato[23].

Il sistema italiano invece allarga il bersaglio e prevede modalità operative concrete per la tutela delle informazioni originali; ne abbiamo incontrate di due tipi: l'impartire prescrizioni ad altri e l'impiego di misure tecniche idonee da parte dell'investigatore. Quest'ultimo, se ne deduce, deve evitare modifiche ingiustificate, ma non basta. Deve saper scegliere la strada più adeguata per raggiungere gli scopi fissati dalla norma, e deve farlo su qualunque sistema informatico sia chiamato a intervenire. Lo scenario appare poco realistico, specie in caso di accertamenti urgenti: gli ufficiali di polizia giudiziaria potrebbero non avere alcuna preparazione specifica né esperienze tali da consentire una vera e propria messa in sicurezza della scena informatica. Il rischio di manovre maldestre è alto[24]. Il pericolo cresce se si deve procedere ad immediata raccolta mediante copia: in questo caso occorre svolgere una serie di valutazioni preliminari sull'idoneità del supporto[25], su quale metodo sia bene

---

[22] La sanzione è comminata dall'articolo L59, Code de procédure pénale.

[23] Anche per queste ragioni la miglior letteratura in materia di indagini informatiche tende a prediligere sistemi che traccino le operazioni compiute in maniera automatica —la videoripresa delle operazioni o un sistema di auditing— alle testimonianze; v. Casey, *Digital Evidence and Computer Crimes,* Waltham, Academic Press, III ed., 2011, p. 232.

[24] Basti pensare al caso della sparatoria di San Bernardino: il Federal Bureau of Investigation, tentando d'accedere all'iPhone aziendale in uso a uno degli attentatori, ha chiesto al proprietario che fosse resettata da remoto la password iCloud. Si credeva di poter superare così le misure di sicurezza del telefono senza tener conto di un elemento fondamentale: la password azzerata serviva per accedere allo spazio di condivisione e salvataggio dei dati online, ma nulla aveva a che vedere con il dispositivo fisico, protetto invece da un diverso codice di sblocco. L'azzeramento della password, anzi, ha reciso il collegamento tra il telefono e il cloud su cui il cellulare, pur bloccato, avrebbe salvato automaticamente tutti i dati: una volta in rete, questi sarebbero stati accessibili all'azienda e quindi agl'investigatori. Apple, infatti, ha messo a disposizione le informazioni salvate su iCloud: si trattava però di materiale ormai risalente, che non comprendeva il periodo di maggior interesse ai fini delle indagini —quello delle settimane precedenti all'attentato. Insomma, se avessero evitato mosse incaute, gl'inquirenti avrebbero probabilmente ottenuto tutte le informazioni che cercavano senza bisogno di imbarcarsi in un'odissea giudiziaria; v. Government's motion to compel, depositata il 16 febbraio 2016, p. 18, nota 7. Pur non riferendosi al panorama italiano, l'esempio ci è utile per illustrare il punto: a prescindere dalle normative, non sempre si hanno tutti gli elementi per stabilire, in pratica, qual è l'operazione più corretta; agire d'istinto, però, può mettere a repentaglio l'indagine.

[25] Un riferimento simile compare, nel codice francese, solo nel già menzionato art. R 15-33-74. Nel caso in cui i dati siano messi a disposizione in formato digitale da soggetti terzi, l'ufficiale di

seguire e su come assicurare la conformità del duplicato all'originale. Ovviamente non esiste una singola ricetta per tutti i casi possibili: estrarre dati da un computer portatile, da un cloud o da un telefono dei primi anni 2000 pone questioni tecniche differenti, tutte da affrontare con cautele specifiche[26].

Per di più, la situazione appare particolarmente delicata a questo stadio: il difensore —ammesso che ne sia già stato nominato uno— ha diritto d'assistere ma non di essere avvisato; in pratica non assiste mai e, qui come per molte altre "prove scientifiche", le conseguenze son difficili da rimediare. Nei fatti, i metodi per la loro stessa rilevazione e raccolta possono influenzare irreversibilmente i risultati delle analisi, cosicché quanto avviene in indagine determina giocoforza il seguito. Cercando di arginare i pericoli a ordinamento vigente, si è cercato di ricondurre le operazioni all'area degli accertamenti tecnici irripetibili, agganciando alla nomenclatura le relative garanzie: le parti avrebbero così diritto ad essere avvisate, nominare consulenti tecnici, formulare riserva di promuovere incidente probatorio[27]. Certo, quest'ipotesi non risolverebbe tutti i problemi, ma costituirebbe innegabilmente un salto di qualità; la giurisprudenza tuttavia non concede spiragli, ferma com'è alla distinzione tra 'accertamento' e 'rilievo'[28]. Il discrimine è però datato e si fa meno sostenibile ogni giorno che passa: le operazioni di acquisizione dei reperti, in ambito informatico ma non solo, stanno strette nella nozione di 'rilievo'; la qualifica di attività «meramente meccaniche» è ormai un'illusione, e un'illusione costosa[29]. Le attuali tecnologie sembrano imporre insomma un cambio di passo e, più che ritoccare, converrebbe ripensare per intero le disposizioni sull'analisi della scena[30].

polizia giudiziaria ha due possibilità: stampare quanto serve o copiare integralmente quanto ricevuto su «un supporto informatico conforme agli standard tecnici validi al momento della trasmissione». Nulla si precisa, invece, rispetto alle altre ipotesi di raccolta del materiale mediante copia.

