Alma Mater Studiorum – Università di Bologna

DOTTORATO DI RICERCA IN

DIRITTO E NUOVE TECNOLOGIE

Ciclo XXVIII

Settore Concorsuale di afferenza: 12/H3

Settore Scientifico disciplinare: IUS/20

Informatica forense e processo penale: la prova digitale tra innovazione normativa e incertezze giurisprudenziali

Presentata da: Antonio Gammarota

Coordinatore Dottorato
Prof. Giovanni Sartor

Relatore
Prof. Cesare Maioli

Esame finale anno 2016

Ad Anna e Francesco

Prefazione

Ho cominciato ad occuparmi professionalmente di informatica giuridica circa venticinque anni fa quando, terminati gli studi giuridici, intrapresi la pratica forense.

Ebbi in sorte di essere accolto in uno Studio legale dove le necessità riorganizzative e la passione per l'innovazione tecnologica imposero l'informatizzazione delle procedure di gestione dello Studio, delle pratiche e della redazione di atti con gli (allora) nuovi strumenti offerti dall'informatica.

Dall'uso dei primi *word processor*, all'utilizzo delle prime banche dati, all'allestimento della rete locale, alla progettazione del programma gestionale dello studio, quella prima esperienza iniziava con un'immersione totale nella nuova dimensione tecnologica della professione che proprio in quegli anni muoveva i primi passi verso l'automazione.

Lavorando al fianco di ingegneri e informatici che modellavano i nuovi strumenti e di fatto reingegnerizzavano l'antica professione, intuii che l'interdisciplinarietà tra il diritto e l'informatica era giunto ad un punto di non ritorno.

Diventato avvocato – anzi, come allora prevedeva la legge, procuratore legale – non solo organizzai la mia professione automatizzandola, ma iniziai ad occuparmi professionalmente quasi esclusivamente di trattamento di dati personali, contratti ad oggetto informatico e reati informatici.

Il punto di non ritorno fu segnato a metà degli anni 90, quando ebbi il privilegio di essere nominato difensore di un impiegato pubblico imputato di danneggiamento aggravato al sistema informatico del grande ente per il quale lavorava.

Si trattava di un caso molto complesso sia sul piano dei fatti che del diritto, apparendo subito evidente che l'accusa di danneggiamento del sistema informatico sollevava molte altre questioni giuridiche: dalle indagini anacronisticamente svolte con metodologie "analogiche", al sospetto di vizi del sistema informatico oggetto di appalto, alla complessità dello scenario informatico interessato, all'elevato numero di testimoni, per lo più informatici, oltre ad una lunga serie di problematiche giuridiche collaterali di natura amministrativa, sindacale e personale intercorrenti tra le parti a vario titolo coinvolte nel procedimento.

I problemi giuridici da affrontare erano molteplici, di diversa natura e di ardua complessità, ma quell'esperienza, risoltasi positivamente[1], mi aveva consentito di maturare un'esperienza scientifica e professionale unica, avendomi costretto ad esplorare pionieristicamete l'ambito dei reati informatici, delle tecniche di investigazione e di indagine informatica, nonché a considerare l'informatica non più come strumento di lavoro, ma come un vero e proprio sistema gnoseologico.

A quei tempi, la letteratura annoverava alcune opere, anche molto pregevoli, di diritto penale informatico sostanziale[2], mentre non si rinvenivano elaborazioni dottrinali e giurisprudenziali significative in merito alle problematiche processuali penali, mancanza che rifletteva il livello della cultura tecnico-guridica sulle problematiche attinenti le indagini informatiche.

Se sparuti erano i casi di giurisprudenza sui reati informatici, praticamente sconosciute erano le decisioni su casi complessi o vertenti sui problemi procedurali ed in particolare sui mezzi di ricerca della prova e sui mezzi di prova ad oggetto informatico.

Quindi, l'approccio non poteva che essere comparativistico, per cui rivolsi l'attenzione alla letteratura d'oltreoceano, ai documenti ufficiali del Federal Bureau of Intelligence (FBI) del Ministero di Giustizia degli Stati Uniti di America, ai già numerosi e pregevoli manuali americani di Computer forensics e ai documenti elaborati da alcune associazioni americane che raccoglievano l'esperienza degli operatori e delle agenzie federali che già da diversi anni si occupavano di reati e indagini informatiche.

Nel 2003, al termine di quel primo processo, fui invitato per la prima volta a svolgere una lezione a professionisti e studiosi di Informatica giuridica proprio sulle questioni giuridiche e informatiche che avevo sviluppato in occasione della mia prima esperienza professionale[3].

Durante quella prima lezione, che intitolai proprio "Dalla Computer forensics all'Informatica forense", esponevo le modalità con le quali, ispirandomi ai principi giuridici e tecnici della Computer forensics americana, avevo impostato l'esame e la difesa nel caso di presunta criminalità informatica, gettando le basi per la modellazione della disciplina.

---

[1] Per un breve resoconto, v. GAMMAROTA A., Danneggiamento di sistema informatico della P.A. e informatica forense: un caso, in POZZI P., MASOTTI R., BOZZETTI M., (a cura di), Crimine virtuale, minaccia reale, Franco Angeli, Milano, 2004, p. 207 e ss.

[2] Tra gli altri, v. GALDIERI P., Teoria e pratica nell'interpretazione del reato informatico, Giuffrè, Milano, 1997; PICA G., Diritto penale delle tecnologie informatiche, Utet, Torino, 1999; PICOTTI L., Reati informatici in Enciclopedia giuridica, Aggiornamento VIII, Istituto della Enciclopedia italiana, Roma, 2000, p. 1-33.

[3] Si trattava della seconda edizione del Master in Diritto delle nuove tecnologie organizzato dal Centro Studi di Informatica Giuridica svoltosi a Bari nel 2003; per un resoconto, v. GALEOTTI P., Master-Post eventum 12.05.03, in *http://www.avvocatiacquavivacassano.it*.

L'impulso a trasferire quel nuovo approccio alla realtà italiana era arrivato dalla lettura di un articolo pubblicato su Alfa-Redi - Revista de Derecho Informatico, una rivista peruviana di Informatica giuridica[4] nel quale per la prima volta l'Informatica forense veniva sistematizzata secondo gli schemi tipici di un ordinamento di *civil law*; mutuai finanche il sintagma "Informatica forense" che, per quanto in lingua castigliana, ben poteva essere usato con pari significato anche in Italia.

