UNA GOVERNANCE INTEGRATA PER NUOVI MODELLI DELL'INFORMATICA FORENSE

RAFFAELLA BRIGHI
UNIVERSITÀ DEGLI STUDI DI BOLOGNA

i-lex

(pagina lasciata intenzionalmente vuota)

i-lex. Scienze Giuridiche, Scienze Cognitive e Intelligenza Artificiale
Rivista quadrimestrale on-line: www.i-lex.it

UNA GOVERNANCE INTEGRATA PER NUOVI MODELLI DELL'INFORMATICA FORENSE

RAFFAELLA BRIGHI

Abstract: Un piano di *governance* integrato, che comprende diversi elementi di armonizzazione, sembra condurre verso nuovi paradigmi per l'Informatica forense. Un nuovo approccio epistemologico, più attento alle fasi precedenti al processo giudiziario e alla valutazione del contesto di riferimento, 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. Anche l'istituzione di centri specializzati per la gestione dei reperti digitali — che, attraverso la realizzazione di ambienti virtuali, automatizzano alcune fasi della gestione, memorizzazione e analisi forense — rende le indagini più efficienti e limita il ricorso alla "cattiva scienza". La formazione interdisciplinare, infine, è una leva strategica per il cambiamento perché ciascuno dei due gruppi, scienziati forensi e operatori del diritto, abbia una comprensione delle necessità e dei limiti dell'altro.

Parole chiave: Informatica forense, armonizzazione, epistemologia, standard condivisi, laboratori virtuali.

1. Il dato informatico come mezzo di prova

Contestualmente ai cambiamenti che le tecnologie informatiche hanno apportato nelle attività umane, sociali e economiche – sempre più legate all'elaborazione e alla trasmissione di informazioni digitali – anche l'attività giurisdizionale si avvale sempre più di informazioni desunte dai dati conservati nei dispositivi elettronici e trasmessi attraverso le reti. Questo è avvenuto in primis per reati connessi con l'informatica: reati informatici[1], ad esempio le frodi informatiche, il

[1] Alcune importanti fattispecie di reato, legate strettamente all'informatica, sono state introdotte nel nostro ordinamento dalla legge del 23 dicembre 1993, n. 547 parzialmente modificata dalla legge 18 marzo 2008, n. 48 in attuazione della Convenzione di Budapest del 2001. Si tratta dei c.d. reati (necessariamente) informatici, ovvero reati che presentano "espressamente, sul piano della loro formulazione letterale, elementi di tipizzazione descrittivi di modalità, oggetti, attività caratterizzanti dalla, o frutto, della tecnologia informatica, vale a dire

Pubblicato il 3 Dicembre 2017

falso informatico, l'accesso abusivo, il danneggiamento di dati e sistemi informatici oppure anche reati non "necessariamente" informatici ma attuati attraverso strumenti informatici [2]. Oggi, tuttavia, è diventato necessario, in fase di indagine, porre attenzione ai dispositivi digitali anche in fattispecie di reato non inerenti l'informatica, per raccogliere da essi dati informatici dai quali trarre informazioni utili per le fasi del processo.

L'utilizzo di strumenti informatici e telematici produce tracce digitali, sotto forma di *file* prodotti dalle applicazioni installate, *file* di sistema, informazioni gestite dal sistema operativo, *log* dei dispositivi di rete e frammenti di *file* cancellati. Questi dati, spesso nascosti all'utente inconsapevole, possono essere recuperati da esperti informatici forensi in grado di desumere importanti informazioni che possono costituire fonte di prova in un processo. Il dato digitalizzato diviene dunque oggetto di indagine.

Le autorità procedenti nell'ambito della loro attività d'indagine, si avvalgono sempre più di tali dati che, una volta correttamente acquisiti e analizzati,potranno, da soli o combinati alle tradizionali modalità investigative, assumere valore di prova contribuendo significativamente all'identificazione dell'autore dell'illecito. Ciò non riguarda solo il processo penale ma è applicabile e tutti i sistemi processuali previsti dall'ordinamento.

