Archivio Penale
settembre–dicembre 2013 fascicolo 3 anno LXV
ISBN 978-88-548-6177-0
DOI 10.4399/97888548617705
pag. 821–836

Le *malpractices* nella *digital forensics*

Quali conseguenze sull'inutilizzabilità del dato informatico?

Filippo Giunchedi

1. La *computer forensics* e la nottola di Minerva. La constatazione che oggigiorno il *personal computer* e, soprattutto, gli *embedded system* costituiscono il "centro motore"[1] per la gestione dei propri interessi, il principale contenitore di frammenti di vita e di dati sensibili, spostamenti e contatti di ognuno di noi[2], porta a variegate conseguenze: dalla necessità di salvaguardare la *privacy* alle garanzie necessarie da porre alla base di un accertamento penale fondato sull'apprensione ed elaborazione di dati digitali[3], i quali tracciano fedelmente i vari passaggi di una condotta[4]. È questa la ragione per cui la letteratura[5] sconsiglia di circoscrivere l'impatto delle tecnologie informatiche ai soli *computer crimes*, posto che proprio la centralità nell'universo quotidiano di ognuno di noi passa sempre più spesso dall'interazione con un *computer*[6].

Logica conseguenza di questa "rivoluzione" nel processo penale, è la necessità di adeguare la metodologia delle indagini alle informazioni digitali, la cui natura giuridica continua a mantenere contorni non completamente definiti[7].

1. Lupária, Computer crimes *e procedimento penale*, in *Trattato di procedura penale*, diretto da Spangher, *Modelli differenziati di accertamento*, a cura di Garuti, Torino, 2011, pp. 374 ss. V., anche, Daniele, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, 283.

2. Si tratta della *information and communication technology* che ha portato, di pari passo, allo sviluppo della *computer forensics*.

3. V., per le ricche informazioni, il lavoro di Mattiucci, *Le indagini sui reperti invisibili*. High tech crime, in *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienze*, a cura di Curtotti, Saravo, Torino, 2013, pp. 707 ss.

4. Meno facilmente, invece, rilasciano elementi utili per poter individuare l'effettivo responsabile, posto che l'universo digitale consente abbastanza agevolmente di crearsi credenziali artificiose.

5. Si vedano, tra le tante, le considerazioni di Orlandi, *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc.*, 2009, 129.

6. Molto efficace risulta il richiamo alla locuzione « *old wine in new bottles* » effettuata da Lupária, *Processo penale e scienza informatica: anatomia di una trasformazione epocale*, in Lupária, Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007, p. 131.

7. Daniele, *Il diritto al preavviso della difesa nelle indagini informatiche*, in *Cass. pen.*, 2012, 441.

Se gran parte delle informazioni relative ad un reato, informatico o comune, sono potenzialmente in grado di "transitare" dal mondo digitale[8], è divenuto di fondamentale importanza adeguare le tecniche investigative alle "nuove" fonti — la c.d. fonte di prova digitale —, mediante una specifica preparazione tecnologica e l'apprestamento, per via legislativa, di un reticolo normativo tale da disciplinare la materia[9], considerato che è inevitabile preconizzare una sempre maggiore diffusione della *digital evidence* nel mondo giuridico[10].

L'irrompere nell'accertamento penale di queste metodologie, oltre che porsi in stridente antitesi con i paradigmi del giusto processo ed in particolare della formazione della prova in dibattimento[11], impegna l'interprete in un dibattito simile a quello che già qualche anno fa vide impegnata dottrina e giurisprudenza in ordine al prepotente ingresso della "prova scientifica" con il conseguente problema, tra gli altri, di arginare la *junk science* e il materiale probatorio inquinato[12].

Di fronte ad un tecnicismo così esasperato e condizionante l'accertamento, tale da parlare di una vera e propria deriva tecnicista, il processo penale assume sempre più le sembianze della nottola di Minerva, e, per evitare di perdere la propria identità, deve aggrapparsi ai diritti fondamentali[13] in

8. Di recente Corte eur. dir. uomo, Sez. I, 3 luglio 2012, Robathin c. Austria, ha fissato i parametri per stabilire quando le indagini informatiche violano il diritto alla riservatezza.

9. Ci si riferisce alla l. 18 marzo 2008, n. 48, recante « *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno* ». A commento della legge v., *inter alios*, *Sistema penale e criminalità informatica. Profili sostanziali e processuali della Legge attuativa della Convenzione di Budapest sul* cybercrime *(l. 18 marzo 2008, n. 48)*, a cura di Lupária, Milano, 2009.

10. Per imprescindibili premesse alla materia si rinvia a Ziccardi, *Scienze forensi e tecnologie informatiche*, in Lupária, Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, cit., pp. 3 ss.

11. Sulle garanzie del giusto processo in riferimento alla prova informatica, Tonini, *Documento informatico e giusto processo*, in *Dir. pen. proc.*, 2009, 405 s. Sui paradossi dell'incedere dell'accertamento penale sotto l'egida del codice Vassalli, sia consentito rinviare alle considerazioni generali contenute in Giunchedi, *I principi, le regole, le fonti*, in *Procedura penale*, a cura di Gaito, Milano, 2013, p. 6.

12. È questa l'ortodossa chiave di lettura per non ricadere nei deragliamenti interpretativi conseguenti alla nota sentenza della Corte Suprema degli Stati Uniti *Daubert v. Merrel Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 113 S. Ct. 2786 (1993), tradotta in Stella, *Leggi scientifiche e spiegazione causale del diritto penale*, II ed., Milano, 2000, pp. 424 ss., dalla quale emerge che le prove addotte dagli esperti possono essere importanti, ma anche del tutto fuorvianti, a causa delle difficoltà nel valutarle. In considerazione di questo rischio, il giudice deve esercitare un controllo maggiore sugli esperti che non sui normali testimoni; il suo compito, pertanto, è — secondo la terminologia utilizzata dalla corte statunitense — quello di *gatekeeper*. Sul punto la letteratura è sterminata. Tra i tanti senza pretesa di completezza, v. gli approfondimenti di Centonze, *Scienza "spazzatura" e scienza "corrotta" nelle attestazioni e valutazioni dei consulenti tecnici nel processo penale*, in *Riv. it. dir. proc. pen.*, 2001, 1232 ss.; Dominioni, *La prova penale scientifica. Gli strumenti scientifico–tecnici nuovi o controversi e di elevata specializzazione*, Milano, 2005, pp. 137 ss.

13. È quanto auspica Lupária, *La ricerca della prova digitale tra esigenze cognitive e valori costituzionali*, in Lupária, Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso*

assenza dei quali il rischio di un « *processo come laboratorio scientifico, affidato ad asettici operatori in camice bianco* »[14], rischia di divenire realtà.

