SU STATUTO EPISTEMOLOGICO E CONSOLIDAMENTO TECNICO-GIURIDICO DELL'INFORMATICA FORENSE

Raffaella Brighi
Ricercatrice e Professoressa di Informatica Giuridica
CIRSFID*, Università degli Studi Bologna, Italia

Resumen

La crisis en las ciencias forenses y, en particular, en la informática forense parece haber quedado superada en la actualidad gracias a un plan integrado que contiene distintos elementos de armonización. Se ha acogido una aproximación epistemológica que presta más atención a las fases previas y de instrucción: se sitúa en un marco jurídico común destinado a luchar contra el ciberdelito, que comparte protocolos operativos y estándares tecnológicos. Además, se han organizado algunas unidades especiales con el fin de gestionar las pruebas digitales; a través de la creación de ambientes virtuales, estas unidades pueden automatizar algunas de las fases de la gestión forense, memorización y análisis, lo que da lugar a investigaciones más efectivas y limita el recurso a la pseudociencia. Por último, la práctica interdisciplinar desempeña un papel estratégico, ya que permite a cada uno de los grupos —científicos forenses y prácticos del derecho— entender mejor las necesidades y limitaciones del otro.

Palabras clave: informática forense, armonización, epistemología, estándares tecnológicos, ambientes virtuales.

Abstract

«On the Epistemological Status and Technico-Legal Consolidation of Digital Forensics». The crisis in forensic science, and in particular in computer forensics, seems to have been overcome today thanks an integrated governance plan containing several harmonizing elements. A new epistemological approach has been embraced that pays closer attention to the pretrial and investigative phases: It is set within a common legal framework for fighting cybercrime and shares operating protocols and technological standards. Also, some special units have been set up for the purpose of managing digital evidence: By creating virtual environments, these units can automate some of the phases in forensic management, memorization, and analysis, thus making investigations more effective and limiting recourse to «junk science.» Finally, interdisciplinary training plays a strategic role by enabling each group —forensic scientists and legal practitioners— to better understand the needs and limitations of the other.

Keywords: digital forensics, harmonization, epistemology, shared standards, virtual labs.

Anales de la Facultad de Derecho, 33; diciembre 2016, pp. 39-55; ISSN: e-2530-8319

1. PREMESSA

Numerosi studi e report governativi, non troppo risalenti nel tempo, hanno denunciato la crisi delle discipline forensi. In particolare il noto rapporto della *National Accademy of Science* del 2009 —*Strengthening Forensic Science in the United States: A Path Forward* (noto come rapporto NAS) sottolinea:

> the forensic science system exhibits serious shortcomings in capacity and quality; yet the courts continue to rely on forensic evidence without fully understanding and addressing the limitations of different forensic science disciplines[1].

Il documento, ampio e articolo, oltre a evidenziare le carenze di molti metodi forensi su cui si basa il lavoro della polizia e dei pubblici ministeri offre un gran numero di raccomandazioni volte a superare le criticità: da questioni strutturali, quali la creazione di enti autonomi e indipendenti (cui il *National Institute of Forensic Science*), all'accreditamento di centri specializzati, alla certificazione degli esaminatori o ancora alla standardizzazione delle procedure. Aspetto comune a tutti i punti sollevati è la creazione di una adeguata *governance*.

Al di là delle critiche che il rapporto NAS ha suscitato nell'immediato, causate soprattutto da una certa resistenza al cambiamento[2], a fronte dei progressi degli ultimi anni, si può affermare che il cambio di paradigma auspicato sia effettivamente in atto. Molti fattori fanno pensare che si stiano gettando le basi per una nuova visione dell'informatica forense, e più in generale, delle scienze forensi ma, in particolare, il cambiamento è trainato dalla coniugazione di due elementi, funzionali uno all'altro: da un lato la definizione di una cornice epistemologica più concreta di riferimento per le scienze forensi, d'altro lato l'armonizzazione degli standard tecnici e giuridici.

2. EPISTEMOLOGIA E SCIENZE FORENSI

Il dibattito filosofico-giuridico per la comprensione e la risoluzione delle questioni giuridico-epistemologiche è stato spesso troppo astratto e, dunque, distante dal «sistema giustizia». Ciò ha portato a trascurare il rapporto tra i professionisti del diritto e gli scienziati forensi che, invece, è fondamentale per il bilancio complessivo dell'ecosistema delle scienze forensi.

---

* Centro Interdipartimentale di Ricerca in Storia del Diritto, Filosofia e Sociologia del Diritto e Informatica Giuridica.

[1] National Research Council, National Academy of Sciences, *Strengthening Forensic Science in the United States: A Path Forward*. Washington, DC: National Academies Press, 2009, p. 53.

[2] Giannelli, Paul C., «The 2009 NAS Forensic Science Report: A Literature Review» in *Crim. L. Bulletin* 378 (2012); Case Legal Studies Research Paper N. 2012-11. Disponibile su SSRN: http://ssrn.com/abstract=2039024.

In tutti i tipi di processo si ravvisa la tendenza a espandere il ricorso alla scienza forense con un impiego massivo di procedure scientifiche da parte degli investigatori, che si pensa possano fornire al giudice elementi più oggettivi, sicuri e controllabili. Il giudice, al momento del processo, per quanto *peritus peritorum*, è costretto a farsi coadiuvare da esperti —non sempre «studiosi»[3]— delle varie scienze che lo aiutino a stabilire quali siano le affermazioni scientifiche vere e quali false delle parti. La scienza ha però modalità e tempi diversi dal diritto. Da un lato è piuttosto chiaro che la conoscenza scientifica non sia sinonimo di verità[4] e che la caratteristica di fondarsi su metodi empiricamente controllabili non garantisca la certezza dei risultati; anzi, in molti contesti, la scienza può fornire solo dati statistici (frequenze) sul verificarsi o meno di una certa affermazione. D'altro canto, le decisioni giuridiche sono soggette a vincoli di tempo e di risorse, e gli interessi contrapposti delle parti possono portare a condurre una «ricerca interessata», volta a trovare evidenze favorevoli o a screditare evidenze non favorevoli piuttosto che a «cercare la verità».

L'epistemologia può aiutare ad affrontare le differenze intrinseche tra scienza e diritto, per quello che attiene prove e procedure probatorie, in particolare in riferimento ad alcune questioni centrali, ovvero indagare il rapporto tra evidenza scientifica[5], ricerca scientifica e ricerca guidata dal contenzioso («interessata»); affrontare il rapporto tra probabilità e giustizia; e chiarire il ruolo della testimonianza scientifica esperta nel difficile bilanciamento tra inammissibilità e completezza[6]. Per definire una cornice concreta per tutte quelle «procedure e pratiche che danno struttura agli sforzi giuridici di determinare la verità»[7] serve infatti comprendere la natura dell'evidenza scientifica e come essa si rapporta al concetto giuridico di prova,

[3] Per un'analisi dei requisiti di periti e consulenti tecnici si veda l'intervento «L'attività del perito e le best practices» di Maioli, C., Rabbito, C. e Gammarota, A. in *Italian Cyberspace Law Conference*, 2004 e Caccavella, D., «Le perizie informatiche: Gli Accertamenti tecnici in ambito informatico e telematico», in Aterno, S. e Mazzotta, P. (a cura di), *La perizia e la consulenza tecnica*, Cedam 2006.