[26] Kessler, *Are mobile device examinations practiced like forensics?,* in *Digital Evidence and Electronic Signature Law Review,* 4/2015, p. 3 s.; Casey, *Digital Evidence and Computer Crime,* cit., p. 227; Federici, *Nuovi orizzonti per l'acquisizione remota di Personal Cloud Storage,* in Maioli, *Questioni di informatica forense,* Roma, Aracne, 2015, p. 113; più in generale, v. Fraser, *Forensics Science: A Very Short Introduction*, New York, Oxford University Press, 2010, p. 17 e ss.

[27] Per un tentativo in questo senso v. Daniele, *Il diritto al preavviso della difesa nelle indagini informatiche*, in *Cassazione penale*, 2012, p. 441 e ss.

[28] Cass., sez. i, 25 febbraio 2009, n. 11503, Rv. 243495; Id., sez. i, 26 febbraio 2009, n. 11863, Rv. 243922; Id., sez. i, 5 marzo 2009, n. 14511, Rv. 243150; Id., sez. i, 30 aprile 2009, n. 23035, Rv. 244454; Id., sez. i, 9 marzo 2011, n. 17244 in *Cassazione penale*, 2012, p. 440; Id., sez. ii, 19 febbraio 2015, n. 8607, Rv. 263797; Id., sez. ii, 4 giugno 2015, n. 24998, Rv. 264286; Id., sez. ii, 1 luglio 2015, n. 29061, Rv. 264572. Salvo diverse indicazioni, le sentenze citate in questo contributo provengono dal *CED Cassazione*.

[29] Lamentando gl'inconvenienti di questa impostazione, la Corte d'assise d'appello di Roma ha sollevato una questione di legittimità costituzionale sull'art. 360 c.p.p. in relazione agli artt. 24 e 111 Cost. «ove non prevede che le garanzie difensive approntate da detta norma riguardano le attività di individuazione e prelievo di reperti utili per la ricerca del DNA». L'ordinanza —la n. 245/2015 del registro della Consulta— è disponibile alla pagina www.cortecosituzionale.it.

[30] V. Camon, *La prova genetica tra prassi investigative e regole processuali,* in *Processo penale e giustizia*, 6/2015, p. 166.

3. RACCOLTA

Una volta individuato, il materiale d'interesse è da prelevare: si procede così al sequestro. La disciplina generale dell'atto, però, non è stata novellata: non contempla quindi la realtà diafana delle informazioni, che non vengono individuate come possibile, autonomo oggetto di sequestro. Nella logica del legislatore, dunque, per mettere le mani sul materiale informatico occorrerà vincolare il supporto fisico: si tratta di una cosa, un oggetto tangibile —realtà che il codice ben conosce e contempla[31].

La scelta potrebbe essere dettata da quell'attenzione all'originale che innerva tutta la riforma: lo si assicura all'indagine attraverso lo spossessamento del dispositivo, evitando anche che il materiale utile venga modificato o cancellato. La soluzione sembra però scambiare il contenitore col contenuto: l'apparecchio, di per sé, è infatti privo d'interesse, rilevano invece le informazioni che incorpora; esse, però, possono essere utilmente raccolte con mezzi ben diversi dall'apprensione del dispositivo. I dati possono essere perfettamente riprodotti, creando un clone in tutto e per tutto identico alla matrice; l'originale può essere ubiquo. Per acquisirlo e impedire che venga alterato, così, non è necessario vincolare le cose; basta una copia ben eseguita.

Su questo punto appare meglio congegnato il sistema d'oltralpe: che proceda la polizia o che proceda un giudice, è espressamente previsto che si possa sequestrare il supporto fisico originale o, in alternativa, una copia realizzata in presenza di chi ha assistito alla perquisizione[32]. Dall'ordinamento italiano, invece, giunge un solo segno di consapevolezza, l'art. 254-*bis*, norma introdotta nel 2008 che regola il sequestro presso i fornitori di servizi informatici e di telecomunicazioni. Si tratta di un'ipotesi speciale, ben circoscritta; in questo caso, tuttavia, l'autorità giudiziaria può limitarsi a duplicare i dati rilevanti[33], che assumono qui —e solo qui— una consistenza autonoma. La disposizione precisa pure la ragione che sta alla base della disciplina: s'intende tutelare la continuità del servizio, evitando di mettere offline un intero server quando è possibile ricorrere a una via alternativa. Si tratta di un'esplicazione del principio di proporzionalità: a parità di risultato, s'impiegheranno le modalità meno invasive, quelle che più lievemente incidono sulle libertà di chi deve subire l'atto.