Solo se si riuscirà a non farsi ammaliare dalle sirene di indagini *prêt à porter* basate sul solo dato digitale, ma si recupereranno gli *essentialia* del processo legale, si potrà disporre di un'informatica forense allineata ai parametri costituzionali.

Sono queste le premesse da cui muovere per indagare sulle ricadute dell'utilizzo dei protocolli nel campo della prova digitale.

2. Il volo di Icaro. Le insidie degli accertamenti in campo digitale. L'immaterialità, la fragilità e l'elevato rischio di contaminazione dei reperti digitali costituiscono le criticità che devono superare gli operatori del sistema giuridico i quali oggigiorno, in considerazione della penetrante diffusione di strumenti di gestione automatica dei dati[15], non possono più eludere l'importanza che va assumendo nelle indagini il patrimonio gnoseologico generato da apparati digitali[16].

Questa realtà virtuale, di non facile gestione, sconta un'altra serie di limiti di natura investigativa poiché gli strumenti impiegati sono esposti ad una costante evoluzione, tale da rendere ben presto obsolete e inefficaci le tecniche utilizzate. Per tutte queste ragioni agli investigatori è richiesta l'adozione di determinate cautele dettate da procedure standardizzate elaborate dalla comunità scientifica internazionale e un aggiornamento tecnico–scientifico continuo, proprio per stare al passo con l'incedere tecnologico.

Se questo è lo stato dell'arte a livello internazionale, volgendo lo sguardo all'interno delle mura domestiche, la situazione risulta allarmante posto che non è stato raggiunto un livello adeguato di preparazione[17]. I tecnici — periti e consulenti di parte — si sono limitati a federarsi in organizzazioni per poter fruire della circolarità di informazioni, mentre, a livello internazionale, grandi comunità scientifiche e di polizia operano alacremente[18]. Nonostante ciò nessuno *standard* procedurale è stato raggiunto, cosicché le innumerevo-

scientifico e garanzie fondamentali, cit., pp. 141 ss.

14. Amodio, *La rinascita del diritto delle prove penali. Dalla teoria romantica della* intime conviction *al recupero della legalità probatoria*, in Id., *Processo penale, diritto europeo e* common law*: dal rito inquisitorio al giusto processo*, Milano, 2003, p. 128.

15. Per Mattiucci, *Le indagini sui reperti invisibili*. High tech crime, cit., p. 707, talvolta « *costituiscono loro stessi "la scena del crimine"* ».

16. Il che impone di interpretare differentemente il *computer*, ossia in un'ottica investigativa. Per approfondimenti non possibili in questa sede si rinvia alla preziosa opera di sintesi effettuata da Ziccardi, *Aspetti informatico–giuridici della fonte di prova digitale*, in Lupária, Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, cit., 52 ss.

17. Mattiucci, *Le indagini sui reperti invisibili*. High tech crime, cit., p. 708.

18. Una ricca panoramica delle procedure *standard* utilizzate a livello internazionale e nazionale è contenuta nel volume curato da Lupária, Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, cit., spec. parte I, capp. IV–VII.

li informazioni alimentano una messe di procedure provenienti da diverse realtà. E a ciò si aggiunga che, utilizzando *tool*[19] di diverse ditte, anche lo strumentario tecnico impiegato si differenzia con evidenti disomogeneità sul piano dei risultati dell'accertamento. Se poi si aggiunge il ritardo con cui il nostro legislatore ha disciplinato una materia particolarmente delicata che, in tal modo, è stata lasciata in balìa dei tecnici, anch'essi operanti in regime di anarchia, si comprendono le ragioni di indagini di *digital forensics* scarsamente controllate e garantite e quindi non adeguatamente attendibili sul piano probatorio[20].

Sotto un profilo prettamente tecnico la *digital forensics* costituisce l'evoluzione della *computer forensics*. Quest'ultima si occupava essenzialmente del recupero dei dati persi o cancellati da *file*, *data base*, ecc., mentre la prima si propone di adattare il recupero di questi dati al contesto giuridico favorendo la loro completa ripetibilità all'interno del procedimento penale[21], in quanto è oramai pacifico che per ottenere risultati giuridicamente plausibili occorre utilizzare metodologie che traggono origine dalla scienza, com'è da considerare a tutti gli effetti la *digital forensics*[22]. D'altronde, la necessità di seguire determinati passaggi — che in concreto rappresentano delle garanzie — costituisce un punto fermo della legge n. 48 del 2008. Nello specifico l'approccio al programma o al sistema informatico nel contesto dell'indagine deve assicurare: la conservazione senza alterazioni, anche successive, del dato informatico originale; la formazione di una copia conforme, non modificabile, dell'elemento acquisito; l'installazione di sigilli informatici sui documenti acquisiti[23].

Nonostante questi progressi, resi possibili dall'utilizzo di rigorose ed accreditate metodologie, il vero punto critico dei differenti protocolli è costituito dalla difficoltà sia ad essere dimostrati in dibattimento mediante la loro validazione con i *tests* di verifica, sia ad integrarsi al sistema giuridico, costituito da regole di esclusione e di valutazione e da *standards* probatori che non possono essere elusi nel momento in cui si pretende di immettere il dato informatico nell'*habitat* processuale. Non a caso uno dei problemi maggiori che deve affrontare la *digital forensics* è proprio quello di assumere

19. Per approfondimenti sul punto Ziccardi, *Aspetti informatico–giuridici della fonte di prova digitale*, cit., 55 ss., nonché, anche per gli ampi riferimenti alla letteratura di settore, Id., *L'ingresso della* computer forensics *nel sistema processuale italiano: alcune considerazioni informatico–giuridiche*, in *Sistema penale e criminalità informatica. Profili sostanziali e processuali della Legge attuativa della Convenzione di Budapest sul* cybercrime *(l. 18 marzo 2008, n. 48)*, cit., pp. 165 ss.

20. Così, con chiarezza, Mattiucci, *Le indagini sui reperti invisibili*. High tech crime, cit., p. 709.

21. In questi termini, esemplarmente, Mattiucci, *Le indagini sui reperti invisibili*. High tech crime, cit., p. 709.

22. In merito v. il lavoro di Peterson, Shenoi, *Advances in digital forensics V*, (IFIP International Federation for Information Processing), Springer edition, 2009.

23. Curtotti, *I rilievi e gli accertamenti sul* locus commissi delicti *nelle evoluzioni del codice di procedura penale*, in *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienze*, cit., p. 68.

un taglio trasversale in modo da « *garantire il controllo delle indagini e dei risultati scientifici forniti* »[24] mediante il rispetto delle regole procedurali, così da assicurare continuità probatoria dall'identificazione del dato alla sua analisi in laboratorio e alla successiva dimostrabilità in sede processuale — ed in particolare in dibattimento[25] — dei risultati conseguiti.