L'Informatica forense è la disciplina che applica tecniche scientifiche e analitiche alle reti, ai dispositivi digitali e ai *file* per individuare, estrarre, elaborare conservare, dati digitali che possano

implicanti, connessi o relativi a procedimenti di elaborazione automatizzata di dati, secondo programmi informatici", in L. Picotti, *La nozione di criminalità informatica e la sua rilevanza per le competenze penali europee*, in *Riv. Trim. dir. Pen. Ec.*, Vol. 4, 2011, pp.827 ss.

[2] Reati come la pedopornografia, gli atti persecutori, la diffamazione e il bullismo trovano nella dimensione *online* nuove forme; accanto a questi le estorsioni, sempre più diffuse nella modalità di *sextorsion* e *ransomware*, i reati di sostituzione di persona o lo spionaggio coniugano fattispecie tradizionali con reati nati digitali, andando a incrementare, secondo una concezione più ampia e elastica, il perimetro dei c.d. *computer crime.* Il quadro giuridico, molto vario e di difficile ricostruzione, ricomprende tentativi di adeguare fattispecie esistenti a nuove realtà tecnologiche, tentativi di applicare vecchie fattispecie a condotte che avvengono online, e interventi d'urgenza in reazione a gravi fatti di criminalità (uno tra tutti la modifica all'art. 612 bis c.p. in tema di *cyberstalking*)

essere valutati come prova nel procedimento. Nel farlo risponde alle esigenze di rigore tecnico e metodologico in attuazione delle norme giuridiche di riferimento e individua le pratiche migliori per la gestione della prova informatica[3].

Nel cyberspazio, senza frontiere fisiche e politiche, essa ha un ruolo di rilievo nell'affrontare difficoltà intrinseche alla ricostruzione di reati globali. Quando si svolgono indagini sul cybermondo – come l'intercettazione di email, o indagini sulla violazione della proprietà intellettuale[4] – si incontrano numerosi tipi di problemi, che possono essere ricondotti a una tassonomia di base.

– Il problema della *locazione* ovvero dell'individuazione della posizione fisica di un sospettato, con le implicazioni giurisdizionali che ne conseguono; si pensi per esempio ai casi in cui una stessa prova lasci traccia in paesi diversi e alla distinzione tra dati statici acquisiti mediante perquisizioni e dati in transito acquisiti mediante intercettazioni.
– Il problema dell'*integrità* che riguarda il rischio di modificabilità dei dati originali e dei metadati minando *ab origine* il valore probatorio del materiale acquisito (ad esempio data e ora);le modalità con cui tali operazioni vengono condotte creano ulteriori

[3] Si richiama l'approccio definitorio e metodologico che della disciplina sviluppa Cesare Maioli: «gli scopi dell'informatica forense sono di conservare, identificare, acquisire, documentare e interpretare i dati presenti su un computer. A livello generale si tratta di individuare le modalità migliori per: - acquisire le prove senza alterare o modificare il sistema informatico su cui si trovano; - garantire che le prove acquisite su altro supporto siano identiche a quelle originarie; - analizzare i dati senza alterarli. In sintesi, di "dare voce alle prove". L'informatica forense comprende le attività di verifica dei supporti di memorizzazione dei dati e delle componenti informatiche, delle immagini, audio e video generate da computer, dei contenuti di archivi e basi dati e delle azioni svolte nelle reti telematiche». In particolare si veda: C. Maioli, *Dar voce alle* prove: elementi di informatica forense, in Crimine virtuale, minaccia reale, Franco Angeli, 2004 e C. Maioli, *Introduzione all'informatica forense*, in *La sicurezza preventiva dell'informazione e della comunicazione,* a cura di P. Pozzi, Franco Angeli, 2004. Per un approfondimento sulle principali frontiere dell'Informatica forense si veda anche C. Maioli (a cura di), *Questioni di Informatica forense*, Aracne, 2015 e A. Gammarota, *Informatica forense e processo penale: la prova digitale tra innovazione normativa e incertezza giurisprudenziali* (tesi di dottorato), 2016.