A ben riflettere, tuttavia, lo stesso ragionamento dovrebbe valere per tutti gli altri soggetti coinvolti, a partire dall'indagato: perché vincolare un computer intero, se un clone delle informazioni utili ne è un sostituto perfetto? Parliamo pur sempre di una compressione dei diritti che non trova nessuna reale giustificazione

---

[31] *Contra* Novario, *Criminalità informatica e sequestro probatorio: le modifiche introdotte dalla l. 18 marzo 2008, n. 48 al codice di procedura penale,* in *Rivista di diritto processuale*, 2008, p. 1070;

[32] Art. L56, art. L97 Code de procédure pénale.

[33] Le accortezze da adottare son descritte nei dettagli: occorre un supporto adeguato, una procedura che assicuri la conformità del duplicato rispetto all'originale e la sua immodificabilità. Al fornitore del servizio è poi ordinato di proteggere gli originali che, nonostante il sequestro, non escono mai dal suo possesso.

nelle esigenze dell'accertamento: queste sarebbero soddisfatte anche dalla soluzione meno incisiva, più rispettosa delle sfere di libertà del soggetto passivo[34]. Il dato letterale che la relega ad eccezione merita d'essere capovolto: sul piano della gerarchia delle fonti, un appiglio potrebbe derivare dalla formula costituzionale del «giusto processo», di cui la proporzionalità, secondo un'opinione qui condivisa, costituisce una dimensione[35].

La prassi, ad ogni modo, conosce già misure intermedie: il supporto fisico è spesso sottratto al proprietario per il tempo necessario a duplicarlo, quindi è restituito. Sarebbe un buon compromesso se non presentasse una controindicazione: come abbiamo detto, l'oggetto dell'atto non è il contenuto, ma il contenitore. Una volta svincolato, dunque, chi ha subito il sequestro si trova a metà del guado: non ha alcun bene da rivendicare, ma l'autorità giudiziaria ha raccolto e conserva tutte le informazioni che ritiene rilevanti. Le conseguenze seguono a fil di logica: la giurisprudenza, a partire da una nota decisione del 2008, ha ritenuto inammissibile la richiesta di riesame perché, una volta restituito l'oggetto, viene meno l'interesse a impugnare[36]. Solo di recente l'indirizzo è stato rimesso in discussione: superando il dato letterale, si è dapprima affermata la capacità del solo dato di essere sottoposto a sequestro[37]; in seconda battuta si sono tratte conclusioni coerenti con la premessa: se il materiale informatico resta nelle mani dell'autorità giudiziaria, il vincolo permane nonostante la restituzione del supporto[38].

Pur per un percorso travagliato, in definitiva, la cassazione si è spinta là dove il legislatore era stato reticente: l'autonomia delle informazioni dal supporto è stata stabilita in via generale —almeno in questo recente approdo— e la sua duplicazione vale a imporre un vincolo.

Perché il clone sia un sostituto perfetto, tuttavia, è necessario che le operazioni siano trasparenti, ripercorribili, ben relazionate. Si torna insomma al nodo cruciale —la documentazione— che dovrebbe essere il più possibile esaustiva, indicando nello specifico le procedure adottate e tutto ciò che serve a identificare univocamente quanto prelevato. Prendiamo ad esempio un hard disk: per effettuarne una riproduzione, s'impiega di norma il bit-stream image, una tecnica che consiste nel copiare una memoria bit per bit. Non ci si limita, insomma, a riprodurre i file salvati conservandone l'ordine, ma si trascrivono anche tutte quelle zone del disco rigido che non contengono nulla di direttamente percepibile all'utente[39]. Per controllare che la

---

[34] Della stessa opinione, ancor prima della riforma del 2008, Manchìa, *Sequestro probatorio di* computers*: un provvedimento superato dalla tecnologia?* In *Cassazione penale,* 2005, p. 1638.

[35] Camon, *cit.*, p. 167 e ss.

[36] Cass., S.U., 24 aprile 2008, n. 18252, in *Diritto penale e processo*, 2009, p. 469 e ss., con nota di Carnevale, *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare*; nella stessa direzione, Cass., sez. vi, 24 aprile 2012, n. 29846, Rv. 253251; Id., sez. i, 8 ottobre 2013, n. 43541, Rv. 257357; Id., sez. iii, 30 maggio 2014, n. 27503, Rv. 259197.

[37] Cass., sez. vi, 24 febbraio 2015, n. 24617, Rv. 164092.

[38] Cass., sez. iii, 23 giugno 2015, n. 38148, Rv. 265181.