Il legislatore italiano, seppur con ritardo, ha cercato di disciplinare il settore intervenendo nell'ambito delle disposizioni relative ai mezzi di ricerca della prova e delle indagini di polizia giudiziaria prevedendo modalità di ispezione, perquisizione e sequestro per il materiale informatico in modo da preservarne integrità ed autenticità[26]. In tal modo si è recepita la necessità, affermata da tempo dalla letteratura statunitense, di adeguare il sistema processuale penale al fenomeno della prova digitale[27].

Si tratta di innovazioni che offrono delle linee generali, aperte all'innovazione per cui si limitano a fissare degli obbiettivi finalizzati a garantire la salvaguardia dell'integrità del dato e la sua verificabilità successiva, pena l'inutilizzabilità.

Un altro problema che pare essere stato eluso dalla giurisprudenza è quella di ritenere la non ripetibilità di determinate operazioni sui reperti digitali.

3. Tra Scilla e Cariddi. Il rigore delle Cattedre. . . A fronte di questo quadro composito si registrano tendenzialmente due voci.

Da un lato, quella dei giuristi e dei tecnici che cercano di plasmarsi, coordinando la disciplina giuridica all'alta tecnicità raggiunta con la predisposizione di protocolli operativi (le cc.dd. S.O.P., *standard operating procedures*). E questo non mediante astratte modellistiche, ma con un armamentario che *in action* assicuri e prevenga le problematiche sottolineate dai tecnici.

Dall'altro lato, quella della giurisprudenza, meno sensibile alle rigorose conclusioni alle quali sono pervenuti i primi.

Uno dei primi aspetti che i tecnici mettono in chiaro è la congenita modificabilità della prova digitale a causa della sua immaterialità. È questa la ragione per cui diviene importantissima la modalità — alla quale devono

24. Mattiucci, *Le indagini sui reperti invisibili*. High tech crime, cit., p. 711.

25. Mattiucci, *Le indagini sui reperti invisibili*. High tech crime, cit., p. 711, sottolinea l'importanza e la decisività della « *descrizione ed interpretazione del verbale redatto in seno alle indagini preliminari* ».

26. Una compiuta analisi degli innovati istituti (artt. 244, 247, 352 e 354 c.p.p.) è contenuta nei contributi di Lorenzetto, *Le attività urgenti di investigazione informatica e telematica*; Braghò, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici* e Monti, *La nuova disciplina del sequestro informatico*, tutti contenuti nel volume curato da Lupária, *Sistema penale e criminalità informatica. Profili sostanziali e processuali della Legge attuativa della Convenzione di Budapest sul* cybercrime *(l. 18 marzo 2008, n. 48)*, cit.

27. Kerr, *Digital Evidence and the New Criminal Procedure*, in *105 Colum. l. Rev.*, 2005, 279; Id., *Searches and Seizures in a Digital World*, in *119 Harv. l. Rev.*, 2005, 531.

conformarsi tutti i protagonisti del rito criminale[28] — con cui viene appresa, in quanto una tecnica errata ne comporta la modificazione o alterazione[29] con tutti i rischi che ne conseguono in ordine alla capacità dimostrativa[30]. E accanto alla voce dei tecnici, si ode l'eco dei giuristi che individuano nell'inosservanza di dette metodologie ricadute sul piano dell'utilizzabilità o, quantomeno — secondo un approccio *soft* — , una attenuazione del valore probatorio dell'evidenza digitale[31].

La modalità per preservare[32] il dato informatico e garantirne l'autenticità è costituito dal rispetto della *chain of custody*, vale a dire il tracciare il procedimento di repertamento ed analisi mediante *report*, così da escludere alterazioni indebite delle tracce informatiche intervenute successivamente alla creazione, trasmissione o allocazione in altro supporto. In tal modo si consente ad accusa e difesa di esperire le relative indagini, consulenze e valutazioni su un dato che risulta genuino e perfettamente cristallizzato[33].

I tecnici ritengono che questi rischi possono essere ridotti mediante l'utilizzo di protocolli operativi, le ricordate S.O.P., che consentono di applicare la miglior tecnica al momento fruibile[34], posto che la non ripetibilità del dato digitale non consente "passi falsi", pena la perdita del patrimonio gnoseologico in esso contenuto[35].

La situazione del nostro Paese è di anarchia nel senso che le forze di polizia utilizzano protocolli differenti[36] che si fondano su quattro princìpi

28. Lupária, *La ricerca della prova digitale tra esigenze cognitive e valori costituzionali*, cit., p. 147 ss.

29. Tonini, *Documento informatico e giusto processo*, cit., p. 404, che qualifica "fragile" il dato digitale.

30. Mattiucci, *Le indagini sui reperti invisibili*. High tech crime, cit., 712.

31. Così, nonostante propenda per la prima soluzione, Lupária, *La ricerca della prova digitale tra esigenze cognitive e valori costituzionali*, cit., p. 147 s.

32. Daniele, *La prova digitale nel processo penale*, cit., 293, sottolinea come il pericolo della contaminazione della prova digitale è un rischio che il legislatore non può ignorare tanto per la vanificazione della pretesa punitiva, quanto per il pericolo di comprimere la prova a discarico dell'accusato.

33. Perri, voce *Computer forensics (indagini informatiche)*, in *Dig. Pen.*, Milano, VI, Agg., 2011, p. 100.

34. Significativi appaiono gli insegnamenti di Mattiucci, *Le indagini sui reperti invisibili*. High tech crime, cit., p. 715: « *la scena del crimine non può considerarsi un'area di laboratorio in cui possono essere applicati i tradizionali protocolli dell'analisi forense. Occorre elaborare delle S.O.P. (*Standard Operating Procedure*) calibrate per le investigazioni da esperire sulla* scena criminis ».

35. Per una disamina, seppur in prospettiva generale, delle problematiche legate alla vanificazione dei contenuti di elementi di prova, ci si permette di rinviare al nostro studio, *Gli accertamenti tecnici irripetibili (tra prassi devianti e recupero della legalità)*, Torino, 2009, *passim*.