[4] A. Gammarota, *Un caso di informatica forense: danneggiamento di un sistema informatico della Pubblica Amministrazione*, in *Crimine virtuale, minaccia reale*, Franco Angeli, 2004, p.207 e ss.

problemi rappresentati dalla mancanza di procedure uniformi e dal diverso trattamento delle *digital evidence* da parte delle legislazioni dei vari Paesi.

– Il problema della *viscosità*: molte copie degli stessi file sono create e memorizzate durante i processi di trasmissione. In generale la viscosità dei dati è un elemento a favore degli investigatori; viceversa, la percezione che i dati provenienti da fonti TIC siano soggetti al rischio di alterazione può essere di aiuto per l'accusato, laddove possano essere sollevati dubbi sull'esistenza stessa e/o il loro valore forense.
– Il problema *del tipo di dati*: oltre al problema della codifica e interpretazione già illustrato nei capitoli precedenti e chi si riflette naturalmente anche nella difficoltà di trarre informazione a partire dai dati informatici acquisiti dai dispositivi digitali se non se ne conosce il senso, vi è anche il problema della compresenza negli spazi virtuali di informazioni che nulla hanno a che fare con il fatto per il quale si procede o, nella più delicata delle ipotesi, siano dati sensibili che riguardano persone estranee ai fatti.
– Il problema della *tracciabilità,* dovuto all'esistenza di molteplici fonti, tra cui dati che l'indagato ha utilizzato o a lui riconducibili a seguito della sua attività, dati creati a seguito dell'utilizzo di un sistema di comunicazione da parte di un sospettato, contenuti delle attività di comunicazione di una persona. In particolare il problema consiste nell'identificare fonte e destinazione facendo riferimento a identificazioni univoche e l'abilità di risalire da un indirizzo IP al soggetto che concretamente pone in essere la navigazione dipendente da input che provengono da più entità e dall'esistenza di vari log e/o registrazioni.
– E, non da ultimo, il problema dell'*analisi* di grandi volumi di dati eterogenei, con limiti dovuti a meccanismi di protezione, limiti di spesa e di tempo richiesti dalla legge.

La natura, spesso intangibile e volatile dei dati digitali, rende il processo di investigazione e raccolta dei dati a fini probatori soggetto a rischio di malfunzionamenti tecnici danneggiamenti o contraffazioni e quindi estremamente pericoloso per i diritti delle parti. Le tracce digitali sono fragili, cioè facilmente modificabili e deteriorabili se i dispositivi che le contengono sono maneggiati in

modo inappropriato[5], occorre inoltre saper valutare il quadro di insieme perché il dato sia fonte di prova.

Proprio nell'ottica della dimensione transnazionale dei reati informatici e delle relative indagini gli interventi normativi sul nostro Codice di Procedura Penale da parte della legge di ratifica della Convenzione di Budapest sul *cybercrime* richiamano frequentemente la necessità di adottare «misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

I dati acquisiti devono essere vagliati in dibattimento da tutte le parte del processo - normalmente a distanza di tempo – e, se non si adottano le misure tecniche opportune, l'attività di acquisizione diventa vana e difficilmente ripetibile; la prospettiva dell'attività tecnica è dunque quella della *utilizzabilità* in dibattimento**,** a disposizione delle parti processuali. Il legislatore, a tale proposito, non indica un metodo migliore di altri (*best practices*) per l'individuazione, l'acquisizione e la salvaguardia delle prove digitali, il che è anche comprensibile vista la pericolosità di una disciplina cristallizzante applicata a una scienza in rapida evoluzione quale l'informatica.

Il trattamento della prova digitale si dipana all'interno di tutte le fasi più importanti dell'attività tecnica organizzativa: dall'individuazione e acquisizione delle prove alla loro analisi, valutazione e conservazione.