[39] Per ulteriori dettagli tecnici, v. Aterno, *Acquisizione e analisi della prova informatica,* cit., p. 62 e ss.

```
Information for H:\server\server.ad1:
[Computed Hashes]
 MD5 checksum:     9aa28d9314de1713c0e936f6af9d1035
 SHA1 checksum:    7fe4a33e5d260fb1b49184b4e2f0bb6729e411cb

Image information:
 Acquisition started:   Wed Mar 30 14:18:26 2011
 Acquisition finished:  Wed Mar 30 15:53:52 2011
 Segment list:
  H:\server\server.ad1
  H:\server\server.ad2
  H:\server\server.ad3
  H:\server\server.ad4
  H:\server\server.ad5
  H:\server\server.ad6
  H:\server\server.ad7

Image Verification Results:
 Verification started:  Wed Mar 30 15:54:19 2011
 Verification finished: Wed Mar 30 16:03:02 2011
 MD5 checksum:     9aa28d9314de1713c0e936f6af9d1035 : verified
 SHA1 checksum:    7fe4a33e5d260fb1b49184b4e2f0bb6729e411cb : verified
```

clonazione sia andata a buon fine, occorre un passaggio preliminare: il calcolo di un hash. Prima di dare inizio alla copiatura, si applica un algoritmo[40] che, a un input di estensione variabile —sia un singolo file, sia un intero disco rigido— produce una stringa alfanumerica di lunghezza predefinita. Ogni cambiamento dell'input, per quanto microscopico, darà luogo a un hash del tutto differente[41]: la sequenza potrà quindi essere utilizzata per individuare il disco a colpo sicuro, come se si trattasse di un set d'impronte digitali[42]. Per assicurare la conformità della copia all'originale occorrerà quindi applicare lo stesso algoritmo e comparare il risultato: se i dati sono rimasti intatti, il valore calcolato dovrebbe essere identico. Lo stesso meccanismo vale per controllare l'integrità delle informazioni a distanza di tempo: basterà confrontare la stringa con cui è stato identificato il disco all'inizio dell'indagine con il risultato dell'algoritmo in qualunque momento successivo; se tutto corrisponde, il materiale non avrà subito variazioni. Per intenderci bene, vediamo un esempio più concreto.

[40] Ne esistono molti, diversi tra loro per struttura e per lunghezza dell'output: uno dei più diffusi è la funzione MD5 che genera una stringa di 128 bit. Lo standard federale statunitense, invece, è dato dai Secure Hash Algorithm, una famiglia che comprende cinque funzioni; la più diffusa è la SHA-1, che produce una sequenza di 160 bit. Per ulteriori dettagli, v. Casey, *Digital Evidence and Computer Crime,* cit., p. 22 e ss.

[41] Il risultato, infatti, non riflette in alcun modo il contenuto dei file né è possibile invertire la funzione e ristabilire, partendo dall'hash, l'insieme di dati cui si ricollega. Tra input e output c'è una relazione matematica, non semantica.

[42] Più precisamente, è molto improbabile che a input diversi corrisponda lo stesso output: la sicurezza dell'algoritmo cresce al diminuire della probabilità di collisioni, ovvero che sia generato un risultato identico per due input diversi.

L'immagine mostra un verbale prodotto per la duplicazione di un disco rigido: sono riportate due stringhe che risultano da due diverse funzioni di hash —MD5 e SHA-1— applicate all'insieme di dati[43]. Vengono poi riportate la data e l'ora di inizio e fine dell'operazione e, per chiudere, viene svolta una verifica sull'immagine forense creata. I valori vengono calcolati sulla base dei medesimi algoritmi, ma questa volta a partire dalla copia; li si confronta poi con quelli elaborati in precedenza sul disco originale: se le stringhe coincidono —come in questo caso, dove il risultato è identico— potremo affermare che il clone è in tutto e per tutto uguale all'hard disk di partenza.

Avendo a disposizione una documentazione esaustiva, sarà possibile ricostruire la correttezza dei singoli passaggi; tuttavia, anche su questo punto il codice è drammaticamente antiquato: la normativa è stata pensata trent'anni fa, mentre i redattori avevano sotto gli occhi una realtà d'indagine tutta diversa. Quali misure tecniche sono state adottate nel caso concreto? Quali programmi si sono utilizzati? Quali operazioni sono state preferite e come sono state svolte? Nulla obbliga gli operatori a riferire su questo[44] e riesce difficile saggiare ex post la correttezza metodologica dell'intervento se le informazioni sono scarse, generiche.

4. CUSTODIA E ANALISI

Una volta raccolto il materiale, la preoccupazione del legislatore si sposta: l'integrità dell'elemento passa attraverso una corretta custodia dei dati e, per provvedervi, schegge specialistiche sono state mescolate alle vecchie disposizioni. S'inizia redigendo il verbale di sequestro (art. 81 disp. att.), che indica la specie e il numero dei sigilli apposti. La norma fa il paio con il primo comma dell'art. 260, che contempla la possibilità di vincolare le cose con mezzi «di carattere elettronico o informatico»[45]. Si tratta, in sostanza, della crittazione dei dati: senza una chiave di decodifica, saranno inaccessibili[46].

---

[43] Utilizzare più funzioni è uno stratagemma per aumentare la sicurezza dell'identificazione: come dicevamo, è improbabile —sebbene possibile— che due input diversi diano luogo alla stessa traccia hash. Il rischio che la difformità tra originale e copia passi inosservata utilizzando due diversi algoritmi è addirittura inverosimile: anche se si verificasse una collisione rispetto a uno dei due risultati, l'altro supplirebbe. Nell'immagine, vediamo che l'hash MD5 dell'originale corrisponde all'hash MD5 della copia; allo stesso modo corrispondono le tracce SHA-1. La corrispondenza della copia all'originale è così accertata con un margine d'errore molto ridotto.