[4] La posizione del realismo scientifico classico, che la scienza si avvicini in modo progressivo alla *verità*, appare debole nel caso delle «rivoluzioni scientifiche» che comportino un cambiamento ontologico radicale dell'immagine del mondo fornita dalla teorie ritenute vere fino a quel momento (Kuhn, T., *The Structure of Scientific Revolutions*, 1962); se, storicamente, teorie molto autorevoli si sono rivelate false o inadeguate si potrebbe pensare che anche le teorie attualmente accettate non siano vere. L'anti-realismo scientifico arriva a negare la portata di verità attribuita alle teorie scientifiche dal realismo scientifico e a affermare che le teorie scientifiche «costruiscano il mondo».

[5] Con evidenza scientifica intendiamo qualsiasi informazione, con valore probatorio, che sia accertata, in senso lato, grazie all'utilizzo di una legge scientifica o di un metodo tecnologico. «È «scientifica» quella prova che, partendo da un fatto dimostrato, utillizza una legge scientifica per accertare un fatto «ignoto» per il giudice», così Tonini P., «Progresso tecnologico, prova scientica e contrattaditorio», in De Cataldo Neuburger, L. (a cura di), *La prova scientifica nel processo penale*, CEDAM, 2007. Taruffo in *La prova dei fatti giuridici,* Milano, 2002 introduce una sotto classificazione della prova in prova scientifica e in prova informatica (o tecnologica), che si caratterizza a sua volta per l'impiego di strumenti informatici.

[6] Haack, S.*, Legalizzare l'epistemologia. Prova, probabilità e causa nel diritto*, Egea, Milano, 2015.

[7] Haack, S., *op. cit*, p. 41.

spiegare come questa debba essere valutata a garanzia del grado di prova richiesto, stabilire come valutare la testimonianza esperta di natura scientifica e definirne le strategie di inammissibilità.

Il problema di come stimare l'evidenza scientifica, e con essa la credibilità dei testimoni esperti[8], nel contesto giuridico è un problema non nuovo ma centrale anche per l'informatica forense. Dall'analisi della giurisprudenza dell'ultimo ventennio, a prescindere dal sistema giuridico di riferimento (accusatorio o inquisitorio), emergono numerosi tentativi di risolvere le criticità e delineare un quadro di riferimento, perché la testimonianza esperta sia di aiuto nel determinare la *verità*. L'approccio teorico più tradizionale, in cui il diritto sostanzialmente recepisce conoscenze accertate dalla scienza ufficiale, sembra ormai superato di fronte alla consapevolezza della non neutralità delle proposizioni scientifiche e dell'incertezza nello stabilire quale sia la scienza valida.

Come noto, i primi passi significativi in questo senso sono venuti dall'esperienza nordamericana con la cosiddetta sentenza *Daubert*[9] del 1993 che ha rappresentato per la giurisprudenza non solo americana, un punto fermo nel dibattito sulla prova scientifica. Con questa discussa sentenza la Corte Suprema degli Stati Uniti ha modificato i criteri di riferimento fino ad allora adottati dalle Corti per il ricorso alla scienza, dando origine a un quadro particolarmente complesso. Fino a quel momento le Corti si basavano sul *Test di Freye*, risalente a una famosa sentenza del 1923, secondo il quale il criterio per stabilire la scienza valida era quello della *general acceptance* da parte della comunità scientifica di riferimento; l'intento era quello di escludere come non ancora validate nuove posizioni scientifiche[10]. Con questo impianto, piuttosto restrittivo, è evidente che la scienza ufficiale tendeva a prevalere sullo stretto diritto e a guidare le decisioni dei giudici, dando adito a sentenze contraddittorie per via della ambiguità nello stabilire il grado del consenso generale e nell'individuare la comunità scientifica di riferimento. Con Daubert e le decisioni che lo seguirono (la cosiddetta trilogia Daubert[11]), dal punto di vista dell'equilibrio tra scienza e diritto, la strategia è stata quella di spostare il primato decisionale sul giudice[12], affidandogli il compito di vagliare l'attendibilità e la pertinenza della evidenza scientifica presentata dall'*expert witness*, per mezzo di una griglia di criteri di valutazione che la Corte stessa definisce. I criteri sono stati sostanzialmente quattro:

---

[8] La prova scientifica è spesso presentata nei processi da parte di un perito, *expert witness*. L'esperto comparirà in giudizio e testimonierà sulla perizia. Le competenze dell'esperto e la determinazione dell'oggetto dell'incarico influiscono chiaramente sull'attendibilità del risultato.

[9] Daubert vs. Merrel Dow Pharmaceuticals, 509 US 579 (1993). Trad. it parziale in *Riv. trim. dir. proc. civ.*, L (1996), p. 277 e ss.

[10] Dominioni, O., *La prova penale scientifica. Gli strumenti scientifico tecnici nuovi o controversi e di elevata specializzazione*, Giuffrè, Milano, 2005, p. 117.

[11] Oltre al caso Daubert, anche General Electric Co. v. Joiner (1997) e Kumho Tire Co., Ltd. v. Carmichael (1999).

[12] In questo caso la Corte dovette trovare un legame tra il test di *Freye* e le *Federal Rules of Evidence* (Rule 702-Testimony of Expert) che assegnano al giudice il compito di assicurare che la testimonianza dell'esperto sia rilevante e affidabile (*reliable*).

(i) se la teoria o la tecnica impiegate alla base della prova siano state testate e siano falsificabili; (ii) se la teoria o tecnica sia stata oggetto di *peer review* e pubblicata; (iii) il tasso di errore, noto o potenziale, associato alla teoria o tecnica e, infine, (iv) se la teoria o tecnica sia stata generalmente accettata dalla comunità scientifica di riferimento[13]. Nello stabilire i criteri la Corte richiama i *metodi* che la scienza usa per valutare l'attendibilità delle teorie scientifiche, facendo esplicito riferimento contemporaneamente alla teoria sulla falsificabilità di Popper[14] —secondo cui la scienza procede tramite falsificazione delle affermazioni—, e al positivismo logico di Hempel[15] in base al quale una teoria scientifica deve avere opportune verifiche empiriche che la confermino. Come è noto, poi, nelle decisioni che seguirono, *Joiner* e *Kumho Tire*, la Corte suprema Suprema degli USA ha in parte ampliato le regole di Daubert lasciando di fatto sempre più margine decisionale alle corti per valutare l'attendibilità di una testimonianza esperta.