L'esperienza divulgativa proseguì nelle aule di Informatica giuridica dell'Alma Mater dove prima venni invitato a comunicare le competenze acquisite in campo professionale e poi a tenere una serie di seminari, fino a quando non venne istituito il modulo giuridico nell'ambito del corso che, negli anni successivi, si sarebbe consolidato come insegnamento stabile di Informatica forense.

Ad un quarto di secolo dall'inizio della mia esperienza professionale, mai avrei pensato che le competenze acquisite soprattutto "sul campo" e convogliate nell'esperienza di studio e di insegnamento sarebbero state un giorno oggetto dell'intero ciclo del mio dottorato svolto giunto ormai al suo compimento.

L'auspicio è che il presente lavoro costituisca solo l'inizio di un nuovo ciclo di pratica e studio delle problematiche sempre nuove che il progresso tecnologico e l'innovazione giuridica impongono all'attenzione dell'Informatica forense.

[4] AIRALA A. D., Argentina: a las puertas de una Nueva Especializacion: La Informatica Forense, "Alfa – Redi Revista de Derecho Informatico", n. 055, 2003, in *http://www.alfa-redi.org/revista/data/57-10.asp*.

Introduzione

I bit, sotto tortura, confessano qualunque cosa

Da tempo capita di leggere articoli o di assistere ad interviste o a spettacoli nelle quali non manca mai qualcuno che riferendosi a impronte, macchie di sangue, o sostanze bioogiche rinvenute sulla scena del delitto, pur trovandosi ancora all'inizio delle indagini, già li definisca "prove" schiaccianti, inoppugnabili, oggettive, incontrovertibili, indiscutibili, e così via, riuscendo pure a trovare qualcuno disposto a credergli.

È il risultato della falsa sensazione di oggettività che caratterizza la cieca fiducia nella c.d. prova scientifica che, apparendo "evidente", annichilisce il senso critico.

Da alcuni anni, tale tendenza sta progressivamente investendo un'altra fonte di informazioni utili alle investigazioni: i dati digitali, informatici e telematici. Per la precisione, ad essere evocati spesso non sono nemmeno i dati, quanto i computer, i telefoni cellulari, i tablet, le fotocamere digitali, i sistemi di navigazione GPS e tutti gli altri dispositivi digitali che ne costituiscono solo l'apparente involucro.

Nella letteratura criminalistica è dato leggere di operatori, anche qualificati, che, travalicando tutte le questioni tecniche, attribuiscono ai documenti estratti dai dispositivi digitali valore oggettivo e incontestabile per il solo fatto che un dispositivo ha registrato dati in grado di rappresentare all'evidenza i fatti di reato da accertare e provare.

Inoltre, si assiste alla progressiva sopravvalutazione dei mezzi di prova digitali, in quanto ritenuti oggettivi, rispetto ad altri mezzi di prova orali, ritenuti maggiormente a rischio di mendacio, di falsa testimonianza, o alla meglio risultato di ricordi incompleti, evanescenti, suggestionabili.

In sede gnoseologica, si è detto che "le parole fanno le cose"[5] e sempre più spesso il processo ricostruttivo della verità giudiziale si fonda su questo principio.

In sede pratica, invece, si assiste al fenomeno per il quale ove il potere performativo delle parole si riveli insufficiente a ricostruire la realtà necessaria

[5]AUSTIN J.L., How to do Things with Words, Second Edition (Oxford: Oxford University Press, 1975).

alla funzione giudiziaria, vengono evocati i numeri, quelli costituenti la base del sistema binario usato per la codifica dei dati, ai quali si attribuiscono qualità di intrinseca oggettività sufficiente a supportare la validità di un percorso logico-argomentativo-probatorio.

Su tali presupposti in ambito forense si è creato il falso mito dell'inoppugnabilità della prova informatica in quanto oggettiva e rappresentativa in sé, e che invece è il risultato di un sistema di sopravvalutazione del potere dei numeri, del sistema digitale e delle rappresentazioni derivate, ai quali si attribuisce una pseudo efficacia performativa.

La concezione che si sta affermando intorno al ruolo dei dati digitali nel processo penale procede sempre più apoditticamente, senza tener conto che il giudizio di inoppugnabilità di una prova è un giudizio sintetico, riassuntivo e finale che può essere raggiunto solo al termine di complesse operazioni logiche di analisi e di comparazione degli elementi rinvenuti, e solo dopo un esame della loro coerenza sia con le leggi scientifiche, sia con le norme giuridiche che regolano la liceità e la legittimità di una prova.

Tale giudizio può giungere solo all'esito di un contraddittorio secondo le regole del Giusto processo durante il quale le parti hanno potuto esaminare gli elementi di prova, discutere in contraddittorio gli accertamenti tecnici compiuti, esaminare i propri consulenti e controesaminare i consulenti delle parti contrapposte, confrontate in contraddittorio e discusso gli esiti.

Difatti, la giurisprudenza di Common law, che in tema di processo accusatorio e di prova scientifica ha una tradizione molto più antica rispetto alla nostra, ha ben chiara la differenza terminologica e logica tra i concetti di "evidence" e "proof".

La differenza tra i due termini risiede nel fatto che l'*evidence* è solo il mezzo mediante il quale i fatti oggetto di esame giudiziario sono resi evidenti o provati a un giudice o a una giuria, e che solo se accettato e creduto, esita nella *proof;* quindi, la proof è l'effetto dell'evidence quando questa induce a concludere sulla verità o meno di fatti oggetto di una indagine[6].

Attribuire alla *digital evidence* il valore di prova prima ancora della celebrazione del processo è il risultato di una insufficiente conoscenza di ciò di cui si sta parlando o, nella migliore delle ipotesi, di una concezione inquisitoria del processo.

Se ci si confronta razionalmente con il fenomeno digitale, ci si accorge che la realtà risulta molto più complessa di quella che appare e che le rappresentazioni digitali non semplificano affatto la ricostruzione dei fatti.

[6] Cfr. voce "Evidence" in DE FRANCHIS F., Dizionario Giuridico. Inglese-Italiano, Giuffrè, Milano, 1984.