[44] A titolo di esempio, v. Cass., sez. III, 28 maggio 2015, n. 37644, Rv. 265180. Nel caso di specie, non era indicata la stringa che risultava dalla funzione di hash, rendendo così impossibile ogni valutazione circa la corrispondenza all'originale.

[45] Si è tuttavia sostenuto che si tratti di «una mera ipotesi di scuola» che difficilmente avrebbe preso piede all'interno del processo; v. Monti, *La nuova disciplina del sequestro informatico*, cit., p. 207.

[46] Si soffermano sul tema Novario, *Criminalità informatica e sequestro probatorio*, cit., p. 1070 e ss.; Massari, *Commento all'art. 260*, in Conso-Illuminati, *Commentario breve al codice di procedura penale*, 2015, p. 998 e ss.

Il supporto fisico andrà quindi riposto in un pacco numerato e sigillato, pronto per essere conservato in cancelleria o in segreteria. Su questo punto, si mostra più confuso il codice francese: in alcuni casi è espressamente previsto che i supporti fisici siano sigillati[47]; in altri del tutto simili, manca una disposizione analoga[48].

L'iter italiano procede lineare: le cose sequestrate saranno inventariate secondo quanto disposto dall'art. 82 disp. att., che prevede le verifiche necessarie in caso di alterazione dei sigilli; se occorresse rimuoverli per il compimento di un atto, sarebbero poi da apporre nuovamente.

Se non è possibile affidare le cose alla segreteria o alla cancelleria, è nominato un custode. I doveri che assume sono ben modellati: deve impedire l'alterazione o l'accesso di terzi non autorizzati ai dati, alle informazioni e ai programmi informatici a lui affidati.

I supporti potrebbero deteriorarsi, e la legge scongiura anche questo rischio contemplando la possibilità di clonare gli originali (art. 260). Anche in questo caso ritroviamo le cautele già viste —l'adeguatezza di mezzi e procedure, l'immodificabilità— e di nuovo ci s'imbatte in una lieve asimmetria rispetto all'art. 258, che regola la copia dei documenti sequestrati. La novella del 2008 ha lasciato intatta quest'ultima disposizione; eppure, se si tratta di requisiti minimi per ritenere una riproduzione affidabile, non avrebbe senso differenziarli a seconda del fine che il duplicato serve.

La legge tace invece rispetto alla fase successiva, quella dell'analisi: si ricadrà nel generale ambito delle consulenze tecniche, lasciando agli esperti il compito d'individuare gli strumenti d'indagine che meglio s'attagliano alle circostanze del caso e le modalità di documentazione più adeguate.

Nel caso in cui il consulente tecnico della parte privata sia autorizzato all'esame delle cose sequestrate ai sensi dell'art. 233, l'autorità giudiziaria potrà imporre «le prescrizioni necessarie per la conservazione dello stato originario delle cose». Forse la previsione meritava di essere sgrossata ed estesa. Abbiamo visto con quanta insistenza si sia inserito un inciso, una clausola a salvaguardia della sacralità dell'originale[49] in quasi tutte le ipotesi di contatto dell'investigatore con l'elemento digitale. Sembra strano che questa attenzione si affievolisca proprio qui, dove il rischio di manipolazione irreversibile del dato è dietro l'angolo. Poteva valere la pena stabilire esplicitamente che le analisi devono essere svolte —ove non sia assolutamente necessario procedere altrimenti— su un clone dell'elemento prelevato: si sarebbe chiuso il cerchio. L'originale rimarrebbe intatto, pronto per essere nuovamente duplicato in caso di necessità: ogni esame sarebbe ripetibile e verificabile da parte di un perito o

[47] È il caso degli articoli L97 e R15-33-74 che si riferiscono, quanto ai sigilli, anche ai supporti informatici.

[48] Art. L56, che non estende ai dati la disciplina invece prevista per documenti e oggetti.

[49] L'espressione è in Ziccardi, *L'ingresso della* computer forensics *nel sistema processual-penalistico italiano: alcune considerazioni informatico-giuridiche*, in *Sistema penale e criminalità informatica*, cit., p. 167.

di un consulente tecnico, lasciando poi al giudice il compito di valutare quale delle ricostruzioni proposte è la più corretta.

5. UTILIZZABILITÀ E MIGLIORI PRATICHE

Se la legge ha il merito di aver fissato obiettivi nitidi, ha però la colpa di non averli costruiti a sufficienza: nonostante la novella, le incertezze che sorgono dal disposto normativo italiano restano molte.

Un primo fronte sguarnito riguarda la violazione degli obblighi sin qui descritti: manca, infatti, una sanzione processuale che colpisca l'inosservanza delle precauzioni stabilite e se le cautele non vengono impiegate, i dati mal raccolti o mal conservati saranno comunque ammissibili e utilizzabili[50]. Alla parte interessata non resta che screditare gli elementi acquisiti mettendo ben in evidenza tanto l'inadeguatezza tecnica delle procedure quanto il loro concreto impatto sulla genuinità del dato.