Il modello proposto, in prima istanza, ha accolto molti pareri favorevoli anche a livello internazionale, perché coniuga e integra tra loro più criteri e in tale maniera sembrerebbe avvicinarsi maggiormente alla metodologia impiegata nelle scienze sperimentali. Esaminato alla luce del rapporto scienza e diritto, però, non si può non rilevare che questo modello, pur salvando il concetto di validità della scienza, consolida il potere del sistema giudiziario di decidere ciò che «*conta come scienza*» per il diritto[16]. Nello stabilire quale sia la scienza valida, il diritto non è più meramente norma tecnica ma contribuisce a definire il sapere scientifico[17].

Da molte parti si è affermato che la sentenza Daubert non abbia raggiunto il suo obiettivo. Daubert e la sua progenie hanno creato, in verità, molte controversie in fase di applicazione, soprattutto per la difficoltà nell'individuare standard di validità per conoscenze scientifiche molto differenti e il conseguente rischio, sottolineato da molti, di fare entrare nei processi la *junk science*[18] —la cattiva scienza, la scienza spazzatura— costituita da quelle conoscenze che, se pur presentate come scientificamente testate, sfuggono da qualunque valutazione di scientificità. Alcuni, per questo, vedono

---

[13] La bibliografia sulla portata della sentenza è vastissima. Cfr. ad esempio Dondi, A., «Paradigmi processuali e «expert witness testimony»»,in *Riv. trim. dir. proc. civ*., 1996; Dominioni, O., *La prova penale scientifica*, cit.; Taruffo, M., «La prova scientifica nella recente esperienza statunitense», in *riv. trim. dir. proc. civ*, L, 1996; Taruffo, M., *La prova dei fatti giuridici*, cit..

[14] Popper, K.R., *The Logic of Scientific Discovery*, Hutchinson, London 1959 e Popper, K.R., *Conjectures and Refutations*, London 1963.

[15] Hempel, C.G., *Filosofia delle scienze naturali*, Bologna, 1978.

[16] Jasanoff, S., *La scienza davanti ai giudici. La regolazione giuridica della scienza in America*, Milano, 2001, p. 372.

[17] Tallachini, M.C., «Scienza e diritto. Verso una nuova disciplina», in Jasanoff S., *op. cit*., p. VI.

[18] È celebre la distinzione tra *good science* e *junk science* in Huber, P., *Galileo's Revenge: Junk Science in the Courtroom.* BasicBooks, (HarperCollins), 1991. Il ricorso alla cattiva scienza ha portato a numerosi errori giudiziari. Utilizzare cattiva scienza, ovvero opinioni presentate come scientifiche quando non hanno alcuna fondatezza, è un modo di influenzare l'opinione pubblica; soprattutto nei sistemi giuridici nord americani è molto sentito il problema di impedire l'ingresso della cattiva scienza nei processi per evitare il condizionamento di giudici e giurie.

in Daubert un paradosso: il giudice nomina il perito proprio perché non è in grado di effettuare egli stesso un accertamento di tipo scientifico ma si pretende che sia il giudice stesso a valutare l'esito della prova peritale, al fine di stabilire se vale la pena di servirsene per la decisione sui fatti. Pertanto, si presuppone che il giudice possa effettuare ex post una valutazione su cognizioni scientifiche che egli non possedeva ex ante[19]. La giurisprudenza nord americana, d'altra parte, evidenzia le debolezze di Daubert nel caso di giudizi penali: mentre pare avere ristretto gli standard di ammissibilità in ambito civile, in ambito penale il suo effetto è spesso irrilevante[20].

Le analisi più recenti degli studiosi di epistemologia individuano la causa dell'incertezza che emerge dalla giurisprudenza e dalla dottrina post Daubert proprio nella scarsa coerenza delle stesse regole di Daubert sul profilo filosofico-scientifico. Particolarmente chiara, a tale proposito, è la posizione di Haack[21] che mostra sia come la Corte nel caso Daubert abbia richiamato in modo improprio le teorie di Popper, che non forniscono al giudice i criteri per stabilire né se un elemento di prova è realmente scientifico né se esso è attendibile, sia elemento ancor più grave come la Corte abbia sbagliato nella pretesa di spiegare cosa distingue un metodo scientifico da un metodo non scientifico e nell'aver identificato il concetto di «scientifico» con «attendibile».

In linea con la posizione di Haack, evidenziamo infatti che alla base della filosofia della scienza di Popper vi è la convinzione che non si possa mai dimostrare la verità di una affermazione scientifica; una teoria scientifica può essere tutt'al più «corroborata» ovvero essere stata testata e non falsificata, ma ciò non implica che la teoria sia vera. Assumere dunque che il criterio di falsificabilità di Popper potesse essere applicabile per valutare l'attendibilità della testimonianza scientifica è stato fuorviante.

Si concorda con Haack anche laddove sostiene che il richiamo al *metodo scientifico* non sia efficace per valutare l'attendibilità di una testimonianza esperta, sia perché scientificità e attendibilità non sono caratteristiche sovrapponibili, e quello che interessa giuridicamente è piuttosto l'attendibilità della testimonianza, sia perché l'accento posto sul metodo scientifico porta a distogliere l'attenzione dalle *conclu-*

[19] Per un esame critico del paradosso si veda Taruffo M., in *Scienza e processo,* Secolo XXI, 2009. Sulle criticità di Daubert anche Welch, C.H., «Flexible standards, deferential review: Daubert's legacy of confusion», 29 *Harvard J. Of Law & Public Policy*, 2006, pp. 1085-1101.

[20] Cfr. Haack, S. in «La testimonianza esperta: lezioni dall'esperienza statunitense» in *Legalizzare l'epistemologia. Prova, probabilità, causa nel diritto*. 2015. Milano, Egea, p. 141. Si veda anche Peter J. Neufeld, «The (Near) Irrelevance of Daubert to Criminal Justice and Some Suggestions for Reform» in *American Journal of Public Health* 95 (2005); Berman, K.R. and McClennen, N., «Daubert Turning 20: Junk Science Replaced By Junk Rulings?», 2012, *ABA Section of Litigation Annual Conference*, 2012.

[21] L'Autrice affronta il tema in diversi suoi scritti. In particolare si veda S. Haack «Prova ed errore: la filosofia della scienza della Corte suprema americana» in *Ars Interpretandi* 11, 2006, pp. 303-326, in cui l'autrice mostra anche come la concezione di Hempel di testabile sia piuttosto distante dalle teorie di Popper e quindi citata impropriamente nella sentenza Daubert.

sioni[22]. Inoltre, se si intende il metodo scientifico come quell'insieme di procedure pratiche e concrete che lo scienziato mette in atto per formulare le sue congetture[23], si può ancora obiettare che tale procedure non sono seguite da tutti gli scienziati e non sono seguite solo dagli scienziati, quindi non può essere questo il criterio per determinare la scientificità di una teoria[24].