Sono questioni che attengono all'operato di tutti gli operatori forensi e degli altri attori impegnati nell'azione processuale penale: dal pubblico ministero (PM) che deve dirigere le indagini ad oggetto informatico o durante le quali emergano documenti informatici, alla polizia giudiziaria (PG) che deve acquisire su propria iniziativa o per delega del pubblico ministero gli elementi di prova digitale a carico o a discarico dell'indagato, ai loro tecnici in materia informatica che sono incaricati di compiere le attività materiali strumentali all'attività di indagine; dall'avvocato ai consulenti tecnici di parte che nell'ambito delle indagini difensive devono acquisire documenti informatici da produrre a discarico dell'indagato; dai cancellieri e agli altri ausiliari che dovranno conservare e custodire i reperti informatici, *rectius*: le memorie con i dati digitali in essi archiviati, sino ai Giudici che, con l'ausilio dei periti, dovranno riesaminare e giudicare la legittimità delle procedure seguite per l'acquisizione del materiale informatico e valutare il loro stesso contenuto al fine di ricostruire gli elementi di fatto e trarre le considerazioni di diritto necessarie per la decisione.

Il presente lavoro, muovendo da una prospettiva di ricostruzione storica e metodologica dell'Informatica forense, si propone di ripercorrere il rapporto tra prova informatica e processo penale alla luce delle innovazioni normative e della giurisprudenza che si sta formando sulle questioni e che presentano rilevanti criticità. L'intento è quello di dare un contributo critico al corretto inquadramento dei principali temi relativi al trattamento dei dati digitali a fini processuali.

Il primo capitolo verte sulla nascita e sviluppo della Computer forensics negli Stati Uniti.

Il secondo capitolo ripercorre le principali tappe dell'affermazione dell'Informatica forense in Italia dal punto di vista empirico, normativo, giurisprudenziale e accademico, per poi affrontare la collocazione sistematica e le problematiche definitorie della materia.

Il terzo capitolo affronta la questione dei presupposti tecnici dell'Informatica forense relativi alla dimensione ontologica e giuridica dei dati e dei bit.

Il quarto capitolo riguarda le questioni terminologiche e scientifiche della prova, nonché le principali innovazioni normative e tecniche rilevanti per l'Informatica forense.

Il quinto capitolo affronta la questione delle *best practice* in Informatica forense e le sentenze di merito più significative sul tema.

Il sesto capitolo esplora il tema della qualificabilità degli accertamenti tecnici informatici svolti durante le indagini alla luce sia delle norme codicistiche che della giurisprudenza di merito e della Cassazione.

Il settimo capitolo verte sulla questione della prova documentale informatica penale, con particolare attenzione alla verifica dell'attualità delle qualificazioni dottrinali in punto di prova documentale.

L'ottavo capitolo chiude la disamina prospettando l'esperimento giudiziale come esempio paradigmatico della ridefinizione in atto degli istituti processuali penali quale conseguenza delle innovazioni tecnologiche informatiche.

Ho obblighi di profonda gratitudine verso molte persone cui vanno i miei ringraziamenti:

al Prof. Enrico Pattaro, perché da studente mi ha inculcato la passione per lo studio dell'Informatica giuridica;

alla Prof.ssa Faralli, Direttrice del CIRSFID ed al Prof. Giovanni Sartor, perché convinti sostenitori dell'Informatica forense nell'ambito dell'Informatica giuridica;

a tutti i Colleghi di Dottorato del CIRSFID di Bologna e amici a me cari, Raffaella Brighi, Donato Caccavella, Massimo Melica, Pierluigi Perri, per i continui scambi di idee, consigli e incoraggiamenti.

Un ringraziamento particolare va a Michele Ferrazzano, autentico sperimentatore di Digital forensics, unico antagonista della legge di Murphy.

Infine, la mia affettuosa gratitudine e riconoscenza va al Prof. Cesare Maioli, che per primo in Italia ha intuito l'importanza scientifica dell'Informatica forense elevandola a scienza accademica: è solo grazie alla sua guida e al suo incoraggiamento che ho raggiunto questo traguardo.

Avvertenze:

- gli articoli indicati nel testo senza ulteriore specificazione nel testo si riferiscono al codice di procedura penale;
- il testo degli articoli citati e i relativi rimandi tra partentesi sono tratti o da ALIBRANDI, L., CORSO, P. (a cura di), Codice penale e di procedura penale, 44 ed., Piacenza, La Tribuna, 2016 o da www.brocardi.it.

1 Dalla Computer forensics all'Informatica forense

1.1 La Computer forensics negli Stati Uniti

La Computer forensics nasce negli Stati Uniti d'America come la disciplina che si occupa di studiare il dato informatico a fini processuali, e a partire dagli anni 70 ha conosciuto un rilevante sviluppo teorico e pratico.

In quegli anni, il panorama sociale e produttivo americano stavano subendo profondi cambiamenti a seguito della crescente e capillare diffusione delle tecnologie informatiche nei più disparati contesti sociali: dall'ambito comunicativo, a quello produttivo, a quello personale.

Di pari passo, la diffusione della tecnologia informatica determinava anche un incremento delle attività criminali nelle quali i dispositivi informatici, all'epoca per lo più computer tutt'al più collegati in rete, costituivano oggetto di reato (c.d. *computer crimes*), o strumento per la commissione di reato (c.d. *computer related crimes*), o quale o, più frequentemente, uno strumento contenente dati relativi relativi ai fatti oggetto di investigazione o indagine (*computer evidence*).

L'avanzato sviluppo tecnologico, il particolare sistema processuale (civile e penale), una capillare organizzazione degli organi investigativi, nonchè una risalente tradizione investigativa incentrata sul metodo empirico-scientifico, sono gli elementi che hanno favorito lo sviluppo di una intera branca specifica delle scienze investigative avente ad oggetto lo studio del computer come archivio di informazioni utile alla ricostruzione dei fatti processualmente rilevanti.

Dall'ampia diffusione della tecnologia informatica è derivata la crescente domanda di analisi di dati digitalizzati a fini investigativi, determinando così lo sviluppo delle tecniche della Computer forensics, caratterizzato sia dalla necessità di procedere adottando tecniche e strumenti che consentissero il rispetto dei principi e delle garanzie riconosciute dal sistema processuale americano, sia dall'applicazione della tecnologia informatica all'attività di investigazione.