Ad avviso di alcuni, un simile assetto finisce per imporre alla difesa un vero e proprio onere probatorio del quale si chiede o si postula il rovesciamento: secondo quest'opinione, infatti, dovrebbe essere l'accusa a dimostrare di aver rispettato tutti canoni della buona indagine informatica e di aver così consegnato al processo del materiale affidabile[51]. Per raggiungere il risultato, si è ragionato attorno alla formula dell'art. 533: il dubbio che basta ad assolvere non può ritenersi fugato se le prove non sono affidabili, e siccome sta all'accusa dimostrare la colpevolezza, spetterà sempre a questa il compito di provare la genuinità dei reperti[52]. L'argomento è suggestivo ma non convince fino in fondo: s'invoca qui, più che la presunzione d'innocenza, una presunzione d'inattendibilità dell'elemento che sembra però logicamente slegata dalla prima. E in effetti, altri si spingono appunto a formulare espressamente una «presunzione di ripudio» del dato, che sarebbe da considerare manipolato «ad arte» fino a prova contraria[53].

Per verità, simili letture sembrano ricalcare lo schema statunitense, dove —lo si è visto— l'unica disposizione espressa si occupa proprio di questo problema: si

---

[50] La giurisprudenza è ferma: Cass., sez. III, 28 maggio 2015, n. 37644; Id. sez. II, 1 luglio 2015, n. 29061; Id., sez. II, 4 giugno 2015, n. 24998; Id., sez. II, 12 dicembre 2008, n. 11135.

[51] Caccavella, *Le perizie informatiche*, cit., p. 198 e ss.; Cajani, *Anatomia di una pagina* web, in *Diritto dell'Internet*, 2007, p. 484; Id., *Il vaglio dibattimentale della* digital evidence, in *Archivio penale,* 2013, p. 851; Luparia, *Il caso "Vierika», cit.*, p. 158, che ritiene si tratti di un aggravio che si colloca «fuori dall'architettura sistematica del nostro ordinamento processuale».

[52] Così Tonini, *Informazioni genetiche e processo penale ad un anno dalla legge,* in *Diritto penale e processo*, 2010, pp. 887-888. La tesi è stata proposta rispetto a un diverso tipo di prova, quella genetica: l'ambito è differente, ma i problemi che si pongono sono affini sia per quanto riguarda il rapporto tra scienza e diritto, sia per quanto attiene alla catena di custodia dei reperti. L'opinione, insomma, sembra poter essere discussa anche in questa sede senza che ne esca snaturata.

[53] Caccavella, *Le perizie informatiche*, cit., p. 198. All'impostazione aderisce Cajani, *Anatomia di una pagina* web, in *Diritto dell'Internet*, 2007, p. 484; Id., *Il vaglio dibattimentale della* digital evidence, cit., p. 851.

stabilisce che la parte interessata all'acquisizione di un reperto ha il dovere di accreditarne la genuinità. Se l'onere non è soddisfatto, gli elementi di prova non saranno ammessi. Riprodurre un regime simile, tuttavia, sembra un'operazione azzardata: l'ordinamento italiano non esprime una norma analoga; non assegna a nessuna delle parti il compito di dimostrare che le operazioni si sono svolte correttamente; non pone nessuno sbarramento all'ingresso dei dati, per quanto mal raccolti. Acquisito il materiale, al giudice spetta il compito di valutarlo liberamente: dovrà farsi carico delle incertezze, ponderarne l'incisività e decidere, tracciando il percorso logico seguito nella motivazione[54]. Mettere in discussione l'elemento, incrinarne l'attendibilità non è allora un onere delle parti, ma un mero interesse: si cercherà di sottolinearne tutte le fragilità non per escluderlo dal compendio probatorio, ma per farlo apparire al giudice come una piattaforma troppo fragile per sorreggere una decisione.

Il rischio, però, è quello di navigare a vista: il contraddittorio tecnico, come s'è detto, è legato a doppio filo al destino dell'originale. Se questo manca, non sarà possibile ripetere le analisi per confermare o smentire la correttezza delle procedure; il dibattito non potrà che arrestarsi a quanto emerge, senza concedere alle parti o al giudice la possibilità di andare più a fondo.

La questione è intimamente connessa a un ulteriore nervo scoperto: anche se la legge ponesse un vero e proprio divieto probatorio —e, abbiamo detto, non lo fa— resterebbe da individuare un modo concreto per centrare gli obiettivi fissati dal codice. Questo, infatti, non detta specifiche tecniche e l'elasticità ha i suoi vantaggi: l'evoluzione dell'informatica è travolgente e il ritmo dell'aggiornamento sarebbe duro da reggere anche per il più attento dei legislatori. Del resto, sta nella natura delle cose: la scienza si nutre di dubbi mentre al codice tocca dare certezze. Inoltre, l'indagine penale può ormai giovarsi di un ventaglio piuttosto ricco di strumenti tecnico-scientifici profondamente diversi l'uno dall'altro; a maggior ragione, un discorso normativo troppo volenteroso dovrebbe spandersi per mille rivoli, col rischio d'irrigidire la disciplina all'eccesso[55]. Tuttavia, limitarsi a dire che le operazioni devono essere svolte in modo corretto rinunciando ad eleggere un metodo significa lasciare quest'affermazione nel vuoto.