La sentenza Daubert, e le sentenze che lo hanno seguito, dunque non si sono riferite con i loro criteri a una specifica epistemologia, ma piuttosto hanno concorso a una «costruzione giuridica della conoscenza specialistica»[25], ovvero definiscono come il diritto vede la scienza e la rende fruibile per i suoi scopi[26].

Questo è il punto da cui muove il dibattito più recente[27]: definire una epistemologia per il diritto partendo da ciò che già è implicito nella giurisprudenza e nelle procedure di armonizzazione e standardizzazione.

Tali basi, a parere di chi scrive, sono ben poste da Haack che, muovendo dal pragmatismo nordamericano, riporta i criteri di validità piuttosto a *canoni di razionalità*[28]: «l'osservazione può contribuire alla solidità dell'evidenza per una teoria scientifica», quindi occorre superare la distinzione netta tra enunciati teorici e osservativi, ammettendo l'esistenza di «un continuum di enunciati più o meno osservativi»; «migliore è l'evidenza rispetto a una teoria, più è verosimile che questa sia vera»; inoltre l'Autrice raccomanda di non trattare le evidenze scientifiche in modo esclusivamente formale e logico, ma di tenere in considerazione che la scienza riguarda anche le nostre interazioni con il mondo e, dunque, il contesto.

È importante sottolineare che questo passaggio non avviene solo con norme giuridiche e regole. Iniziative come l'istituzione di centri forensi specializzati, tra cui i laboratori forensi virtuali, lo mostrano: l'attenzione deve essere posta maggiormente alle fasi precedenti il processo per evitare la cattiva scienza. Vi è la necessità di scavare a fondo nel lavoro scientifico per comprendere eventuali debolezze piuttosto che etichettarlo come pseudoscienza. Ciò assume rilievo ancora maggiore nel contesto della informatica forense, disciplina in continuo cambiamento per la rapidissima evoluzione delle tecnologie, dove è strategica la definizione di protocolli operativi per gli accertamenti informatici e la documentazione delle prove.

Il principio fondamentale —sviluppato e consolidato a partire dalla sentenza Daubert— che le prove fornite dall'esperto non siano vincolanti per il giudice e che, per quanto esse siano complesse, il giudice ha l'onere di interpretarne e rie-

---

[22] Cfr. Haack, S., *Legalizzare l'epistemologia*, cit. p. 196.

[23] Sulla storia della concezione del metodo scientifico nel pensiero occidentale si veda Oldroy D., *Storia della filosofia della scienza*, Milano, Il saggiatore, 1998.

[24] Haack, S., *Six Signs of Scientism*, Logos & Epiteme, III, 1, 2012, pp. 75-95.

[25] Jasanoff, S., *op. cit.*, p. 372.

[26] Fuselli, S., *Apparenze. Accertamento giudiziale e prova scientifica*. Milano, FrancoAngeli, 2008, p. 54.

[27] Tra tutti si rimanda a Black S. and Nic Daied N., «Time to think differently: catalysing a paradigm shift in forensic science», in *Philosophical Transactions of the Royal Society* London, Biol Sci., 2015.

[28] Haack, S., *op. cit.*, pp. 199-205.

laborarne i contenuti informativi in modo autonomo, è ormai da tempo alla base degli ordinamenti processuali. In particolare nel contesto europeo, soprattutto in ambito penale, importanti basi normative per la disciplina della prova scientifica nei distinti momenti della ammissione, dell'assunzione e dell'utilizzazione dell'elemento di prova contribuiscono a definire il ruolo della scienza nel processo; inoltre diverse sentenze fissano criteri per la validazione del sapere scientifico non consolidato[29]. In Italia è la sentenza della Cassazione penale 43789/2010[30] che affronta esplicitamente la questione:

> Per valutare l'attendibilità di una teoria occorre esaminare gli studi che la sorreggono; le basi fattuali sulle quali essi sono condotti; l'ampiezza, la rigorosità, l'oggettività della ricerca; il grado di sostegno che i fatti accordano alla tesi; la discussione critica che ha accompagnato l'elaborazione dello studio [...]. Infine, dal punto di vista del giudice è di preminente rilievo l'identità, l'autorità indiscussa, l'indipendenza del soggetto che gestisce la ricerca, le finalità per le quali si muove. [...] Gli esperti dovranno essere chiamati [....] a delineare lo scenario degli studi e a fornire gli elementi che consentano al giudice di comprendere [...]. Di tale complessa indagine il giudice infine è chiamato a dar conto in motivazione, esplicitando le informazioni scientifiche disponibili e fornendo razionale spiegazione, in modo completo e comprensibile a tutti, dell'apprezzamento compiuto.

Dunque il consulente non si sostituisce al giudice ma deve fornirgli tutti gli strumenti affinché possa formulare un giudizio, analitico e rigoroso, su quanto prodotto. In particolare, l'obbligo di motivazione della decisione —sia quando il giudice ritiene di non seguire il parere dell'esperto sia quando invece aderisce alle sue conclusioni— appare determinante, in quanto garantisce la funzione autonoma del giudice rispetto all'esperto, sostenendo l'esigenza di un *controllo razionale*. Tale obbligo implica che il giudice analizzi e controlli la prova scientifica e giustifichi esplicitamente le proprie valutazioni, anche quando ritiene che la prova scientifica acquisita sia valida e attendibile.

Questo è tanto più rilevante se si pensa che ad oggi nelle questioni attinenti alla informatica forense, in particolare in ambito penale, non pare essere mai stata sollevata in giudizio, almeno in Italia, la questione della cattiva scienza e nemmeno casi in cui il procedimento acquisitivo della *digital evidence* sia caratterizzato da una tale illegittimità che lo renda inutilizzabile nel processo[31]. Le tecniche di informatica forense peraltro possono esprimere una valutazione sul grado di compromissione di un dato informatico e quindi il giudice dovrà valutare se estromettere totalmente il dato o piuttosto valutare sia pur parzialmente il contenuto informativo dello stesso.

---

[29] Tra le numerose fonti si veda Sallavaci, O., *The Compact of scientific evidence on criminal trial*, Routledge, 2014.

[30] Cass. pen., sez. IV, 17 settembre 2010, n.º 43786.

[31] Cajani, F., «Il vaglio dibattimentale della digital evidence», in *Archivio Penale* LXV(3), 2013, pp. 837-852.

Sicuramente per il giudice è un compito difficile ma, se da un lato il ricorso alla scienza costituisce uno strumento poderoso di accertamento processuale della verità dei fatti, è illusorio pensare che esso abbia l'effetto di rendere più facile il lavoro del giudice e gli consenta di delegare ad altri decisioni tanto complesse[32].