In questo iter un corretto approccio metodologico, in primis, impone di assicurare un'acquisizione completa, che significa prendere il dato nel suo contesto[6]. Anche per questo, l'individuazione dei reperti deve avvenire nel tempo più prossimo all'accadere dell'evento di interesse. Devono poi essere garantite l'integrità dei dati acquisiti e dimostrata la paternità del dato, per questo si impiegano tecniche per "congelare"(*freezing*) le memorie di massa (per esempio copia forense o copia *bit stream*) e strumenti quali l'*hash* e la firma digitale. Un

[5] Per esempio: l'accensione di un computer spento comporta la scrittura e/o modifica di numerosi file sul disco; l'esplorazione del contenuto di un hard-disk comporta la modifica di varie proprietà importanti dei file (ora e date ultimo accesso; lo spegnimento di un computer determina la perdita di fonti di prova contenute nella memoria volatile.

[6] Una singola mail, per esempio, può essere stata alterata e contraffatta, occorre dunque valutare anche le tracce che la stessa mail ha lasciato sui mail server.

corretto approccio metodologico impone inoltre di salvaguardare la verificabilità delle procedure poste in essere e la riproducibilità delle operazioni compiute sui reperti a garanzia dei diritti di tutte le parti (*accountability*). Questo può avvenire, per esempio, con l'accortezza di utilizzare software a codice aperto per consentirne lo studio e non sono il *testing*. A fronte di queste esigenze, l'attività di informatica forense si sviluppa secondo un continuo dovere di documentare ogni fase del procedimento con il paradigma della catena di custodia ovvero una documentazione cronologica che permetta di tracciare (e protocollare) il percorso completo compiuto dalla prova dalla fase dell'individuazione fino ad arrivare al dibattimento, in modo tale da garantirne la limpidezza e l'integrità.

2. Crisi delle scienze forensi

Numerosi studi e report governativi, non troppo risalenti nel tempo, hanno denunciato la crisi delle discipline forensi[7]. 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[8].

Il documento, ampio e articolato, 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

[7] 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 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.

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

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 e-saminatori o ancora alla standardizzazione delle procedure.

Queste criticità riguardano anche l'Informatica forense. In un articolo molto citato del 2006 Bhaskar[9] preconizzava che "Cyber Katrina" – una sorta di versione *cyber* dell'uragano Katrina – aleggiava sulle reti informatiche degli Stati Uniti, minacciando di travolgere con una alluvione di presunti reati informatici, e la conseguente moltitudine di reperti da analizzare, qualsiasi piano di sicurezza delle autorità statunitensi. Tali piani, focalizzati solo su risposte tecniche, secondo l'autore non prendevano infatti in adeguata considerazione le esigenze e i principi dell'informatica forense. Molteplici le vulnerabilità evidenziate: dalla grave carenza nella preparazione del personale investigativo per le indagini forensi (in particolare sul profilo giuridico), alle risorse limitate e, non ultimo, alle procedure investigative poco efficienti e sviluppate in modo disarmonico. Vi è la falsa convinzione che la tecnologia informatica garantisca di per sé l'affidabilità dei dati oggetto delle elaborazioni dalla quale deriverebbero informazioni incontrovertibili. Spesso il solo fatto che un dato sia stato registrato da un dispositivo elettronico lo rende in grado, anche agli occhi degli operatori del settore, di rappresentare all'evidenza i fatti di reato da accertare e provare. La carenza di preparazione adeguata rispetto ai meccanismi di funzionamento della tecnologia digitale inasprisce difficoltà intrinseche nella disciplina[10].

Anche se probabilmente alcune criticità sono legate a una certa resistenza al cambiamento[11], aspetto comune a tutti i punti sollevati dal rapporto NAS e dagli altri documenti ufficiali è la creazione di una adeguata *governance*. A fronte dei progressi degli ultimi anni, si

[9] R. Bhaskar, *State and local law enforcement is not ready for a cyber Katrina*, Communications of the ACM, 2006, Vol. 49 (2), pp. 81–83.

[10] In argomento A. Gammarota *Cit*., G. Vaciago, *Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Giappichelli, 2012, Monti, A., *Attendibilità dei sistemi di computer forensic*, in *ICT-Security*, Vol. 9, 2003 (disponibile on line: http://www.ictlex.net/?p=287, p. 2.