Potrebbe forse essere più saggio rinviare alle migliori pratiche di ciascun settore[56]: si guadagnerebbe in aggiornamento e agilità, lasciando stabilire agli esperti quali sono i requisiti minimi per ritenere tecnicamente affidabili le operazioni. La soluzione, del resto, è tutt'altro che sconosciuta. Diversi ordinamenti, per ragion pratica prima che per forza di legge, hanno visto crescere l'integrazione tra le norme e i protocolli operativi: per non veder falcidiati i risultati d'indagine, le forze dell'ordine si sono dotate di linee guida tali da assicurare la catena di custodia del dato.

---

[54] Su questo punto, pur riferito a un diverso ambito, v. Spangher, *Considerazioni sul processo «criminale» italiano*, Giappichelli, Torino, 2015, p. 39.

[55] V. Camon, *La prova genetica, cit.,* p. 167.

[56] Suggerisce di inserire «uno schema di protocollo generale» nelle disposizioni di attuazione del codice di procedura penale Macrillò, *Le nuove disposizioni in tema di sequestro probatorio e di custodia ed assicurazione dei dati informatici*, in *Diritto dell'Internet,* 2008, p. 516.

Questo è, ad esempio, il caso degli Stati Uniti, dove la proliferazione delle buone pratiche in materia informatica è sorprendente[57]: il solo National Institute of Justice ha emesso una serie di manuali mirati, che differenziano le prescrizioni a seconda del tipo d'intervento richiesto[58] e del tipo di soggetto agente[59]. Lo stesso vale per il Regno Unito, dove l'associazione degli ufficiali di polizia si è data standard giunti ormai alla quinta edizione[60].

Anche là dove la catena di custodia è istituto codificato anello per anello, non mancano i protocolli che, senza le formalità della legge, precisano i requisiti minimi per l'affidabilità del materiale raccolto: il codice venezuelano, per esempio, rimanda a un manuale[61]; questo contiene direttive dedicate a ciascuna area scientifica d'interesse —tra cui l'informatica forense— tanto rispetto al lavoro di raccolta sul campo quanto alla successiva fase d'analisi in laboratorio.

Una soluzione simile sarebbe auspicabile anche in Italia non per consegnare alla scienza la disciplina del processo, ma per rendere più controllabili —e dunque più garantite— le procedure che coinvolgono saperi specialistici: gli obblighi elastici che il codice esprime potrebbero essere concretamente valutati alla stregua d'un modello definito. Gl'inquirenti sarebbero così portati a muoversi con più circospezione e perizia, evitando disattenzioni che potrebbero intaccare l'indagine intera. Gl'indagati avrebbero miglior gioco nello sfidare l'accusa anche sul piano tecnico e il giudice non sarebbe lasciato solo a indovinare dell'attendibilità del dato: stabilito un metodo, se ne farebbe garante.

Agognando questo equilibrio, si è sostenuto che la legge 48 del 2008 contenesse un implicito rinvio alle migliori pratiche così da conferire a queste ultime un'efficacia quasi normativa. L'impostazione, per certi versi confortante, non può essere condivisa: il riferimento, per essere tale, dovrebbe essere tutt'altro che sottinteso, indicando chiaramente l'insieme di regole tecniche da prediligere; né da un richiamo tacito si possono dedurre reazioni eloquenti[62]. D'altronde non esistono,

---

[57] Per una panoramica esaustiva si rinvia a Casey, *Digital Evidence and Computer Crime*, cit., p. 230; Raghavan, *Digital forensic research: current state of art*, in *CSI transactions on ICT*, 1/2013, p. 95. Mescola spunti di comparazione con le linee guida australiane Mc Kemmish, *When is digital evidence forensically sound*, in *Advances in digital forensics IV,* Elsevier, 2008.

[58] v. Keisler-Daley-Hagy, *Investigative Uses of Technology: Devices, Tools, and Techniques*, National Institute of Justice, www.ojp.usdoj.gov/nij.

[59] Hagy, *Electronic Crime Scene Investigation: A Guide for First Responders,* National Institute of Justice, www.ojp.usdoj.gov/nij.

[60] Si allude al *ACPO Good Practice Guide for Digital Investigation*, v version, 2012, in www.digital-detective.net.

[61] Più precisamente, si tratta del *Manual Único de Procedimientos en Materia de Cadena de Custodia da Evidencias Físicas*, previsto dall'art. 187 del Código Orgánico Procesal Penal venezuelano.