Il nuovo approccio epistemologico —più attento alle fasi precedenti al processo giudiziario e a alla valutazione del contesto di riferimento— ben si coniuga con la definizione di un quadro giuridico comune di contrasto al crimine informatico e con la condivisione di protocolli operativi e standard tecnologici.

Cardini dell'armonizzazione: norme, regole e tecniche per l'informatica forense

L'informatica forense raggiunge, oggi, una maggiore centralità nelle aule di giustizia grazie alla diffusione di standard tecnici e protocolli operativi nonché alla armonizzazione del quadro giuridico di riferimento per il contrasto al crimine informatico. L'ecosistema informatico, altresì, esercita una importante influenza sui giudici (come cittadini) che va valorizzata soprattutto con ricerche che non siano finalizzate solo alla realizzazione di nuovi *widget* per la polizia e nuovi strumenti per la fase istruttoria, ma piuttosto rafforzino le basi olistiche —senza soluzione di continuità: principi, pratiche, procedure— di quanto disponibile e contribuiscano a definire e diffondere le pratiche migliori[33]. Probabilmente la lezione di progettazione centrata sull'utente che tanti risultati positivi ha dato in molti settori delle Tecnologie della Informazione e della Comunicazione (TIC) va estesa di più al sistema giudiziario e alla magistratura, pena un disallineamento tra gli strumenti disponibili agli investigatori[34].

La prima leva di armonizzazione, guida del cambio di paradigma, va individuata senza dubbio nella definizione di un *quadro giuridico comune*. È generalmente accettato che un certo grado di armonizzazione tra i paesi è di vitale importanza se si vuole raggiungere una regolamentazione efficace di contrasto ai reati informatici: anche se sono sempre esistiti reati di natura transnazionale —per esempio il traffico di esseri umani, armi e droga, il contrabbando, il riciclaggio di denaro e il terrorismo— la criminalità informatica ha caratteristiche uniche per via della natura intrinsecamente globale della sottostante tecnologia. La cooperazione, per essere proficua, richiede la definizione di un quadro legislativo comune e le opportune salvaguardie: gruppi di specialisti sul *cybercrime*, addestramento degli investigatori

---

[32] Così Taruffo, M., in *Scienza e processo*, cit.

[33] Pollitt, M., «A History of Digital Forensics». *Advances in Digital Forensics* VI, Springer, 2010.

[34] Hibshi, H., Vidas, T. and Cranor, L., «Usability of Forensics Tools: A User Study». *Sixth InternationalConference on IT Security Incident Management and IT Forensics*, USA, 2011; Jarrett, M.H., Bailie, M.W., Hagen E. and Eltringham, S., *Prosecuting Computer Crimes Computer Crime and Intellectual Property Section Criminal Division*. Office of Legal Education Executive Office for United States Attorneys, 2009.

e dei magistrati, cooperazione inter-agenzie, cooperazione tra pubblico e privato, cooperazione internazionale sia tra polizie (Europol) che tra magistrati (Eurojust).

Dal punto di vista giuridico il riferimento fondamentale, come è noto, è rappresentato dalla *Convenzione di Budapest*[35] del Consiglio di Europa[36], primo strumento internazionale vincolante per affrontare in modo globale il problema, che cerca di armonizzare le leggi sui reati informatici dei vari Stati aderenti, migliorare le capacità e le modalità di indagine e accrescere la cooperazione investigativa internazionale. La Convenzione si occupa dei reati contro la confidenzialità, integrità e disponibilità di sistemi e dati informatici, di quelli relativi a contenuti in cui si utilizzino le tecnologie della informazione e della comunicazione per facilitare la distribuzione di materiali illegali o illeciti e di reati relativi alla effrazione della tutela della proprietà intellettuale.

È evidente che, oggi, passati quindici anni dalla promulgazione, la Convenzione risente della maturità della tecnologia; per cui trascura, a livello di diritto sostanziale, reati allora meno sentiti come, per esempio, l'uso di Internet per terrorismo, gli attacchi *botnet*, il *phishing* e a livello di diritto procedurale, questioni ora molto attuali, quali le intercettazioni di comunicazioni *Voice over IP* (VOIP) e l'ammissibilità di elementi di prova di procedure per il trattamento di informazioni criptate[37].

Va notato come la Convenzione allarghi le disposizioni a qualunque reato in cui sia necessario raccogliere elementi probatori in formato elettronico[38]: diversi Stati che l'hanno ratificata, dunque, hanno promulgato, in buona parte, leggi che consentono agli investigatori di individuare e sequestrare computer e dati digitali, effettuare intercettazioni telematiche, ottenere dati relativi a comunicazioni registrate o in tempo reale, indipendentemente dalla circostanza che il reato su cui si indaga sia un reato informatico.

L'armonizzazione delle norme è necessaria soprattutto per eliminare «porti franchi» e per facilitare la cooperazione internazionale. La modalità di armonizzazione della Convenzione —che è del tipo che Sieber definì «armonizzazione flessibile»[39]— fa riferimento a un modello uniforme per la costruzione delle regole che stabilisce i parametri di accettazione del diritto sostanziale mentre lascia la formulazione del regole procedurali alle peculiarità culturali di ciascuna nazione.

ANALES DE LA FACULTAD DE DERECHO, 33; 2016, PP. 39-55

---

[35] Aperta alla firma il 23 novembre 2001, dopo un percorso di 16 anni, la Convenzione è entrata in vigore il 1 luglio 2004.

[36] Il cibercrimine minaccia l'obiettivo del Consiglio di Europa di potenziamento dei diritti umani, democrazia e norme giuridiche.

[37] Gercke, M., «10 Years Convention on Cybercrime», *Computer Law Review International* 142, 2011, pp. 147-149.

[38] Vatis, M.A., «The Council of Europe Convention on Cybercrime» in Proc. of a Workshop on *Deterring CyberAttacks: Informing Strategies and Developing Options* for US Policy, National Academies Press, 2010.

[39] Sieber, U., «Memorandum für ein Europäisches Modellstrafgesetzbuch», *Juristen Zeitung* 52, 1997.

Considerando che armonizzazione non implica identità di trattamento, la Convenzione rappresenta lo strumento multilaterale più significativo nella regolazione del cibercrimine e dell'adattamento reciproco delle legislazioni, dal punto di vista (I) della completezza (reati sostanziali, modalità procedurali, cooperazione internazionale); (II) della protezione dei diritti (tra cui applicazione degli strumenti per la tutela dei diritti umani, di rispetto del principio di proporzionalità, impatto su terze parti, poteri di indagine, assistenza reciproca tra gli Stati, estradizione, sovranità territoriale) e (III) della rappresentatività (attualmente gli Stati[40] la cui legislazione per il contrasto alla criminalità informatica sono ispirate e conseguenza della Convenzione sono oltre 120)[41]. Anche se non è incisiva come un trattato internazionale, non esiste alcuna iniziativa equivalente che si avvicini a questo livello di accettazione mondiale.