36. I modelli di riferimento sono indicati in Mattiucci, *Le indagini sui reperti invisibili*. High tech crime, cit., 715. V., anche in riferimento all'eterogeneità di protocolli, Lupária, *Accertamenti tecnico–informatici e* best prectices *internazionali*, in Lupária, Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, cit., pp. 192 s., il quale ritiene trattarsi di « *una situazione inaccettabile, che pone giudici e parti processuali nella situazione di dover fare i conti con un contesto variegato e frammentato che certamente non agevola l'attività di interpretazione giudiziale* ».

che si concretizzano nei seguenti passaggi:

a) nessuna azione deve essere svolta se può cambiare dei dati direttamente o indirettamente e se può successivamente essere segnalata in dibattimento come invalidante della relativa fonte di prova;
b) i dati sulla scena del crimine non dovrebbero mai essere acceduti direttamente; se questo, tuttavia, si rende indispensabile per il rischio della loro definitiva perdita, chi vi accede deve possedere la competenza tecnica e la conoscenza giuridica necessarie a spiegare in dettaglio i passaggi che ha seguito nelle attività informatiche;
c) tutte le azioni sulla scena del crimine devono essere documentate. Ciò consente al giudice e alle parti processuali di valutarle ma anche di utilizzarle ai fini di ulteriori accertamenti tecnici;
d) il responsabile delle indagini è anche responsabile della mancata attuazione dei tre principi (principio di responsabilità indiretta tipicamente anglosassone)[37].

Questo protocollo configura una *best practice* di alto livello, in grado cioè di gestire un ampio numero di situazioni in quanto fondata su linee guida universali. Diverso è il caso del protocollo di basso livello, molto più performante e, quindi, fruibile in ipotesi ben determinate[38].

Ora, superando gli aspetti relativi all'utilizzo di una *best practice* di alto o basso livello, occorre volgere lo sguardo verso il profilo soggettivo e cioè di coloro deputati ad intervenire in siffatte situazioni[39]. In Italia non vi è un vero e proprio *team* specificamente preparato nel settore come in altre realtà quali U.S.A. e Giappone, ove esistono squadre di intervento forensi locali, operative ventiquattro ore su ventiquattro. Nonostante ciò tutti i protocolli redatti a livello internazionale non possono prescindere dalle figure investigative del *Digital Evidence First Responder* e del *Digital Evidence Specialist*.

Il primo, operante singolarmente o in *team*, costituisce il soggetto autorizzato e qualificato per agire per primo sulla scena del crimine in relazione alla raccolta e all'acquisizione delle fonti di prova digitale; il secondo, invece, è la persona fisica o il *team* che, oltre a poter svolgere la prima funzione, possiede professionalità in materia di *digital forensics* tanto in campo tecnico che legale, tale da consentirgli l'intera gestione della situazione e quindi di

37. Riprodotti fedelmente dal contributo di Mattiucci, *Le indagini sui reperti invisibili*. High tech crime, cit., p. 715.

38. Diffusamente sul punto Ziccardi, *Le linee guida della* Association of Chief Police Officers *inglese*, in Lupária, Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, cit., pp. 115 ss.; e Perri, voce *Computer forensics (indagini informatiche)*, cit., p. 102, i quali sottolineano il differente procedere a seconda che la scena *criminis* si caratterizzi per la presenza di un *computer* acceso o spento.

39. In riferimento alle singole figure operanti sulla scena *criminis* v., seppur in una prospettiva generale, Saravo, *CSI: il metodo di ricerca e valutazione delle tracce*, in *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienze*, cit., p. 369.

poter effettuare le attività di repertamento, copia, analisi di laboratorio e refertazione[40].

Il ritardo del legislatore italiano nel disciplinare la materia è parsa un occasione in parte mancata[41] per intervenire con una rigorosa disciplina, preferendo, al contrario, un approccio più morbido in nome di un reticolo normativo elastico di fronte all'inevitabile mutare delle tecniche di apprensione e valutazione del dato digitale.

La realtà effettuale mostra due criticità. L'aver disatteso un'esigenza fondamentale della Convenzione di Budapest sul *Cybercrime* che auspicava la creazione di un *corpus* normativo omogeneo in termini di criminalità informatica[42], da una parte; e, dall'altra, l'aver collocato le norme in merito tra le attività di polizia giudiziaria nel segno di un'impostazione che ha inevitabili riverberi sul diritto di difesa, poiché l'elevato tecnicismo che caratterizza tali operazioni richiede figure dotate di grande competenza, spesso mancante a coloro che intervengono in prima battuta sulla scena *criminis*.

Naturalmente l'attività demandata alla p.g. è circoscritta al solo congelamento dei dati digitali. E la ragione si spiega con la necessità di intervenire con urgenza; situazione che non "tollera" il ricorso a istituti più garantisti. Estratta la copia dei dati l'operazione non può spingersi oltre, dovendo successivamente spostarsi in laboratorio il lavoro di selezione e analisi dei dati[43].

Ed è proprio l'attività di copia che riserva maggiori oscillazioni sul piano esegetico. Per i giuristi costituisce atto non ripetibile, ragion per cui è opportuno avvalersi del garantito[44] modello dell'accertamento *ex* art. 360 c.p.p.[45] e mentre per la giurisprudenza la procedura disegnata dal legislatore non consente cedimenti garantistici, data la ripetibilità dell'operazione che deve ritenersi pienamente utilizzabile qualora siano stati rispettati i protocolli.

Un aspetto che suscita perplessità è la mancata previsione espressa del-

40. Mattiucci, *Le indagini sui reperti invisibili*. High tech crime, cit., pp. 716 s.

41. Lupária, *La ratifica della Convezione* Cybercrime *del Consiglio d'Europa. Legge 18 marzo 2008, n. 48. I profili processuali*, in *Dir. pen. proc.*, 2008, 718; nonché, volendo, Giunchedi, *Considerazioni a prima lettura sulla l. 18.3.2008, n. 48 in materia di criminalità informatica*, in *www.foroeuropa.it*, 2008, n. 1.

42. Curtotti, *I rilievi e gli accertamenti sul* locus commissi delicti *nelle evoluzioni del codice di procedura penale*, cit., p. 69.

43. Curtotti, *I rilievi e gli accertamenti sul* locus commissi delicti *nelle evoluzioni del codice di procedura penale*, cit., p. 70, la quale ricorda che in indagini aventi ad oggetto tracce biologiche e dattiloscopiche l'attività d'urgenza di p.g. può allargarsi anche al rinvenimento di indizi utili al prosieguo delle indagini.

44. Sulla relatività di detta garanzia si rinvia a Giunchedi, *Gli accertamenti tecnici irripetibili (tra prassi devianti e recupero della legalità)*, cit., spec. pp. 155 ss.