[11] P. C. Giannelli, *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.

può affermare che sia effettivamente in atto un cambio di paradigmi. Molti fattori fanno pensare che si stiano gettando le basi per una nuova visione dell'informatica forense, e più in generale, delle scienze forensi. 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.

3. Epistemologia ed informatica forense

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.

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"[12] – 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[13] e che la caratteristica di fondarsi su metodi

[12] D. Caccavella, *Le perizie informatiche: Gli Accertamenti tecnici in ambito informatico e telematico*, in S. Aterno, P. Mazzotta (a cura di), *La perizia e la consulenza tecnica*, Cedam 2006.

[13] Cfr. T. Kuhn, *The Structure of Scientific Revolutions*, 1962. 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; 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

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[14], 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[15]. Per definire una cornice concreta per tutte quelle «procedure e pratiche che danno struttura agli sforzi giuridici di determinare la verità»[16] serve infatti comprendere la natura dell'evidenza scientifica e come essa si rapporta al concetto giuridico di prova, 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[17], nel contesto giuridico è un proble-

---

teorie scientifiche "costruiscano il mondo".

[14] 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, utilizza una legge scientifica per accertare un fatto "ignoto" per il giudice», così P. Tonini, *Progresso tecnologico, prova scientifica 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,* 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.

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

[16] S. Haack, *Op.cit*, p. 41.

[17] 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

ma non nuovo ma centrale anche per l'informatica forense. 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*[18] del 1993 che ha rappresentato per la giurisprudenza non solo americana, un punto fermo nel dibattito sulla prova scientifica.

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[19]. Nello stabilire quale sia la scienza valida, il diritto non è più meramente norma tecnica ma contribuisce a definire il sapere scientifico[20].

Da molte parti si è affermato che la sentenza Daubert non abbia raggiunto il suo obiettivo e piuttosto abbia creato molte controversie in fase di applicazione[21], 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

---

competenze dell'esperto e la determinazione dell'oggetto dell'incarico influiscono chiaramente sull'attendibilità del risultato.

[18] Daubert vs. Merrel Dow Pharmaceuticals, 509 U.S. 579 (1993). Trad. it parziale in *Riv. trim. dir. proc. civ.*, Vol. L, 1996, pp. 277 e ss.

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

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

[21] S. Haack S., *Prova ed errore: la filosofia della scienza della Corte suprema americana* in *Ars Interpretandi*, Vol. 11, 2006, pp. 303-326. Si veda anche J. Peter Neufeld, *The (Near) Irrelevance of Daubert to Criminal Justice and Some Suggestions for Reform* in *American Journal of Public Health,* Vol. 95, No S1,2005; K. R. Berman, N. McClennen, "Daubert Turning 20: Junk Science Replaced By Junk Rulings?", 2012, in *ABA Section of Litigation Annual Conference*, 2012.

la *junk science*[22] – la cattiva scienza, la scienza spazzatura – costituita da quelle conoscenze che, se pur presentate come scientificamente testate, sfuggono da qualunque valutazione di scientificità.

Il dibattito più recente muove dunque dall'obiettivo di definire una epistemologia per il diritto partendo piuttosto da ciò che già è implicito nella giurisprudenza e dalle procedure di armonizzazione e standardizzazione in via di definizione.

Questo cambio di paradigma[23] non può avveniretuttavia con la sola definizione di norme giuridiche e protocolli operativi per le varie scienze forensi. 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 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 rielaborarne 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 cri-

[22] È celebre la distinzione tra *good science* e *junk science* in P. Huber., *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.

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

teri per la validazione del sapere scientifico non consolidato[24]. In Italia è la sentenza della Cassazione penale 43789/2010 che affronta esplicitamente la questione.

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[25]. 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.

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[26].

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

---

[24] Tra le numerose fonti si veda O. Sallavaci O., *The Compact of scientific evidence on criminal trial*, Routledge, 2014. In Italia è la sentenza della Cassazione penale 43789/2010 che affronta esplicitamente la questione. Cass. pen., sez. IV, 17 settembre 2010, n. 43786

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

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

comune di contrasto al crimine informatico e con la condivisione di protocolli operativi e standard tecnologici.