In particolare, l'origine della Computer forensics va rinvenuta nella prassi investigativa sviluppatasi sui dispositivi informatici, correttamente ritenuti oltre che strumenti di commissione di reati, informatici o comuni, anche dei formidabili archivi di informazioni utili, talvolta indispensabili, per la ricostruzione ex post delle dinamiche oggetto di investigazione.

Il fenomeno dell'attenzione ai sistemi informatici è stata agevolata dalla cultura e dalla tradizione investigativa tipica della realtà statunitense,

storicamente rivolta all'applicazione dei principi, strumenti e metodologie scientifiche all'attività di acquisizione di informazioni utili alla ricostruzione ex post dei fatti rilevanti a fini giudiziari.

Tale approccio è stato imposto, o quantomeno avvantaggiato, dal sistema processuale americano basato sui principi del processo accusatorio (*due process of law*)[7] che, basato su una rigida ripartizione dell'onere probatorio tra la parte procedente e la parte resistente, gravando la prima dell'onere di provare l'assunto, fa sì che questa lo assolva facendo ricorso a tutte le informazioni assumibili legalmente. Pertanto, la parte procedente assume informazioni da ogni oggetto dal quale, sulla base delle costanti derivate dalle leggi scientifiche, possano fornire informazioni utili ad inferire gli accadimenti oggetti di accertamento processuale.

A tal proposito vanno ricordati i principi fondamentali del processo (penale) americano[8], quali la correttezza legale, sostanziale e processuale (*legal and procedural fairness*), il diritto a conoscere tempestivamente gli elementi di prova e le loro fonti (*timely notice of the charges*), il diritto alla legalità delle prove di colpevolezza (*guiltness must be proven by legally obtained evidence*), il sostegno della sentenza su elementi di prova legittimamente assunte (*the verdict must be supported by the evidence legally presented*).

Da tali principi discendono alcuni corollari.

Innanzitutto vige l'obbligo di rigore scientifico e metodologico nell'acquisizione dei mezzi di prova da esibire in dibattimento, se si vuole evitare che un approccio non rispettoso dei presupposti di fatto consentano alla controparte processuale di minarne l'affidabilità e il valore probatorio.

In secondo luogo, è onere principale della parte procedente (*Plaintiff*) esibire mezzi di prova a carico della parte resistente (*Defendant*) e quindi provare efficacemente gli assunti a sostegno della propria posizione processuale, oppure provare l'erroneità degli assunti della controparte minando così l'efficacia rappresentativa dei mezzi di prova avversari ove in mancanza l'azione rimane senza esito favorevole al procedente (*Actore non probante, reus absolvitur*).

In terzo luogo, è onere della parte resistente esibire a sua volta le prove a proprio discarico e quindi provare efficacemente gli assunti a sostegno della propria posizione processuale, oppure evidenziando la erroneità degli assunti della controparte minando l'efficacia rappresentativa dei mezzi di prova avversari.

---

[7] Cfr. voce "Due process of law" in BLAK, H. C., Blak's Law Dictionary, West Publishing CO, St. Paul, Minnesota (USA), 1990; cfr. anche MERCONE M., Diritto Processuale Penale, Simone, Napoli, 2001, p. 44 e ss.).

[8] Sulle caratteristiche salienti del processo penale americano, v. PALERMO G. B., STRONARDI V., AGOSTINI S., Il processo investigativo e accusatorio negli Stati Uniti d'America e in Italia, in Rivista di Psichiatria, Supplemento, 2012, 47, p. 42 e ss..

A seguito dello sviluppo delle reti, di Internet e delle telecomunicazioni basate su tecnologia digitale, tale approccio è stato esteso anche ai sistemi di teletrasmissione dei dati tra due o più punti della Rete. Ciò ha determinato la necessità di sviluppare tecniche e strumenti nuovi per l'intercettazione dei dati a fini processuali, secondo le procedure previste dalle norme processuali e dagli altri diritti fondamentali quali, ad es., quello alla libertà e segretezza della corrispondenza elettronica, delle comunicazioni telematiche e telefoniche, nonché alla riservatezza in generale.

Questo nuovo ambito è denominato *Network forensics* e studia le norme, le metodologie e gli strumenti per il trattamento dei dati a fini investigativi e giudiziari dei dati teletrasmessi per mezzo delle reti[9].

L'affermazione della Computer Forensics negli anni è stata progressiva e costante, investendo di pari passo tutti i dispositivi prodotto dell'evoluzione tecnologica, e articolandosi in ulteriori branche quali la *Mobile forensics*, relativa alle indagini sui dispositivi telefonici cellulari, tablet, altri dispositivi mobili come i GPS e da ultimo gli smartphone che, in rapporto alla loro modalità di funzionamento, assommando le caratteristiche e le problematiche di tutti gli altri dispositivi e sistemi digitali[10], e in rapporto alla loro diffusione ormai di gran lunga superiore a quella dei computer, si sta affermando come compendio di riferimento di tutte le problematiche della Computer forensics.

Computer forensics, Network forensics e Mobile forensics si sono successivamente affermate nelle aree di Common Law, i cui sistemi processuali sono caratterizzati dal modello processuale accusatorio (Regno Unito, Paesi del Commonwealth) per poi diffondersi, per effetto dell'influenza culturale e giuridica tra aree geografiche contigue, nelle aree di Civil Law dell'America Latina dove sono ricomprese nell'area disciplinare dell'*Informatica forense*[11].

1.2 L'oggetto della Computer forensics

La rilevanza assunta dalle Computer forensics nel panorama delle tecniche investigative americane, vede i primi tentativi di standardizzazione nei "Proposed Standards for the Exchange of Digital Evidence a cura dello Scientific Working Group on Digitale Evidence" (SWEDGE) International e dell'Organization on Digital Evidence (IOCE)[12] pubblicati nel 1998.

---

[9] V. CASEY E., Digital Evidence and Computer Crime - Forensic Science, Computer and the Internet, Academic Press, 2004.

[10] Gli *smartphone* assommano in sé le caratteristiche dei sistemi informatici e telematici, essendo dotati di memoria primarie, di memoria secondaria,, nonché di un sistema operativo che sovrintende alle funzioni di elaborazione, archiviazione, nonché del sistema di connessione e trasmissione telematica di dati digitali.

[11] AIRALA, A. D., op.cit., *passim*.