45. Daniele, *La prova digitale nel processo penale*, cit., 295 ss. prospetta differenti ipotesi di contraddittorio tecnico.

l'inutilizzabilità[46] qualora non siano rispettate le procedure previste per l'estrazione del dato[47]. Pregevole, quindi, il suggerimento di agire precauzionalmente mediante una procedura più garantita come quella degli accertamenti tecnici non ripetibili[48]. Aspetto questo che deve tenere conto di un elemento di non poco momento per gli effetti non desiderati che ne possono conseguire in ragione della particolare morfologia del contraddittorio tecnico[49]. Vi è, infatti, un dato che occorre chiarire fin da subito onde sgombrare il campo da possibili equivoci. Il tenore dell'art. 360, co. 3 c.p.p. prevede che difensori e consulenti tecnici abbiano diritto di « *assistere al conferimento dell'incarico, di partecipare agli accertamenti e di formulare osservazioni e riserve* ». Il punto è chiarire il significato da attribuire al verbo « *assistere* » ed in particolare se poterlo ritenere quale prologo al successivo diritto di formulare osservazioni e riserve. Se, infatti, lo si intende come attività di osservazione passiva, volta sul piano processuale a verificare la regolarità del compimento degli atti, è ovvio che il diritto di difesa risulta seriamente compromesso; diverso è il caso in cui l'accertamento tecnico *ex* art. 360 c.p.p. sia da assimilarsi per analogia alla perizia; qui il termine assistenza va letto in termini più ampi — di contraddittorio — e in correlazione logica con i diritti successivamente assicurati (partecipazione agli accertamenti, formulazione di osservazioni e riserve). L'art. 226, co. 2 c.p.p. prevede, infatti, un contraddittorio nella formulazione dei quesiti (« *Il giudice formula quindi i quesiti, sentiti il perito, i consulenti tecnici, il pubblico ministero e i difensori presenti* »).

Tornando all'acquisizione "viziata", vi è un ulteriore nodo da sciogliere e cioè se il successivo sequestro possa sanare l'omesso rispetto di procedure qualitativamente garantite[50]. Il quesito riporta all'annosa diatriba circa il rapporto tra perquisizione inutilizzabile e conseguente sequestro[51], risolta con l'insoddisfacente principio del *male captum, bene retentum*. In questo caso il giudice dovrà soffermarsi sulle modalità di acquisizione del dato probatorio, accertando che sia avvenuto secondo i protocolli operativi a cui rimandano le specifiche norme in tema di ispezione e perquisizione informatica e che la validità dell'atto non sia compromessa da vizi tali da inficiare la genuinità delle informazioni che ne scaturiscono[52]. Ne consegue

46. Daniele, *Indagini informatiche lesive della riservatezza. Verso un'inutilizzabilità convenzionale?*, in *Cass. pen.*, 2013, 368 s.

47. Condivisibilmente Daniele, *La prova digitale nel processo penale*, cit., 295.

48. Lupária, *La ratifica della Convezione* Cybercrime *del Consiglio d'Europa. Legge 18 marzo 2008, n. 48. I profili processuali*, cit., 720.

49. Considerazioni sviluppate più diffusamente nel più ampio studio, *Gli accertamenti tecnici irripetibili (tra prassi devianti e recupero della legalità)*, cit., pp. 109 ss.

50. Curtotti, *I rilievi e gli accertamenti sul* locus commissi delicti *nelle evoluzioni del codice di procedura penale*, cit., pp. 98 ss.

51. Cass., Sez. un., 27 marzo 1996, Sala, in *Cass. pen.*, 1996, 3268.

52. Dinacci, *L'inutilizzabilità nel processo penale. Struttura e funzione del vizio*, Milano, 2008, pp. 91

quel principio definito di propagazione dell'inutilizzabilità, in forza del quale da un atto non utilizzabile non possono discendere effetti, se non quando siano favorevoli all'imputato[53]. Più specificamente, si ritiene che un vizio che infici il valore probatorio di un elemento gnoseologico imponga che tutti gli altri elementi conoscitivi che a questi sono causalmente legati[54] debbano essere dichiarati inutilizzabili in quanto, colpendo la prova, ne inibiscono la funzione di unico sapere processuale sulla base del quale adottare la decisione[55].

In relazione a queste premesse, si può tentare di offrire una prima risposta tendente ad escludere che l'eventuale vizio genetico nell'acquisizione di una prova digitale possa essere superato con l'*escamotage* legato al successivo sequestro. Sarebbe contrario a ragionevolezza, nonché alla tutela di interessi processuali, consentire questa possibilità per sanare un atto per sua natura non ripetibile il quale, pur mantenendo intatto il profilo dell'attendibilità gnoseologica, ne vede svalutate le potenzialità dimostrative a causa di un processo di ricostruzione fattuale non ortodosso[56]. Si tratta, quindi, di dare piena espansione alla teoria dei « *frutti dell'albero avvelenato* » enucleata dalla giurisprudenza statunitense[57], la quale, in prospettiva di salvaguardia del sistema, impone di escludere tutto quanto possa trasformarsi in un comodo artifizio per eludere un divieto[58].

4. (Segue) . . . e la *nonchalance* delle Corti. La giurisprudenza, come anticipato, si muove su posizioni meno garantistiche rispetto alla letteratura, in quanto quest'ultima, miscelando aspetti tecnici e sistematicità, perviene a considerare come non ripetibili gli accertamenti di *digital evidence* con l'inevitabile necessità di fruire del contraddittorio tecnico previsto dall'art. 360 c.p.p.

Cerchiamo, quindi, di tracciare un quadro che, seppur non esaustivo, sia indicativo della posizione tenuta dai giudici al cospetto della *digital forensics*.

In una delle prime decisioni che ha tracciato linee guida in materia, affiora un orientamento che sul crinale della ripetibilità delle operazioni di

ss.

53. Dinacci, *L'inutilizzabilità nel processo penale. Struttura e funzione del vizio*, cit., p. 89.

54. Sabatini, *Trattato dei procedimenti incidentali nel processo penale*, Torino, 1953, p. 4.

55. Dinacci, *L'inutilizzabilità nel processo penale. Struttura e funzione del vizio*, cit., pp. 92 ss.; Spangher, *"E pur si muove" dal* male captum bene retentum *alle* exclusionary rules, in *Giust. pen.*, 1997, III, 139. Di diversa opinione, in quanto la dipendenza sarebbe solo psicologica e non giuridica, Cordero, *Tre studi sulle prove penali*, Milano, 1963, p. 141.

56. Galantini, voce *Inutilizzabilità (dir. proc. pen.)*, in *Enc. Dir.*, I, Agg., Milano, 1997, p. 701.

57. Kacynsky, *Admissibility of illegally obtained evidence: a comparative study*, in *Modern Legal System Cyclopedia*, I A, II, 1988, 1A.80.12.