4. Armonizzazione giuridica

La prima leva di armonizzazione, guida del cambio di paradigma, va individuata senza dubbio nella definizione di un *quadro giuridico sovranazionale comune* e nella riformulazione delle norme processuali tenendo conto delle innovazioni tecnologiche.

È generalmente accettato che un certo grado di armonizzazione tra i paesi sia 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 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*[27] del Consiglio di Europa[28], 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 il-

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

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

leciti 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[29].

Va notato come la Convenzione allarghi le disposizioni a qualunque reato in cui sia necessario raccogliere elementi probatori in formato elettronico[30]: 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.

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[31]. 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 stra-*

---

[29] M. Gercke, *10 Years Convention on Cybercrime*, *Computer Law Review International*, Vol. 12(5), 2011, pp. 142-149.

[30] M. A. Vatis, *The Council of Europe Convention on Cybercrime* in Proc. of a Workshop on *Deterring Cyber Attacks: Informing Strategies and Developing Options* for U.S. Policy, National Academies Press, 2010.

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

tegy[32] 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[33]. 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 *cyber crimine* e ha collaborato con altre commissioni delle Nazioni Unite[34] 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 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[35].

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"[36]. L'ideale che tutti gli Stati

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

[33] N. Di Noto, *Europe's fight against cybercrime*, in *The ReSHAPE Research Project*, Vol. 5, 2013.

[34] U. N. Crime Prevention and Criminal Justice.

[35] UNODC, Comprehensive Study on Cybercrime, UN, 2014.

[36] J. Clough, *A World of Difference: The Budapest Convention on Cybercrime*

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[37] 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[38] 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.

5. Standard internazionali, protocolli operativi e laboratori centralizzati

Ciò che può essere senza dubbio utile nell'interazione tra informatica e diritto è l'adozione di standard che evitino di canonizzare specifiche scelte tecnologiche e al contempo individuino una base condivisibili di procedure operative e modalità di indagini per gli informatici forensi. Questo si è raggiunto con la convergenza verso gli standard ISO/IEC[39] per il trattamento dei dati digitali, internazionali e del tutto autonomi e indipendenti rispetto ai singoli ordinamenti giuridici e in particolare la ISO 27037:2012 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.

Alla ISO 27037, ormai consolidata, si è recentemente aggiunto, nel 2015, un sistema organico di standard internazionali che copre ulte-

and the Challenges of Harmonisation, in *Monash University Law Review*, Vol. 40(3), 2014, p.729.

[37] UNODC, Comprehensive Study on Cybercrime, UN, 2014.

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

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

riori aspetti fondamentali, secondo quattro direzioni:[40] 1) gestione degli incidenti per la definizione dei processi di preparazione che devono venire previsti, sviluppati e implementati, per poter effettuare in modo efficace le investigazioni senza pregiudicare la ripresa delle attività; 2) analisi delle evidenze, loro interpretazione e comunicazione dei risultati, per i processi successivi a quelli coperti dalla ISO 27037; 3) valutazione dell'idoneità e dell'adeguatezza dei metodi e degli strumenti di investigazione per delinearne le modalità di validazione; 4) 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. Tra tutte di particolare interesse sono: la ISO 27041:2015, sui meccanismi per garantire che i metodi e i processi utilizzati nelle indagini siano andati allo scopo; la ISO 27042:2015, per l'analisi e l'interpretazione delle prove digitali affrontando problemi di continuità, validità e ripetibilità e la ISO 27043:2015 per la definizione dei principi generali su cui si compone una investigazione[41].

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 a un tribunale.

Non di secondaria importanza per evitare che la cattiva scienza entri nei processi è, inoltre, 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*[42] che

[40] M. Ferrazzano M., Indagini forensi in tema di scambio di file pedopornografici mediante software di file sharing a mezzo peer-to-peer, http://amsdottorato.unibo.it/6697, 2014.

[41] Tali standard sono dettagliatamente documentati dalla organizzazione ISO sul sito www.iso.org.