[12] SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE (SWEDGE), International Organization on Digital Evidence (IOCE), Proposed Standards for the Exchange of Digital Evidence, 1999, in Forensic Science Communications, 2000, Vol. 2 n. 2, in *https://www.fbi.gov*

Poco dopo, nell'ambito del "Handbook of Forensic Services" pubblicato nel 1999 sul sito dell'FBI, fu introdotto un elenco di tecniche per il trattamento dei dispositivi digitali a fini di giustizia[13]. Nella sezione del Manuale riguardante l'assicurazione e l'esame dei mezzi di prova, oltre agli oggetti tradizionali di investigazione[14], veniva elencata una nuova serie di servizi e tecniche per il trattamento ed esame a fini investigativi e giudiziari di reperti informatici, formalizzati come servizi di "Computer forensics" e, in tipico stile statunitense, organizzati secondo metodologie e strumenti standardizzati.

In relazione alle nuove esigenze, l'FBI aveva approntato e messo a disposizione di autorità, enti e agenzie pubbliche, una nuova competenza specifica per il trattamento a fini di indagine dei dispositivi e dei dati digitali, quali il sequestro dei dati (*data seizure*), la loro duplicazione (*data duplication*), la protezione e conservazione dei dati (*data preservation*), il recupero dei dati (data recovery), la ricerca di documenti (*document searches*), la conversione di formati (*media conversion*) e la formazione di consulenti tecnici (*expert witness services*).

In particolare, nel Manuale dei servizi forensi veniva esposta un'articolata serie di servizi relativa ai dati e ai dispositivi digitali: dall'"Analisi del computer", per cui i tecnici potevano eseguire operazioni di analisi del dispositivo in relazione al contenuto ("*Gli esami possono stabilire quali tipi di dati sono contenuti in un computer*"), alla comparazione dei dati ("*Gli esami possono comparare file di dati per conoscere il contenuto di documenti e file di dati),* alla ricostruzione della *s*uccessione di creazione dei dati ("*Gli esami possono determinare tempo e sequenza con la quale i file di dati furono creati"),* all'estrazione e recupero di file di dati cancellati dal computer ("*I file di dati possono essere estratti dal computer")*, alla conversione di formati ("*I file di dati possono essere convertiti da un formato ad un altro),* alla ricerca per parola chiave ("*I file di dati possono essere cercati per parola o frase ed i risultati possono essere registrati"*), alla ricerca e decifratura di password, di analisi e comparazione del codice sorgente anche se protetto, all'esame degli strumenti di memorizzazione di scrittura (macchine da scrivere, wordprocessor, ecc.), alla ricerca per testi o per campi, e quindi alla conduzione di laboratori dedicati allo svolgimento di tali attività.

/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/; v. anche NOBLETT M. G., POLLITT M.M., PRESLEY L.A., Recovering and Examining Computer Forensic Evidence, in Forensic Science Communications, 2000, Vol. 2 n. 4, in *https://www.fbi.gov/about -us/lab/forensic-science-communications/fsc/oct2000/index.htm/com puter.htm*.

[13] Cfr. il capitolo sull'"Evidence Examinations" in F.B.I. HANDBOOK OF FORENSICS SERVICES, 1999, in http://www.fbi.gov/hq/lab/handbook/forensics.pdf .

[14] L'FBI svolgeva già l'esame scientifico ad uso forense di elementi di prova costituiti da oggetti vari (vestiti, auto, armi), materiale biologico (sangue, saliva, DNA), impronte digitali, sostanze e materiali di vario tipo (legno, metalli, liquidi, esplosivi, sostanze chimiche e stupefacenti), fotografie, suoni, documenti cartacei e di ogni altro tipo.

L'FBI offriva le metodologie, procedure e i servizi di Computer forensics appena rassegnati ad un'ampia serie di destinatari: a favore degli uffici della stessa FBI decentrati sul territorio, agli organi statali della Pubblica accusa, ai tribunali militari, alle altre Agenzie federali quali il Dipartimento della Giustizia, della Difesa, della Sicurezza Nazionale, del servizio postale nazionale[15].

Nel 2001, sulla base di una ricerca sui reati informatici dalla quale si assumeva la necessità di una diffusa consapevolezza tra le forze dell'ordine statali locali dei problemi e delle pratiche di Computer forensics[16], il National Institute of Justice (NIJ), l'agenzia di ricerca e sviluppo del Dipartimento di Giustizia americano, vara una prima guida per le attività di primo sopralluogo[17].

Nel 2002, il Dipartimento di Giustizia, pubblicava la seconda versione del Manuale sulla "Perquisizione e sequestro di computer ed estrazione del mezzo di prova informatica nelle investigazioni penali"[18], aggiornata alle previsioni del Patriot Act[19] approvato a seguito dei fatti dell'11 settembre 2001, mentre lo IOCE presentava al G8 una prima serie di principi sulle procedure relative a mezzi di prova digitale[20].

Parallelamente, i contenuti della Computer forensics trovavano ampia diffusione anche in ampi settori aziendali (industrie, banche, assicurazioni, sanità, ICT), professionali (avvocati, investigatori privati e consulenti) e in enti non governativi, nell'ambito dei quali venivano prodotti studi per la raccolta e l'archiviazione di mezzi di prova informatici nel caso di violazione della sicurezza[21].

---

[15] Successivamente, a seguito della complessità e continua ricorrenza delle problematiche di investigazione in ambito digitale, i Dipartimenti e le Agenzie federali statunitensi si sarebbero dotate di autonomi servizi di Digital forensics che tuttavia trovano in Gruppi comuni di studio frequenti momenti di coordinamento e definizione delle pratiche e delle metodologie comuni.

[16] NATIONAL INSTITUTE OF JUSTICE (NIJ), Electronic Crime Needs Assessment for State and Local Law Enforcement, Washington, D.C., 2001, in *https://www.ncjrs.gov/pdffiles1/nij/186276.pdf*.

[17] Cfr. TECHNICAL WORKING GROUP FOR ELECTRONIC CRIME SCENE INVESTIGATION (TWGECSI), Electronic Crime Scene Investigation: A guide for First Responders, National Institute of Justice (NIJ), Washington D.C., 2001, in https://www.ncjrs.gov/pdffiles1/nij/187736.pdf; dopo qualche anno, è seguito il secondo manuale, Forensic Examination of Digital Evidence: A guide for Law Enforcement, National Institute of Justice (NIJ), Washington D.C., 2004, in *https://www.ncjrs.gov/pdffiles1/nij/199408.pdf*; per altri documenti prodotti dal NIJ nell'ambito della computer forensics, v. *https://www.ncjrs.gov/App/Search/SearchResults.aspx?txtKeywordSearch=digital+evidence& fromSearch=1*.