58. Gaito, *Aspetti problematici in tema di prove*, in Gaito, *Procedura penale e garanzie europee*, Torino, 2006, p. 96. *Contra* Iacoviello, *La Cassazione penale. Fatto, diritto e motivazione*, Milano, 2013, p. 210, ritiene che « *da noi l'albero della perquisizione più che avvelenato è selvatico. Le cose sequestrate non sono velenose, ma magari asprignole. Dunque processualmente commestibili* ».

repertamento e copia del dato digitale tende ad eludere, sotto il pretesto della sussistenza di ragioni tecniche, il contraddittorio tra gli esperti. Per la Suprema Corte, infatti, « *non rientra nel novero degli atti irripetibili l'attività di estrazione di copia di* file *da un* computer *oggetto di sequestro, dal momento che essa non comporta alcuna attività di carattere valutativo su base tecnico–scientifica, né determina alcuna alterazione dello stato delle cose, tale da creare pregiudizio alla genuinità del contraddittorio conoscitivo nella prospettiva dibattimentale, essendo sempre e comunque assicurata la riproducibilità d'informazioni identiche a quelle contenute nell'originale* »[59]. I giudici di legittimità con sopraffina tecnica argomentativa, superano il problema delle garanzie utilizzando una solida base sistematica, ritenendo che in considerazione dell'assenza di oneri valutativi in capo al soggetto che compie l'attività di estrazione dei dati da *computer*, viene meno uno dei presupposti dell'accertamento tecnico irripetibile, dal che l'impossibilità di utilizzarne il modulo. La motivazione non considera gli aspetti tecnici legati alla molteplicità di procedure operative e quindi la circostanza che la decisione in ordine all'opzione per l'una o per l'altra implica una valutazione. Tanto che sotto questo profilo, in virtù di una rigida interpretazione dell'istituto in esame, riteniamo preferibile utilizzare il più garantito incidente probatorio in forma "accelerata"[60].

Sulla medesima falsariga si muove altra decisione di legittimità. Il ricorrente lamentava la nullità delle operazioni di *computer forensics* a causa del mancato avviso in ordine all'esame dell'*hard disk* del suo *computer*, come previsto dall'art. 360, co. 2 c.p.p. Per la Cassazione, però, non costituendo « *accertamento tecnico irripetibile l'estrazione dei dati archiviati in un* computer, *trattandosi di operazione meramente meccanica, riproducibile per un numero infinito di volte* », non sussiste « *nullità quando l'accertamento in questione sia effettuato senza preavvisare il difensore della persona sottoposta alle indagini* »[61]. In questa ipotesi non siamo al cospetto di un divieto che colpisce la prova, ma di un vizio nel procedimento che si riverbera sul risultato dello stesso, anche se trattandosi di nullità (a regime intermedio attenendo all'assistenza) risulta sanabile se non eccepita nelle paratie di tempo fissate dal legislatore[62].

Il quadro tracciato — idoneo, pur se molto limitato, per scattare un'istantanea del panorama nazionale nell'approccio alla *digital evidence* — pare non potersi nemmeno giovare dei diversi approdi della Corte europea che, di fronte ad ipotesi di perquisizioni informatiche e conseguente ablazione del *computer* senza specifiche garanzie, ha ritenuto concretizzarsi la violazione

59. Cass., Sez. I, 5 marzo 2009, A.S.A., in *Dir. pen. proc.*, 2010, 337, con nota critica di Ricci, Digital evidence *e irripetibilità delle operazioni acquisite*.

60. Per il quale ci si permette di rinviare a Giunchedi, *Gli accertamenti tecnici irripetibili (tra prassi devianti e recupero della legalità)*, cit., pp. 157 s.

61. Cass., Sez. I, 9 marzo 2011, E.M. in *Cass. pen.*, 2012, 440, con nota di Daniele, *Il diritto al preavviso della difesa nelle indagini informatiche*, cit., del quale si leggano gli interessanti spunti.

62. Sul punto Daniele, *Il diritto al preavviso della difesa nelle indagini informatiche*, cit., 445.

del diritto alla riservatezza, proprio perché l'evanescenza del dato richiede ulteriori cautele non superabili nemmeno in ipotesi di apposizione dei sigilli[63]. Nonostante ciò anche la giurisprudenza sovranazionale esclude che la violazione dell'art. 8 CEDU importi riflessi immediati sull'iniquità del processo[64] con conseguente necessità di dover ripetere il processo depurato dalle prove reperite ledendo il diritto alla riservatezza. D'altronde i limiti posti dalla giurisprudenza costituzionale alla penetrazione dei princìpi espressi dalla Corte di Strasburgo nel tessuto connettivo del rito criminale interno, impone sì « *di apprezzare la giurisprudenza europea consolidatasi sulla norma conferente, in modo da rispettarne la sostanza, ma con un margine di apprezzamento e di adeguamento che le consenta di tener conto delle peculiarità dell'ordinamento giuridico in cui la norma convenzionale è destinata a inserirsi* »[65].

Peraltro questo epilogo in una materia ove si giocano gran parte dei processi, era scritto nel preludio. Tutti ricorderanno il disinvolto approccio della giurisprudenza nel *leading case* Vierika[66]. Secondo il Tribunale di Bologna dal mancato rispetto delle *best practices* non consegue automaticamente un'inutilizzabilità, spettando alla difesa l'onere di dimostrare che la metodologia utilizzata ha concretamente alterato i dati ottenuti. Allo stesso tempo — sempre per il giudice felsineo — possono ritenersi accertate le modalità di funzionamento di un sistema informatico anche dalla testimonianza resa in dibattimento dall'operante di polizia giudiziaria purché dotato di specifiche competenze.

Le considerazioni a trarsi da un simile approccio portano a conseguenze aberranti tanto per il disinteresse del giudice dall'utilizzo dei protocolli operativi, quanto per la *probatio diabolica* che si pone a carico della parte: dimostrare cioé le conseguenze derivanti dalla deviazione dalla *best practice*. Il sistema accusatorio, al contrario scrollandosi di dosso incrostazioni inquisitorie, dovrebbe pretendere che sia la parte che di quei dati vuol farne uso a dimostrare che, nonostante le *malpractices*, questi non risultano aver subito alterazioni[67]. Non si trascuri, infatti, che condotte maldestre da parte degli inquirenti, possono influire sulla costruzione della prova d'alibi da parte dell'imputato[68], come è stato dimostrato in una nota vicenda[69].

63. Corte eur. dir. uomo, Sez. I, Robathin c. Austria, cit.

64. *Contra* Corte eur. dir. uomo, Gr. Cam., 10 marzo 2009, Bykov c. Russia.

65. Corte cost., n. 236 del 2011.

66. Trib. Bologna, 22 dicembre 2005, Vierika, in *Dir. internet*, 2005, 153, con nota di Lupária, *Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova penale digitale. I profili processuali*.

67. Per approfondite considerazioni Lupária, *Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova penale digitale. I profili processuali*, cit., 158 s.; nonché, più di recente, Marafioti, Digital evidence *e processo penale*, in *Cass. pen.*, 2011, 4521.