[42] L'ipervisore è un software specializzato in grado di emulare il funzionamento

consentono a una molteplicità di macchine virtuali di operare sullo stesso hardware ospite[43]. 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 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[44].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[45], sono seguite parecchie iniziative, che si consolidano e diffondono, per la costru-

contemporaneo di più server sulla stessa macchina.

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

[44] 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.

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

zione di piattaforme condivise e di laboratori virtuali in vari settori delle scienze forensi[46] 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[47].

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.

6. 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. Come si è ampiamente argomentato la sentenza Daubert ha avuto il pregio di rimarcare

[46] 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.

[47] 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.

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[48].

L'apporto dell'Informatica forense a tutte le fasi del processo sembra oggi in fase di consolidamento a fronte delle iniziative di armonizzazione giuridica, ma anche di un rigore scientifico e tecnologico che si sta costruendo alla base della disciplina, e non da ultimo grazie a un approccio epistemologico più vicino al sistema giustizia che riguarda più in generale il ricorso a tutte le scienze forensi.

Nel quadro delineato non si deve trascurare la formazione interdisciplinare, 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[49] 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[50].

Per concludere occorre riflettere sul fatto che mentre negli USA l'iter formativo, selettivo e professionalizzante dei *digital forenser* ormai standardizzato in quanto muove da percorsi accademici ad hoc, in Italia non esistono corsi di laurea o specializzazioni specifiche in Informatica forense, ma non esiste nemmeno uno specifico albo degli Informatici né sono previsti presso i Tribunali e Corti d'Appello, e-

[48] Così Jasanoff, *op. cit*..

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

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

lenchi o sezioni dedicati alla specifica figura dell'esperto di Informatica[51].

Per la stesura di questo contributo sono particolarmente grata a Cesare Maioli, a Antonio Gammarota e a Michele Ferrazzano per il loro supporto continuo, i materiali e gli stimoli.

Riferimenti bibliografici

P. Bates, *The Rising Impact of Virtual Machine Hypervisor Technology on Digital Forensics Investigations*, *ISACA journal*, 2009.

E. Huebner, *Computer Forensic Analysis in a Virtual Environment*, *International Journal of Digital Evidence*, Vol. 6(2), 2007.

K. R. Berman, N. McClennen,*"Daubert Turning 20: Junk Science Replaced By Junk Rulings?"*, 2012, *ABA Section of Litigation Annual Conference*, 2012.

R. Bhaskar, *State and local law enforcement is not ready for a cyber Katrina*. Communications of the ACM, 2006, Vol. 49(2).

S. Black, N. Nic Daied, *Time to think differently: catalysing a paradigm shift in forensic science*, in *Philosophical Transactions of the Royal Society* London, Biol Sci., 2015.

D. Caccavella, *Le perizie informatiche: Gli Accertamenti tecnici in ambito informatico e telematico*, in S. Aterno, P. Mazzotta (a cura di), *La perizia e la consulenza tecnica*, Cedam 2006.

F. Cajani, *Il vaglio dibattimentale della digital evidence*, in *Archivio Penale,* Vol.LXV(3), 2013, pp. 837-852.

J. Clough, *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation*, *Monash University Law Review*, Vol. 40(3), 2014, p.729.

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

[51] A. Gammarota, E. D. Caccavella, *L'Informatica forense per l'E-Health*, in: Strumenti, diritti, regole e nuove relazioni di cura. Il paziente europeo protagonista nell'eHealth, Giappichelli, 2015, pp. 205 – 220.

P. Craiger, P. Burke, M. Marberry C. Pollitt, *A Virtual Digital Forensics Laboratory*, in *Advances in Digital Forensics* IV (I. Ray and S. Sheroy eds., Springer, 2008.

Daubert vs. Merrel Dow Pharmaceuticals, 509 U.S. 579, 1993. Trad. it parziale in *Riv. trim. dir. proc. civ.*, Vol. L,1996, pp. 277 ss.

M. Davis, G. Manes and S. Shenoi, *A network-based architecture for storing digital evidence*, in *Advances in Digital Forensics*, (M. Pollitt and S. Shenoi eds.), Springer, 2005.