[18] UNITED STATES DEPARTMENT OF JUSTICE, Searching and Seizing Computers ad Otaining Electronic Evidence in Criminal Investigations, 2002, *http://www.finer-bering.com/GULAW_PDFs/s&smanual2002.pdf*.

[19] USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001), in *https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf*.

[20] Cfr. INTERNATIONAL ORGANIZATION ON COMPUTER EVIDENCE (IOCE), G8 Proposed Principles For The Procedures Relating To Digital Evidence, 2002, in http://www.ioce.org .

[21] Cfr. RFC 3227 - Guidelines for Evidence Collection and Archiving, Internet Society, 2002, in *http://www.rfc-base.org/rfc-3227.html*.

Negli stessi anni, diversi studiosi americani di Computer forensics, seppur con diverse sfumature, avanzavano varie definizioni dell'oggetto di studio della "Computer forensics" che, seppur con diverse sfumature, convergevano sostanzialmente su alcuni aspetti costituenti il denominatore comune: il trattamento dei dati informatici finalizzato ad un uso forense, e quindi investigativo e giudiziario, doveva essere effettuato secondo principi scientifici, metodologie tecniche certe e conformemente alle norme processuali.

Per Caloyannides, la Computer forensic "*...è la raccolta della tecnica e degli strumenti utilizzati per cercare un mezzo di prova in un computer"*[22].

Per Vacca, "*La Computer forensics concerne la protezione, identificazione, estrazione e documentazione della prova informatica memorizzata come dato o come informazione codificata magneticamente (...) altresì riguarda l'analisi forense del computer, l'esibizione elettronica, l'esibizione della prova elettronica, l'esibizione digitale, il recupero di dati, l'analisi del computer, mentre l'esame del computer è il processo di esaminare metodicamente i mezzi del computer (hard disk, floppy disck, nastri, etc.) per la prova.*[23]

Per Kruse II e Heiser, "*La Computer forensics (...) riguarda la conservazione, identificazione, estrazione, documentazione e interpretazione dei dati del computer*"[24]

Per Marcella e Greenfield, "*La Computer Forensics (...) tratta la conservazione, identificazione, estrazione e documentazione della prova informatica. (...) Come ogni altra scienza, la computer forensics riguarda l'uso di sofisticati strumenti tecnologici e procedure che devono essere seguite per garantire l'esattezza della conservazione della prova e l'esattezza dei risultati riguardanti l'elaborazione della prova informatica.*"[25].

Casey, infine, superando la categoria della Computer forensics, si rivolgeva allo studio della "digital evidence", definita come "*Ogni dato archiviato o trasmesso mediante un computer a sostegno o smentita di una teoria su come è*

---

[22] Cfr. COLOYANNIDES M. A, Computer Forensics and Privacy, Norwood, MA, 2001.

[23] Cfr. VACCA J. R., Computer Forensics – Computer Crime Scene Investigation, Charles River Media, Hingham, Massachusetts, 2002, Intr., XIX: "*Computer forensics involves the preservation, identification, extraction and documentation of computer evidence stored as data or magnetically encoded information (...) Computer forensics also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination, is the process of methodically examining computer media (hard disk, diskettes, tapes, etc.) for evidence.*".

[24] Cfr. KRUSE II W. G., e HEISER J.G., Computer Forensics: Incident Response Essentials, Addison-Wesley, Boston, USA, 2002, per i quali "*Computer forensics (...) involves the preservation, identification, extraction, documentation and interpretation of computer data.*"

[25] Cfr. MARCELLA A.J., GREENFIELD R.S., Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, USA, Auerbach, 2002, per i quali "*Computer Forensics (...) deals with the preservation, identification, extraction, and documentaton of computer evidence. (...) Like any other forensics science, computer forensics involves the use of sophisticated technology tools and procedures that must be followed to garantee the accuracy of the preservation of evidence and the accuracy of results concerning computer evidence processing.*".

stato commesso un reato o che indirizza elementi critici in merito al reato come il fine o l'alibi"[26].

L'*excursus* delle pur varie definizioni conferma la natura strettamente interdisciplinare della Computer forensics, la cui teoria e pratica non poteva prescidere dalla profonda intercorrelazione tra l'Information and Communication Technology (ICT) e il diritto nonché, per quanto rileva ai fini della presente disamina, del diritto penale e processuale penale.

Nel frattempo, la Computer forensics si è evoluta e diversificata rivolgendo l'attenzione ai diversi settori offerti dall'evoluzione tecnologica[27]. Difatti, oggigiorno, negli Stati Uniti, è la più ampia Digital forensics science[28] che ricomprende la Computer forensics[29] al fianco di altre branche analoghe quali la Network forensics, che attiene ai dati veicolati in rete, alla *Forensic data analysis*, che attiene all'analisi specifica dei dati, alla *Mobile devices forensics*, che attiene ai dati dei dispositivi mobili con particolare riguardo alla telefonia, alla *Database forensics*, che attiene all'analisi delle basi di dati.

[26] CASEY E., Digital evidence and computer crime. Forensics science, computers and the Internet, op.cit.; delle stesso Autore, v. anche Handbook of Computer Crime Investigation: Forensic Tools and Technology, Academic Press, 2001 e Handbook of Computer Crime Investigation, Academic Press, 2002.

[27] Sulla Computer forensics, v. anche ANASTASI J., The new forensics, John Wiley & Sons, 2003.

[28] Cfr. voce Digital forensics in *https://en.wikipedia.org/wiki/Digital_forensics*.

[29] Cfr. voce Computer forensics, in https://en.wikipedia.org/wiki/Computer_forensics, per la quale "*...is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.(...)"*.

2 L'Informatica forense in Italia

Anche in Italia, a seguito della diffusione delle tecnologie informatiche verificatasi nell'ultimo trentennio, si è verificato un incremento della domanda di analisi di dati digitali a fini processuali, soprattutto in ambito penale.

Tale domanda ha subito un rilevante incremento a seguito del concorso di almeno cinque distinti fenomeni, spesso in tutto o in parte coincidenti o convergenti.