L'Unione Europea ha assunto negli anni un approccio proattivo al problema concentrandosi sulla creazione di una *cybersecurity strategy*[42] e della *European Union Agency for Network and Information Security* (ENISA), per una prevenzione efficace piuttosto che rispondere, reattivamente, ai vari tipi di attacco informatico[43]. Un insieme di iniziative internazionali, regionali di area e nazionali sono state attivate a partire dal 2001 e la Convenzione rappresenta la pietra di paragone rispetto alla quale possono essere misurati tali sforzi.

Di importanza centrale, a livello globale, sono gli sviluppi della *Salvador Declaration* del 2010 del *United Nations Office on Drugs and Crime* (UNODC) detta anche «UN Convention». UNODC assiste gli Stati membri sul contrasto al *cybercrimine* e ha collaborato con altre commissioni delle Nazioni Unite[44] a effettuare un ampio studio che, ultimato nel 2013, ha portato a numerose proposte di rafforzamento a livello nazionale e internazionale, in relazione alla crescita di comprensione del fenomeno, alle competenze per individuare e contrastare i reati e al potenziamento della cooperazione e dei i meccanismi di scambio informativo.

Iniziative significative sono state intraprese a livello internazionale in seguito alla Convenzione, tra il 2005 e il 2014, da parte di *Commonwealth*, *Shanghai Cooperation Organization*, *League of Arab States*, *Caribbean* ITU, *ITU/Secretariat of the Pacific Community*, *Convention on the Establishment of a Legal Framework Conductive to Cybersecurity in Africa*.

Il risultato di tale convergenza di sforzi di armonizzazione legislativa, siano essi strumenti giuridicamente vincolanti o non vincolanti, internazionali o regionali

---

[40] Di cui: è stata ratificata da 47 Stati; sottoscritta da 11; 8 Stati invitati a sottoscriverla; 22 altri Stati la cui legislazione è in linea; 45 altri Stati che stanno legiferando, ispirandosi ad essa.

[41] Seger, A., «The cost of cybercrime-the benefits of cooperation», *CTO cybersecurity Forum*, Forum, CoE, 2013.

[42] EU, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 7.2.2013 JOIN (2013), 2013.

[43] Di Noto, N., *Europe's fight against cybercrime*, The ReSHAPE Research Project, 5/13, 2013.

[44] UN, Crime Prevention and Criminal Justice.

di area, ha accresciuto, nel breve periodo, la capacità di contrasto e l'autosufficienza dei singoli Stati e, nel lungo periodo, la capacità di cooperazione internazionale contro una sfida globale[45]. L'influenza della Convenzione è stata così pervasiva sulle legislazione in materia di criminalità informatica di tutto il mondo che qualsiasi accordo internazionale dovrebbe in gran parte rispecchiarne i termini e, ove se ne discostasse in maniera significativa, porterebbe a disaccordi con i Paesi che hanno ratificato la Convenzione. Allo stesso modo, al fine di garantire un accordo con quei Paesi che si sono opposti a vari aspetti della Convenzione, per esempio su temi dei diritti umani e della protezione della privacy, non si potrebbe che diluire, sospendere o rimuovere norme già adottate. Inoltre alcuni reati sostanziali potrebbero non essere inclusi. In definitiva, il perseguimento di accordi più ampi non porterebbe che a iniziative «al ribasso».

L'armonizzazione legislativa è un processo e non una destinazione; così come la tecnologia si evolve e cambia così anche le «nostre risposte dovranno evolversi e cambiare»[46]. L'ideale che tutti gli Stati membri abbiano un'ampia legislazione in materia di criminalità informatica è un obiettivo nobile, ma è superato da molti anni. Con quasi il 60 per cento dei paesi esaminati nella *Comprehensive Study* dell'UNODC[47] sulla criminalità informatica, che indicano la necessità di dotarsi di nuove evolute normative in tale ambito, è di vitale importanza che venga fornita una base condivisa e un sostegno. Piuttosto che considerare le differenze di approccio come un impedimento di armonizzazione, è preferibile concentrarsi su come tali differenze possano essere ridotte nell'obiettivo comune di un'efficace cooperazione internazionale per lo sviluppo della capacità[48] di contrasto. Ciò si sostanzia nella consapevolezza dei Governi del dovere di proteggere i diritti dei cittadini, le infrastrutture critiche e fornire a ogni agente di polizia, ogni giudice, ogni investigatore le competenze sulla gestione delle evidenze elettroniche in ogni Paese.

Secondo punto cardine dell'armonizzazione è individuabile nella condivisione di *standard tecnologici* e *protocolli operativi*. In particolare va evidenziata la convergenza della disciplina ISO/IEC 27037:2012[49] che costituisce una valida base di condivisibili procedure operative e modalità di indagini per gli informatici forensi in tema di identificazione, raccolta, acquisizione e conservazione delle prove.

Il progetto di un sistema organico di standard internazionali è in fase di sviluppo nel 2015 con il rilascio di standard relativi a quattro linee[50]:

---

[45] UNODC, *Comprehensive Study on Cybercrime*, UN, 2014.

[46] Clough, J., «A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation», *Monash University Law Review* 01/2014; 40(3), pp. 729, 2014.

[47] UNODC, *Comprehensive Study on Cybercrime*, UN, 2014.

[48] *CoE, Capacity building on cybercrime*, Consiglio di Europa, 2013; Action against Cybercrime, T-CY 14th Plenary, Consiglio di Europa, 2015.

[49] http://www.iso.org.

[50] Ferrazzano, M., *Trattamento dei reperti informatici alla luce dello standard ISO/IEC 27037: 2012*, http://www.bit4law.com/2015-03-27-trattamento-dei-reperti-informatici-alla-luce-dello-standard-isoiec-270372012, 2015.

(I) analisi delle evidenze, loro interpretazione e comunicazione dei risultati, per i processi successivi a quelli coperti dalla ISO 27037;
(II) gestione degli incidenti per la definizione dei processi di preparazione che devono venire previsti, sviluppati ed implementati, per poter effettuare in modo efficace le investigazioni in risposta ad un incidente senza pregiudicare la ripresa delle attività;
(III) valutazione dell'idoneità e adeguatezza dei metodi di investigazione per delineare le modalità di validazione di metodi e strumenti usati nelle investigazioni digitali;
(IV) principi e processi delle investigazioni per raffinare la descrizione della fasi di investigazione.

Le prime due linee si collocano rispettivamente prima e dopo i processi trattati nella ISO 27037, mentre le ultime due contengono principi trasversali da applicare a tutte le fasi. Si forma dunque un *corpus* coerente che può costituire un riferimento per la conduzione di investigazioni digitali in tutti gli ambiti, quindi non solo nei processi penali ma anche in quelli civili e nelle indagini condotte internamente nelle varie organizzazioni pubbliche o private che possono anche non finire mai davanti ad un tribunale.