N. Di Noto, *Europe's fight against cybercrime*, The ReSHAPE Research Project, Vol. 5, 2013.

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

M. Ferrazzano, *Indagini forensi in tema di scambio di file pedopornografici mediante software di file sharing a mezzo peer-to-peer*, http://amsdottorato.unibo.it/6697, 2014.

S. Fuselli, *Apparenze. Accertamento giudiziale e prova scientifica*, FrancoAngeli, 2008.

A. Gammarota, E. D. Caccavella, *L'Informatica forense per l'E-Health*, in: Strumenti, diritti, regole e nuove relazioni di cura. Il paziente europeo protagonista nell'eHealth, Giappichelli, 2015, pp. 205 – 220.

A. Gammarota, *Informatica forense e processo penale: la prova digitale tra innovazione normativa e incertezza giurisprudenziali* (tesi di dottorato), 2016.

A. Gammarota, *Un caso di informatica forense: danneggiamento di un sistema informatico della Pubblica Amministrazione*, in: Crimine virtuale, minaccia reale, FrancoAngeli, 2004.

M. Gercke, *10 Years Convention on Cybercrime*, *Computer Law Review International,* Vol. 12(5), 2011, pp. 142-1499.

P. C. Giannelli, *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.

S. Haack "Prova ed errore: la filosofia della scienza della Corte suprema americana" in *Ars Interpretandi*, Vol. 11, 2006.

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

P. Huber, *Galileo's Revenge: Junk Science in the Courtroom.* BasicBooks, (HarperCollins), 1991.

S. Jasanoff, *La scienza davanti ai giudici. La regolazione giuridica della scienza in America*, Milano, 2001.

T. Kuhn, *The Structure of Scientific Revolutions*, 1962.

S. Lo Russo, *Investigazioni scientifiche, verità processuale e etica degli esperti*, in *Dir. proc*., Vol.11, 2010.

C. Maioli (a cura di), *Questioni di Informatica forense*, Aracne, Roma, 2015.

C. Maioli, *Dar voce alle* prove: elementi di informatica forense, in Crimine virtuale, minaccia reale, Franco Angeli, Milano, 2004.

C. Maioli, *Introduzione all'informatica forense*, in *La sicurezza preventiva dell'informazione e della comunicazione,* a cura di P. Pozzi, Franco Angeli, Torino, 2004.

A. Monti, *Attendibilità dei sistemi di computer forensic*, «ICT-Security», 9, 2003 (disponibile on line: http://www.ictlex.net/?p=287)

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.

National Research Council, National Academy of Sciences,*Strengthening Forensic Science in the United States:A Path Forward*. Washington, D.C.: National Academies Press, 2009.

P.J. Neufeld, "The (Near) Irrelevance of Daubert to Criminal Justice and Some Suggestions for Reform" in *American Journal of Public Health*, Vol. 95, 2005.

L. Picotti La nozione di criminalità informatica e la sua rilevanza per le competenze penali europee. *Riv. trim. dir. pen. ec.,* Vol.4, pp. 827 ss, 2011.

O. Sallavaci, *The Compact of scientific evidence on criminal trial*, Routledge, 2014.

A. Seger, *The cost of cybercrime - the benefits of cooperation*, in *CTO cybersecurity Forum*, Forum, CoE, 2013.

M.C. Tallachini, *Scienza e diritto. Verso una nuova disciplina*, in S. Jasanoff, *La scienza davanti ai giudici. La regolazione giuridica della scienza in America*, Giuffrè, 2001.

Taruffo, *La prova dei fatti giuridici,* Giuffrè, 2002

P. Tonini, *Progresso tecnologico, prova scientica e contrattaditorio*, in L. De Cataldo Neuburger (a cura di), *La prova scientifica nel processo penale*, CEDAM, 2007

UNODC, *Comprehensive Study on Cybercrime*, UN, 2014.

G. Vaciago, *Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Giappichelli, 2012.

M. A. Vatis, *The Council of Europe Convention on Cybercrime* in Proc. of a Workshop on *Deterring CyberAttacks: Informing Strategies and Developing Options* for U.S. Policy, National Academies Press, 2010.