68. Sull'alibi informatico, Nicosia, Caccavella, *Indagini della difesa e alibi informatico: utilizzo di nuove metodiche investigative, problemi applicativi ed introduzione nel giudizio*, in *Dir. internet*, 2007, 520 ss.

69. Trib. Vigevano, 17 dicembre 2009, Stasi, citato in Marafioti, Digital evidence *e processo penale*,

L'altro aspetto che emerge dalla decisione Vierika attiene al mancato esperimento di consulenze e di una perizia da parte del giudice, ritenendo sufficienti le informazioni riversate in dibattimento dall'ufficiale di polizia giudiziaria che ha effettuato l'analisi del sistema informatico. Accreditare una simile impostazione significa scivolare in un crinale molto pericoloso per le sorti del processo penale poiché permeato da forti tratti inquisitori. Proviamo a pensare alle possibili conseguenze che, in un contesto più generale[70], avevamo già respinto con fermezza.

La questione attiene alla possibilità di recuperare i risultati di un accertamento effettuato secondo modalità invalidanti. Questo sia su istanza di parte che mediante i poteri istruttori suppletivi previsti dall'art. 507 c.p.p.

Trascurando di trattare dei princìpi che stanno alla base della scelta del legislatore di derogare nel dibattimento, mediante gli artt. 506 e 507 c.p.p., alla scelta di metodo fondata sul potere dispositivo della prova in capo alle parti, va sottolineato come ai fini della risoluzione del problema, sia fondamentale ripercorrere i passaggi compiuti dalla Corte costituzionale e dalle Sezioni unite nell'allargare e chiarire la portata delle disposizioni appena ricordate, cercando un punto di equilibrio in relazione ai possibili abusi che possono derivare da un simile potere. La giurisprudenza costituzionale[71] ha ritenuto di ampliare i poteri di intervento del giudice con l'esigenza di evitare disattivazioni dell'azione penale da parte di un pubblico ministero che non la coltivi con le necessarie richieste probatorie e, al contempo, che lacune difensive pregiudichino il diritto di difesa. Ed è inevitabile che, da un lato, si alimentano i timori di minare la purezza decisionale del giudice il quale, mediante incursioni probatorie, rischierebbe di perdere quel distacco dalla controversia che lo rendono imparziale; dall'altro lato che i poteri giudiziali in punto di prova tendono a salvaguardare la giurisdizione purificandola dai vuoti e dai limiti che l'attività delle parti può evidenziare, a condizione che i poteri probatori del giudice si proiettino « *verso la decisione e non verso la conferma e la smentita di una determinata tesi* »[72]; che tendano, in breve, a completare il panorama probatorio offerto dalle parti solo in ipotesi di assoluta necessità. Il problema è costituito dall'utilizzo dei poteri istruttori del giudice per finalità non propriamente ortodosse in relazione all'impronta accusatoria del processo le quali tendono anche a sconfinare dalla incompletezza del panorama probatorio — ipotesi in cui è legittimo il potere integrativo del giudice — all'incertezza che è coerente con gli epiloghi codificati in forza dei canoni valutativi previsti dagli artt. 530, co. 2,

cit., 4523, sentenza in cui si legge che il « *danno irreparabile prodotto dagli inquirenti attiene proprio all'accertamento della verità processuale* ».

70. Giunchedi, *Gli accertamenti tecnici irripetibili (tra prassi devianti e recupero della legalità)*, cit., 139 ss.

71. Corte cost., n. 111 del 1993.

72. De Caro, *Poteri probatori del giudice e diritto alla prova*, Napoli, 2003, p. 130.

e 533, co. 1 c.p.p.

Più specificamente, va ripudiato un potere vicario del giudice per « *supplire alla totale inerzia delle parti* »[73] che è stato ritenuto degno di cittadinanza nell'ordinamento dalle Sezioni unite[74] e dalla Corte costituzionale[75], le quali, riproponendo le finalità inquisitorie della ricerca della verità, hanno degradato lo spirito agonista del processo penale ove il ruolo e le strategie delle parti giocano un peso decisivo nelle dinamiche contraddittoriali.

Sulla scorta degli insegnamenti predetti si ritiene che il giudice, in forza dei poteri integrativi *ex officio*, possa recuperare, assumendo la relativa testimonianza del consulente tecnico, un accertamento non ripetibile nullo (ad esempio per mancanza dell'avviso), ma non di un accertamento inutilizzabile, trattandosi di vizio che inficia patologicamente il risultato dell'atto.

5. Verso un "Rinascimento" giuridico nella *digital forensics*. È giunto il momento di trarre delle conclusioni estremamente sintetiche onde evitare di ritornare su aspetti già illustrati nei paragrafi precedenti.

Che le prove digitali si contraddistinguano per immaterialità e fragilità è pacifico; cosi come è altrettanto certo che richiedano metodi di raccolta per i quali sono necessarie competenze tecniche diverse da quelle solitamente utilizzate dagli inquirenti per le altre risultanze probatorie[76].

In relazione a ciò è evidente la loro facile modificabilità, possibile anche con un semplice accesso da parte di soggetto non adeguatamente specializzato.

Da qui l'esigenza, sollecitata e da tecnici e giuristi, che il dato informatico venga cristallizzato mediante complesse operazioni tecniche accompagnate dalla loro tracciabilità tale da evidenziare quella che in gergo viene definita *chain of custody*.

Queste motivate esigenze sono state in parte recepite dal legislatore con la legge n. 48 del 2008, costituente un testo normativo che offre delle coordinate programmatiche, con il limite di non prevedere delle sanzioni in caso di loro inosservanza.

In questa vaghezza, dettata dall'esigenza di non chiudersi di fronte alle possibili innovazioni tecnologiche finalizzate a preservare il quadro digitale, la giurisprudenza si è ingiustificatamente insinuata con una retrospettiva inquisitoria che desta non poche perplessità in ordine ad un processo penale

73. Cass., Sez. II, 23 ottobre 1991, P.m. in proc. Marinkovic, in *Arch. nuova proc. pen.*, 1992, 436.

74. Cass., Sez. un., 6 novembre 1992, Martin, in *Cass. pen.*, 1993, 280; e, sotto l'egida dell'art. 111, co. 2, Cost., Id., Sez. un., 17 ottobre 2006, P.m. in proc. Greco, in *Guida dir.*, 2007, 2, 78.

75. La già citata Corte cost., n. 111 del 1993.

76. Per tutti Casey, *Digital Evidence and Computer Crime. Forensic science, Computers and the Internet*, London–San Diego, Academic Press, 2004, 15; Kerr, *Digital Evidence and the New Criminal Procedure*, cit., 291.

che, proclamato il contraddittorio nella formazione della prova, lo ha poi abbandonato in nome della prova tecnica, molto spesso recuperata dalla fase di indagine, in merito alla quale si può solo pretendere un contraddittorio *sul* dato gnoseologico.