Non di secondaria importanza per evitare che la cattiva scienza entri nei processi è, infine, l'*istituzione di centri specializzati* per la gestione dei reperti digitali che, anche attraverso la realizzazione di *ambienti virtuali*, remoti rispetto ai luoghi delle indagini, consentano di automatizzare alcune fasi della gestione, memorizzazione e analisi forense, inclusa l'interpretazione. Si tratta di laboratori con ampie capacità di memorizzazione dati, comunicazioni sicure, autenticazioni a diversi livelli, controllo dell'accesso basato sui ruoli, e strumenti forensi per la gestione di casi, dotati di sistemi gestiti da *ipervisori*[51] che consentono a una molteplicità di macchine virtuali di operare sullo stesso hardware ospite[52]. Il laboratorio centralizzato riduce la duplicazione delle risorse e dei compiti, fornisce agli investigatori strumenti all'avanguardia, valorizza risorse e competenze, e abbassa il costo delle analisi forensi.

Con «sistema virtualizzato» si intende un sistema informatico in cui un unico server fisico consente di emulare il funzionamento contemporaneo di più

[51] L'ipervisore è un software specializzato in grado di emulare il funzionamento contemporaneo di più server sulla stessa macchina.

[52] All'origine si collocano i lavori di Craiger P., Burke P., Marberry, C. and Pollitt, M., «A Virtual Digital Forensics Laboratory», in *Advances in Digital Forensics* IV (I. Ray and S. Sheroy eds., Springer, 2008) che riconoscono l'idea di Davis, M., Manes, G. and Shenoi, S., «A network-based architecture for storing digital evidence», in *Advances in Digital Forensics*, (M. Pollitt and S. Shenoi eds.), Springer, 2005; e, per gli hypervisor di Bates, P., «The Rising Impact of Virtual Machine Hypervisor Technology on Digital Forensics Investigations», *ISACA journal*, 2009 e Bem, D. and Huebner, E., «Computer Forensic Analysis in a Virtual Environment», *International Journal of Digital Evidence*, 6(2), 2007. Prodotti commerciali pionieristi in questo settore sono *Virtual Forensic Computing* e *Getdata Forensic Explore*r: si basano su lavori di Penhallurick, M.A di cui *Metodologies for the use of vMware to boot cloned/mounted subject hard disk image*, Digital Investigation, 2, 2005.

server, definiti come «macchine virtuali», attraverso la gestione simultanea di più sistemi operativi. Il cuore di questa architettura è l'ipervisore, o monitor delle macchine virtuali, che opera in maniera trasparente svolgendo attività di controllo e di attivazione dell'esecuzione dei programmi dei vari ambienti ospitati, allocando le risorse dinamicamente, e gestendo in maniera autonoma e relativamente semplice risorse e processi disomogenei[53]. Alle prime implementazioni di una decina di anni fa —frenate dai limiti della tecnologia e dalla difficoltà di ammissione nei dibattimenti giudiziari di evidenze raccolte in modo inconsueto— a fronte dell'avanzata globale della criminalità informatica, della disponibilità di un quadro legislativo internazionale facilitatore e delle sollecitazioni a una maggiore efficienza delle scienze forensi da parte dei Governi[54], sono seguite parecchie iniziative, che si consolidano e diffondono, per la costruzione di piattaforme condivise e di laboratori virtuali in vari settori delle scienze forensi[55] e per l'adozione di metodologie che possano essere applicate su ampia base.

I vantaggi del tempo reale nelle indagini forensi remote sono molteplici e la diffusione dell'approccio ha il potenziale di accrescere fortemente l'efficienza e l'efficacia del sistema di giustizia penale. Si pensi, per esempio, alla c.d. *live forensics* dove una disconnessione elettrica del sistema può comportare la perdita della memoria volatile che invece spesso contiene dati importanti, soprattutto nel caso di dispositivi crittati (la password di cifratura), di memorie molto estese e qualora siano state adottate tecniche di anti-forensics[56].

L'adozione di strumenti forensi di questo tipo pone però alcuni problemi: procedure legali corrette richiedono che gli strumenti utilizzati negli esami, hardware o software che siano, siano continuamente validati e, purtroppo, la maggior parte degli esaminatori non ha le competenze necessarie per eseguire tali convalide. Inoltre, a livello di sistema giustizia, vi è una quantità enorme di duplicazioni se ogni esaminatore deve validare gli stessi strumenti.

Superate a livello di *governance* le criticità descritte, tuttavia, la crescita degli ambienti di *cloud* e di virtualizzazione lascia prevedere che i laboratori di informatica forense del futuro saranno sempre più centralizzati e non limitati da confini geografici.

---

[53] I primi ipervisori sono stati progettati negli anni 80 per sistemi *mainframe*; negli ultimi dieci anni sono divenuti una *commodity* per la soluzione di problemi di sicurezza, amministrazione delle risorse e affidabilità nei sistemi distribuiti. Anche molti sistemi personali presentatano opzioni di utilizzo di un livello di virtualizzazione atto a ospitare sistemi operativi diversi da quello nativo.

[54] Cfr. il già citato Rapporto NAS, *Strengthening Forensic Science in the United States*.

[55] Il Network di Eccellenza sulla genetica forense EUROFORGEN-NoE, 2012-2017, realizza un laboratorio virtuale di genetica forense in cui partner da nove paesi —scienziati, docenti, forze di polizia, membri del sistema giudiziario— collaborano in indagini penali con riferimento a problemi di privacy e di protezione dei minori.

[56] Le tecniche di anti-forensics sono un insieme di strategie che possono essere state impiegate sul reperto informatico per mettere in difficoltà gli investigatori in modo da riuscire ad occultare il reperimento di evidenze digitali.

Le prime iniziative significative in questa direzione riguardano gli Stati Uniti, dove dal 2014 sono state attivate cooperazioni tra importanti organizzazioni[57], centrate su laboratori virtuali per rafforzare le discipline forensi (in particolare di informatica), attraverso lo sviluppo di linee guida condivise sia per determinare regole e misure sia per la verifica della fondatezza delle basi tecniche e scientifiche. Anche in risposta alle critiche del rapporto NAS, nel 2013 il *Department of Justice* degli USA ha attivato un'organizzazione per il miglioramento della affidabilità delle pratiche di indagine forense[58] con lo scopo di promuovere la qualità scientifica delle indagini, ridurre la frammentazione organizzativa, e accrescere il coordinamento federale: i laboratori virtuali hanno un ruolo strategico a fronte di questi obiettivi.

In questa ottica si ricordano anche l'esperienza olandese con l'istituzione del *Netherlands Forensic Institute* (NFI)[59] in cui si utilizzano piattaforme forensi integrate che consentono di effettuare indagini su grandi insiemi di evidenze digitali e su altri reperti oggetto di indagine scientifica (biologia, chimica, farmacologia, informatica) e permettono indagini sul campo, forniscono evidenze solide e validate e permettono indagini forensi con l'uso mirato di esperti di qualità che operano nei vari istituti collegati. Questa rivoluzione tecnico-organizzativa lascia prefigurare un cambiamento di ruolo del perito forense che acquista connotatati di sviluppatore e manutentore di ambienti virtuali forensi integrati.