Il primo di questi è un fenomeno tipicamente criminologico[30]: a partire dagli anni 90, si sono verificati diversi casi in cui reati a c.d. condotta libera e quindi non tipicamente informatici, come ad es. il danneggiamento, gli atti persecutori, la diffamazione on line, la violazione dei del diritto d'autore sulle opere dell'ingegno, ecc., stati commessi utilizzando sistemi informatici e telematici. In tali casi, lo strumento tecnologico ha costituito un elemento accidentale del reato che però ha caratterizzato la condotta integrante la fattispecie penale della condotta.

In tali situazioni, l'esigenza di analizzare i dati e gli altri aspetti informatici diventa imprescindibile per la corretta ricostruzione dei fatti[31].

Il secondo fenomeno è prettamente giuridico[32]: per contrastare l'aumento delle condotte lesive ai danni di strumenti informatici, telematici e di beni giuridici comuni commessi con tecnologie informatiche, dal 1993 in poi nel nostro ordinamento sono stati inseriti a più riprese nuove figure di reato strettamente connesse con la protezione dei dati e dei beni informatici, i c.d. reati informatici, in particolare ad opera della L. 547/93, della L. 48/08 e della normativa relativa alla pornografia infantile. In buona sostanza, la

[30] Per una panoramica sui reati informatici dal punto di vista criminologico, v. SERRA C., STRANO M., Nuove frontiere della criminalità – La criminalità tecnologica, Giuffrè Editore, Milano, 1997; STRANO M., Computer crime, Apogeo, 2000; FTI, Forum per la Tecnologia dell'Informazione, Osservatorio sulla criminalità informatica. Rapporto 1997, Franco Angeli, Milano, 1997 ; BOZZETTI, M., POZZI, P., (a cura di), Cyberwar o sicurezza ? Secondo Osservatorio Criminalità ICT, FTI, Franco Angeli, Milano, 2000; POZZI P., MASOTTI R., BOZZETTI M., op.cit.,; AA.VV., Crimes & computers (Delitti e computers), Presidenza del Consiglio dei Ministri, Dipartimento per l'Informazione e l'Editoria, Roma, Istituto Poligrafico e Zecca dello Stato, 2004; da ultimo, NERI G., Criminologia e reati informatici. Profili di diritto penale dell'economia, Jovene, Napoli, 2014, pp. 1 e ss..

[31] Per l'esame di un caso relativo ad un reato a condotta libera ante novella ex L. 547/93, sia consentito rinviare a GAMMAROTA A., Danneggiamento di sistema informatico della P.A. e informatica forense: un caso, op.cit., p. 207 e ss..

[32] Cfr. SOLA L., FONDAROLI D., A proposito della criminalità informatica, Editrice CLUEB, Bologna, 1992, SOLA L., FONDAROLI D., La nuova normativa in tema di criminalità informatica: alcune riflessioni, Editrice CLUEB, Bologna, 1993, CECCACCI, G., Computer Crimes – La nuova disciplina sui reati informatici, Edizioni FAG, Milano, 1994; FAGGIOLI, G., Computer Crimes, Edizioni Simone, Napoli, 1998.

criminalizzazione di determinate condotte ha creato la domanda di analisi di "fatti informatici" costituenti reato.

Il terzo fenomeno è costituito dalla crescente attenzione rivolta dalla polizia giudiziaria e dagli organi inquirenti ai dispositivi e sistemi digitali al fine di trarre informazioni utili all'accertamento di fatti costituenti ipotesi di reato, a prescindere dall'attinenza o meno della fattispecie con l'informatica. Infatti, in molti casi di procedimenti per fatti di omicidio, terrorismo, istigazione al suicidio, falso in bilancio, corruzione e molti altri ancora, i sistemi informatici e telematici rilevano solo come archivi di dati dai quali trarre informazioni sul comportamento delle parti coinvolte nel procedimento o per acquisire elementi di prova o indizi utili alle indagini. In buona sostanza, si inizia a trattare ogni dispositivo digitale alla stregua di una scatola nera personale che raccoglie dati dai quali si ritiene che possono essere tratte informazioni utili alle investigazioni per la ricostruzione *ex post* del comportamento degli individui coinvolti e dei fatti processualmente rilevanti. Tuttavia, come l'esperienza dimostra, l'evoluzione delle modalità di indagine non sempre è stata sostenuta da un affinamento delle metodologie applicate e dall'indispensabile attenzione alle tecniche proprie dell'informatica forense[33].

Il quarto fenomeno, parzialmente coincidente con il precedente, è derivato dal crescente utilizzo di sistemi informatici e telematici da parte degli investigatori e inquirenti per raccogliere dati digitali o informazioni direttamente dalle parti a vario titolo coinvolte nella realizzazione della fattispecie: in tale fenomeno rientrano tutti quei dispositivi software e hardware che vengono utilizzati, come ad esempio i c.d. siti civetta, detti anche *honeypot*, utilizzati nelle attività di contrasto alla pedopornografia[34] e, per le

[33] Sono ancora numerosi i casi nei quali durante la fase delle investigazioni di polizia giudiziaria è dato osservare un malgoverno degli elementi di prova digitale archiviati nei dispositivi digitali; v. ad es. Trib. Vigevano, sent. 17 dicembre 2009, pp. 37-63, in *http://static.repubblica. it/laprovinciapavese/pdf/SENTENZA_STASI.pdf*.