[62] Leggendo nell'intervento del 2008 la volontà di escludere materiale informatico raccolto e conservato in maniera scorretta, in molti hanno intravisto diverse forme d'invalidità, dalla nullità dell'atto con cui l'elemento è stato raccolto —v. Vitale, *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico*, in *Diritto dell'Internet,* 2008, p. 509— all'inutilizzabilità: tra i molti, v. Luparia, *Il caso «Vierika»*, cit., p. 158; Id., *Processo penale e tecnologia informatica*, *ibidem*, 2008, p. 221; Lorenzetto, *Le attività urgenti di investigazione informatica e*

allo stato, protocolli o accordi italiani in grado d'imporsi sul piano nazionale. Alla mancanza, tuttavia, si potrebbe rimediare facendo riferimento alle autorevoli linee guida elaborate dall'Organizzazione internazionale per la normazione in materia di prova digitale[63]: si tratta di un punto di riferimento mondiale, spesso preso in considerazione nella redazione degli standard nazionali.

Uno stimolo in questo senso potrebbe arrivare dalle crescenti esigenze di circolazione della prova: non è un caso che uno degli organismi d'indagine attualmente al lavoro in seno all'Unione Europea —l'OLAF[64]— si sia dotata di linee guida parecchio stringenti. In materia di accertamenti informatici, si è scelto di abbracciare sia gli standard inglesi sia le linee guida ISO: le prescrizioni puntano al livello più alto di pulizia metodologica, così da troncare sul nascere ogni questione relativa all'ammissibilità dei dati raccolti, qualunque sia l'autorità chiamata ad utilizzarli. Il poco sta nel molto, e dato che l'ufficio raccoglie elementi senza sapere in anticipo come e dove saranno utilizzati, si cerca di soddisfare i criteri di ammissibilità di ciascun tribunale, indipendentemente dal paese in cui si trova o dal tipo di giurisdizione che esercita.

Abbracciare uno standard metodologico sarebbe un passo avanti, ma il cerchio si chiuderebbe se la legge fosse un poco più decisa nel regolare pure le conseguenze delle eventuali violazioni.

Lo scenario attuale offre qualche apertura, qualche segno di un'accresciuta consapevolezza da parte della prassi[65]. Una rimeditazione approfondita, tuttavia, sembra tanto urgente quanto lontana: anche nei più recenti innesti normativi, il legislatore non ha approfittato dell'esperienza per aggiustare il tiro. Nella disposizione che regola l'acquisizione di documenti e dati conservati all'estero —l'art. 234-*bis,* introdotto dalla legge del 17 aprile 2015, n. 43— la preoccupazione per l'autenticità nemmeno traspare: nella migliore delle ipotesi, se si trattasse d'informazioni disponibili al pubblico, si potrebbe imbastire un confronto; diversamente, entrerà a processo del materiale rispetto al quale la controparte non ha immediate possibilità d'interazione. Inoltre, non si è stabilita alcuna regola metodologica per il suo prelievo o per la sua conservazione: non si sono nemmeno replicati gli obblighi premurosamente aggiunti nel 2008; di certo, il livello di garanzie non sembra essersi innalzato.

---

telematica, cit., p. 135. Per un affresco esaustivo delle diverse posizioni dottrinali, v. Cajani, *Il vaglio dibattimentale della* digital evidence*,* cit., p. 835.

[63] Ci si riferisce a *Guidelines for identification, collection, acquisition and preservation of digital evidence* ISO/IEC 27037: 2012.

[64] Acronimo francese per *Office européen de Lutte Anti-Fraude*. Si tratta di un corpo esclusivamente amministrativo che ha per obiettivo il contrasto alle frodi capaci di ledere gli interessi finanziari dell'Unione Europea: v. Lasagni, *Cooperazione amministrativa e circolazione probatoria nelle frodi doganali e fiscali,* in *Diritto penale contemporaneo* (web), 23 settembre 2015.

[65] Pur esulando dal campo informatico, merita di essere segnalata Cass., sez. iii, 16 dicembre 2009, n. 2388, in www.iusexplorer.it. Dinanzi alla perizia svolta su cose non sigillate e non corrispondenti nella quantità all'indicazione del verbale di sequestro, la Corte ha affermato che «prima di utilizzare la perizia, si sarebbero dovuti svolgere accertamenti per stabilire se, nonostante la mancanza dei sigilli, dovessero escludersi ipotesi di manomissione o di confusione tra reperti».

Insomma, la strada da fare sembra essere ancora molta: occorre da un lato un legislatore più pronto e preciso, disposto a un dialogo maturo con le istituzioni scientifiche.

Dall'altro, tuttavia, anche la disciplina più raffinata potrebbe non essere metabolizzata da chi è chiamato a rispettarla: sarebbe indispensabile una presa di coscienza da parte di tutti i soggetti coinvolti —polizia, magistrati e avvocati— mentre il tema appare accantonato, poco approfondito e ancor meno compreso[66]. Si tratta, spesso, di una mancanza di strumenti: un'alfabetizzazione condivisa avrebbe ricadute importanti, forse anche a ordinamento invariato; sarebbe più semplice promuovere metodi d'indagine comuni, chiederne il rispetto e stigmatizzare le negligenze.

Recibido: julio 2016; aceptado: mayo 2017

[66] Della stessa opinione, Caccavella, *Le perizie informatiche*, cit., p. 195. Lapidario il giudizio di Mason, cit., ad avviso del quale «data in digital format has brought about a revolution that most lawyers and judges have failed to understand», p. xxxvii.