In questo contesto *mettre à côté* le conseguenze derivanti dall'omesso o maldestro utilizzo delle *best practices* significa non considerare l'importanza degli accertamenti relativi alla prova digitale, piegandosi ad una logica autoritaria svincolata dai canoni della prova sia scientifica che logica[77].

Sono queste le ragioni, recepite dalla dottrina[78], della necessità di un contraddittorio effettivo nel momento in cui si accede al dato digitale, in considerazione dell'irreversibilità dei risultati raggiunti.

Siamo consci che questo non sempre possa avvenire per la necessità di intervenire con urgenza e anche perché il contraddittorio tecnico implica l'avviso all'indagato che, in tal modo, è potenzialmente in condizione di manipolare il sistema informatico ed inquinare i dati[79]. In queste situazioni l'effetto "sorpresa" può offrire dei risultati diversamente non ottenibili. La potenziale proficuità dell'indagine, però, non può andare a discapito della genuinità della prova; per tal motivo, in tali situazioni, l'unica garanzia possibile è un controllo *ex post* fondato sulla verifica della correttezza della metodologia utilizzata, senza alcun onere probatorio in capo alla parte che eccepisce una deviazione dal modello operativo.

Il diverso approccio di giurisprudenza e dottrina riflette due differenti culture processuali[80]: la prima di stampo inquisitorio, che non dovrebbe più godere di cittadinanza in un processo accusatorio, con il giudice attore incontrastato in tema di prova; la seconda costituente il portato del giusto processo e dei moderni approdi del rapporto tra scienza e diritto, ove il giudice non è più succube della scienza, ma neppure *peritus peritorum* dovendo porsi come consumatore informato di leggi scientifiche con l'obbligo di motivare logicamente la propria decisione. Solo seguendo queste coordinate non si depaupererà l'importante patrimonio culturale faticosamente acquisito.

Queste conclusioni non devono, però, portare ad assolutizzare il risultato dell'accertamento informatico in quanto per un ortodosso utilizzo della

77. Molto efficace il richiamo effettuato da Marafioti, Digital evidence *e processo penale*, cit., 4523, ad un risalente scritto di Pagano, *Logica de' probabili applicata a giudizi criminali, o Teoria delle prove*, in *Opere*, III, Lugano, 1832, nel quale emerge la necessità che l'indizio sia provato, in quanto qualora sia solo probabile, il fatto risulterà sempre dubbio. Dal che l'impossibilità per indizi mal provati, in quanto solo probabili, di affermare la sussistenza di un fatto, indipendentemente dal numero di essi.

78. Tonini, *Documento informatico e giusto processo*, cit., 406.

79. Daniele, *La prova digitale nel processo penale*, cit., 297 s., in relazione a queste problematiche suggerisce una graduazione del contraddittorio tecnico.

80. Esemplari sul punto le pagine di Tonini, *La sentenza di Perugia come occasione di ripensamento sul metodo scientifico di conoscenza*, in *L'assassinio di Meredith Kercher. Anatomia del processo di Perugia*, a cura di M. Montagna, Roma, 2012, pp. 25 ss.

prova scientifica non bisogna mai relegare il ruolo del giudice — e quello delle parti — a fruitore passivo della scienza, in quanto la prova tecnica costituisce uno dei tanti ingredienti — magari, in taluni casi, quello più rilevante — della piattaforma probatoria, ove l'*assist* spetta sempre al giudice quale conseguenza di una serie di valutazioni complesse, prima fra tutte l'inferenza[81]. D'altronde è in questi termini che la Suprema Corte ha "relativizzato" l'apporto tecnico in processi connotati da una forte matrice scientifica[82], ritenendo che molto spesso la logica consente di raggiungere *aliunde* gli stessi risultati dello scienziato e, soprattutto, di fungere da *gatekepper* della scienza.

Sono queste le ragioni per auspicare un ritorno al tradizionale processo accusatorio, arricchito però dall'importante, ma non decisivo, apporto scientifico.

Insomma, ci troviamo in pieno "*Rinascimento*" giuridico.

81. Per più approfondite considerazioni in merito, anche per la ricca bibliografia citata, Santoriello, *La prova penale e la sua valutazione*, Roma, 2012, pp. 174 ss.

82. Cass., Sez. I, 21 maggio 2008, Franzoni, in *Cass. pen.*, 2009, 1840, secondo cui « *il requisito della certezza che deve assistere gli elementi indizianti, requisito non espressamente enunciato dall'art. 192, co. 2 c.p.p. ma postulato come indefettibile dalla giurisprudenza ed intrinsecamente connesso alla sistematica della prova indiziaria, non può assumersi in termini di assolutezza e di verità in senso ontologico, in quanto la certezza del dato indiziante è pur sempre una certezza di natura processuale e partecipa di quella specie di certezza che si forma nel processo attraverso il procedimento probatorio* ». Nel caso specifico — il c.d. delitto di Cogne — le prove tecniche sono state bilanciate da una considerazione logica (« *quando la possibilità dell'azione di una terza persona sia stata esclusa dal giudice al di là di ogni ragionevole dubbio, la prova logica della responsabilità dell'imputato che ne deriva può essere correttamente posta come caposaldo della sequenza indiziaria, laddove la suddetta responsabilità si presenti come l'unica realistica e necessitata alternativa residuale* »). Cfr., anche, Cass., Sez. I, 25 marzo 2013, P.G. in proc. Knox ed altro, in *www.archiviopenale.it*, ove dalla condanna per calunnia della Knox — e al rigetto del relativo motivo ricorso — ha tratto, secondo le regole della logica, una correlazione con il più grave delitto di omicidio di Meredith Kercher: « *La motivazione della sentenza sulla correlazione da istituire tra il fatto di calunnia ed il più grave reato di omicidio e quindi sulla sussistenza o meno del nesso teleologico inizialmente contestato e ritenuto, è manifestamente illogica e deve essere riformulata secondo parametri di maggiore plausibilità e con maggiore aderenza ai flussi informativi, essendo mancato un approfondimento critico sulla plausibilità del collegamento sostenuto dai primi giudici. Il passaggio è fondamentale nell'economia della ricostruzione, perché impinge il profilo, tutt'altro che irrilevante, della presenza della giovane all'interno della casa al momento del fatto di sangue, presenza che pur non potendo tradursi in automatica prova del concorso nell'omicidio, è tale da illuminare con intensa luce lo sviluppo ed i protagonisti dell'orribile delitto* ».