Analogamente, e limitatamente all'informatica forense, in Italia, all'Università di Bologna (CIRSFID), è stato sviluppato *Virtual Forensic Ambient* (VFA)[60] un sistema versatile, scalabile e di buona usabilità indirizzato a magistrati, forze di polizia, avvocati e consulenti tecnici per consentire l'analisi forense di reperti acquisiti fisicamente in ambiente virtuale e integrato, con connessioni sicure in rete e accessi controllati. Il sistema è stato progettato per dare la possibilità a ogni attore giudiziario di poter disporre dei contenuti dei supporti informatici senza dover conoscere necessariamente le tecniche di informatica forense e senza dover utilizzare strumentazioni specialistiche. I risultati delle virtualizzazioni dei dischi e delle macchine possono essere fruibili da qualunque elaboratore connesso alla rete internet se preventivamente autorizzato. Si sottolinea che il metodo risulta veramente efficace però solo qualora vengano messe in atto le procedure informatico forensi ormai consolidate nei sistemi nord-americani, tra cui: verificare accuratamente lo stato di ogni supporto magnetico; individuare virus e altro software malevoli; ricostruire

[57] Nell'ambito del *Overseas Security Advisory Council* (OSAC), creata nel 1985 per promuovere la cooperazione su temi di sicurezza tra il Department of State degli Usa e le più grandi multinazionali americane.

[58] *National Commission on Forensic Science* (NCFS).

[59] Kloosterman, A. *et al*., «The interface between forensic science and technology: how technology could cause a paradigm shift in the role of forensic institutes in the criminal justice system», *Philosophical Transactions of the Royal Society* London, Biol. Sci., 2015.

[60] Bardari, U., *Caratteristiche innovative nell'acquisizione di dati di informatica forense in ambienti virtuali*, 2014, http://amsdottorato.unibo.it/6107.

la successione dei compiti e delle azioni; ricostruire l'attività di un accesso abusivo dalla rete; ripetere almeno due volte le analisi, ecc.

Il sistema VFA può essere impiegato efficacemente in analisi informatiche forensi di supporti digitali inerenti un procedimento giudiziario per cui si richieda una consulenza tecnica, con la partecipazione diretta della Polizia Giudiziaria e della Autorità Giudiziaria, allo scopo di rendere disponibile, sotto forma di macchine e dischi virtuali, il contenuto dei supporti sequestrati che potrà essere visionato alla pari del supporto originale. L'intera procedura consta di più fasi. Dapprima si prevede l'acquisizione dei supporti informatici sequestrati in duplice copia fisica attraverso noti strumenti d'acquisizione tramite fibra ottica. La copia fisica è realizzata in formato intellegibile e compatibile per permettere la migliore fruibilità alle parti e riversata su hard disk esterno per motivi di costo e di trasporto. Depositata la copia fisica con le dovute garanzie di ripetibilità, nella fase successiva si procede alla creazione di dischi e macchine virtuali delle copie riversate nei server del data center e l'eventuale *crack* delle password di accesso ai profili utente dei vari sistemi operativi. In questa fase vi potrebbe essere un'alterazione di una delle copie fisiche utilizzate per la virtualizzazione ma di fatto grazie a un sistema di *cache* e di *snapshots* si preserva il dato originale da tale rischio. Per rendere visibile tutto il contenuto del computer come se fosse stato acceso in un momento successivo al sequestro si ha un'alterazione di alcuni file di sistema, tuttavia possono essere preservati tutti i dati contenuti nel supporti ripristinando la *Virtual Machine* al primo avvio. Nella fase successiva si stabilisce una *Virtual Private Network* (VPN)[61] tra il data center e il personale giudiziario che sta eseguendo le indagini per consentire a chi sia preventivamente autorizzato al trattamento dati di poter visualizzare i contenuti di ogni singolo supporto. Oltre alla modalità di accesso alle informazioni in VPN, per ridurre ulteriormente le possibilità di accesso indesiderate o non autorizzate in un test specifico, viene utilizzato un sistema di rilevazione e valutazione di credenziali biometriche con l'ausilio di un apparato dedito al riconoscimento dell'iride. Rispondendo alla necessità giuridica della genuinità della prova è sempre possibile effettuare l'estrapolazione dalla copia fisica integra di quei dati che l'autorità inquirente ritenesse utile ai fini dell'indagine.

4. CONCLUSIONI

La convergenza verso una base normativa comune e protocolli operativi condivisi è rilevante per la selezione delle conoscenze scientifiche valide per uno specifico contesto[62]. Come si è ampiamente argomentato la sentenza Daubert ha

[61] Le VPN sfruttano reti pubbliche e condivise (internet) per creare canali virtuali e privati tra due soggetti.

[62] A tale proposito si sottolinea che il termine scienza forense ricomprende oggi molte discipline, ognuna delle quali con metodi e paradigmi differenti. Cfr. ad esempio alla categorizzazione

avuto il pregio di rimarcare l'autonomia del giudice in riferimento alle conoscenze scientifiche, però la riflessione che ne è scaturita ha portato a una concezione della scienza funzionale all'accertamento della verità nel processo, ovvero di una scienza riferita al *contesto* processuale[63].

Anche la formazione interdisciplinare è una strategica leva di cambiamento perché ciascuno dei due gruppi, scienziati forensi e operatori del diritto, abbia una comprensione delle necessità e dei limiti dell'altro. Gli scienziati devono far crescere la fiducia negli elementi di prova che presentano durante un procedimento, attraverso un comportamento etico[64] che escluda metodi non robusti scientificamente e il ricorso alla cattiva scienza; devono inoltre riuscire a presentare le loro conoscenze in modo coerente e comprensibile per gli operatori del diritto. D'altro canto i professionisti del diritto devono accettare e comprendere che la scienza è raramente assoluta. Tali fiducia e comprensibilità fanno intrinsecamente affidamento su un rapporto simbiotico tra la scienza e i suoi scienziati e la legge e i propri giuristi, e sul rispetto di linee guida e standard che distinguano ciò che è accettato e incontrovertibile da temi aperti al dibattito e all'approfondimento[65].

Recibido: marzo 2016; aceptado: mayo 2017

del National Institut of Justice, *Status and Needs of Forensics Science Service Providers: A Report to Congress*, 2006, in https://www.ncjrs.gov/pdffiles1/nij/213420.pdf.

[63] Così Jasanoff, *op. cit.*.

[64] Lo Russo, S., «Investigazioni scientifiche, verità processuale e etica degli esperti», in *Dir. proc.*, 2010, 1449.

[65] Black, S. e Nic Daied N., *op. cit.*