[34] Un sito civetta o *honeypot* (lett. "barattolo del miele"), v. in *https://it.wikipedia.org/wiki/Honeypot*, è un sistema hardware o software usato come "trappola" o "esca" a fini di protezione contro gli attacchi di pirati informatici . Il sistema può essere utilizzato nell'attività di contrasto alla pedopornografia dalla Polizia delle telecomunicazioni la quale, agendo sotto copertura, può attivare, anche per via telematica, siti nelle reti, realizzare o gestire aree di comunicazione o scambio su reti o sistemi telematici, ovvero per partecipare ad esse, nei quali realizzare scambi di materiale pedopornografico al fine di individuare i responsabili e reprimere tale attività illecita. Tale strumento è previsto dall'art. 14 (Attività di contrasto) della L. 3 agosto 1998, n. 269 (Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù.) il quale prevede "*(...) 2. Nell'ambito dei compiti di polizia delle telecomunicazioni, definiti con il decreto di cui all'art. 1, comma 15, della legge 31 luglio 1997, n. 249, l'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione svolge, su richiesta dell'autorità giudiziaria, motivata a pena di nullità, le attività occorrenti per il contrasto dei delitti di cui agli articoli 600-bis, primo comma, 600-ter, commi primo, secondo e terzo, e 600-quinquies del codice penale commessi mediante l'impiego di sistemi informatici o mezzi di comunicazione telematica ovvero utilizzando reti di telecomunicazione disponibili al pubblico. A tal fine, il personale addetto può utilizzare indicazioni di copertura, anche per attivare siti nelle reti, realizzare o gestire aree di comunicazione o scambio su reti o sistemi telematici, ovvero per*

intercettazioni ambientali o di flussi informatici e telematici, i c.d. captatori informatici[35], le sonde[36], i telemonitor[37].

partecipare ad esse. Il predetto personale specializzato effettua con le medesime finalità le attività di cui al comma 1 anche per via telematica. 3. L'autorità giudiziaria può, con decreto motivato, ritardare l'emissione o disporre che sia ritardata l'esecuzione dei provvedimenti di cattura, arresto o sequestro, quando sia necessario per acquisire rilevanti elementi probatori, ovvero per l'individuazione o la cattura dei responsabili dei delitti di cui agli articoli 600-bis, primo comma, 600-ter, commi primo, secondo e terzo, e 600-quinquies del codice penale. Quando é identificata o identificabile la persona offesa dal reato, il provvedimento é adottato sentito il procuratore della Repubblica presso il tribunale per i minorenni nella cui circoscrizione il minorenne abitualmente dimora. 4. L'autorità giudiziaria può affidare il materiale o i beni sequestrati in applicazione della presente legge, in custodia giudiziale con facoltà d'uso, agli organi di polizia giudiziaria che ne facciano richiesta per l'impiego nelle attività di contrasto di cui al presente articolo."; tale pratica, in assenza di determinati presupposti di legge, è stata già ritenuta illecita da Cass., Sez. III pen., sent. 5 maggio – 22 settembre 2004 n. 37074, Gullello, in *http://www.ictlex.net/?p=399*; con nota IASILLO A., Agenti provocatori e sequestro probatorio. Male captum, (non) bene retentum? in D & G. Diritto e giustizia, n. 40/2004, p. 40-46; v. Cass., Sez. III pen., sent. 17 febbraio-11 maggio 2005 n. 17662, Favalli, e Cass., Sez. III pen., sent. n. 17662/05.

[35] Il captatore informatico è costituito da un programma, un vero e proprio virus autoinstallante, che viene inviato da remoto (ad es. mediante un allegato ad una email) al dispositivo digitale obiettivo (che può essere indifferentemente un computer, un tablet, un telefono cellulare, uno smartphone) e di cui prendono il possesso, consentendo a chi lo gestisce di controllarlo in modo completo e svolgere sul sistema e sui dati qualunque operazione consentita all'utente dello stesso, quali ad es., attivare o disattivare funzioni, analizzare, modificare i dati, cancellarli, senza peraltro lasciare tracce dell'intervento nei file che gestiscono lo stesso dispositivo. Potendo il gestore del captatore azionare da remoto il microfono e la telecamera di cui il dispositivo è dotato, quest'ultimo viene usato come "cimice" per l'effettuazione di intercettazioni ambientali ai sensi dell'art. 266, 2° c., ; sul funzionamento e sull'impatto di tali dispositivi sull'assetto sociale e giuridico, v. Atti e documenti del Convegno E-Privacy 2015, Autumn Edition, Captatori informatici e società civile: una convivenza possibile? Cagliari, 16 e 17 ottobre 2015, in *http://e-privacy.winstonsmith.org/e-privacy-XVIII-programma.html*; in dottrina, v. TESTAGUZZA M., I Sistemi di Controllo Remoto: fra normativa e prassi, in Dir. pen. proc., 2014, p. 759, TORRE M., Il virus di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali, in Dir. pen. proc., 2015, p. 1163 e ss., e CAMON, A., art. 266 c.p.p., in AA.VV., Commentario breve al codice di procedura penale, a cura di CONSO G., ILLUMINATI, G., II ed., Padova, 2015, p. 1016 e ss.; sui limiti giuridici all'utilizzabilità del captatore informatico, v. Cass., Sez. Un., c.c. 28 aprile 2016, Pres. Canzio, Rel. Romis, Ric. Scurato (informazione provvisoria, in attesa della pubblicazione delle motivazioni), in http://www.penalecontemporaneo.it ; per l'ordinanza di rimessione della questione alle Sezioni Unite, v. Cass. pen., sez. VI, 10 marzo 2016 (dep. 6 aprile 2016), n. 13884, Pres. Carcano, Rel. Fidelbo in http://www.penalecontemporaneo.it ; per l'orientamento contrario all'uso dei captatori informatici, v. Cass., sez. VI penale, 26 maggio 2015 (dep. 26 giugno 2015), n. 27100, in *http://www.penale.it*.

[36] La sonda viene collocata presso l'*access provider* per captare il traffico di dati intercorrente nelle due direzioni tra due dispositivi intercettati e trasferirlo ad un terzo dispositivo che archivia e consente di leggere i dati scambiati; sui sistemi di captazione dati e sugli aspetti giuridici, v. Relazione del Gruppo di studio del 6 luglio 2011 coordinato da BONOMO, A., su "Le investigazioni con l'impiego di intercettazioni di comunicazioni e di flussi informatici o telematici. I nuovi strumenti di comunicazione telematica ed informatica: aspetti tecnici e questioni giuridiche coordinatore", CONSIGLIO SUPERIORE DELLA MAGISTRATURA, Incontro di studi sul tema "Tecniche di indagine e rapporti tra p.m., polizia giudiziaria, consulenti tecnici e difensori", Roma, 4-8 luglio 2011, in http://docplayer.it/5178908-Consiglio-superiore-della-magistratura-le-investigazioni-con-l-impiego-di-intercettazioni-di-comunicazioni-e-di- flussi-informatici-o-telematici.html .

[37] I *telemonitor* sono dispositivi hardware che possono essere installati in vari punti di diverse linee per captare i dati dell'intercettando e deviarne una copia su un dispositivo remoto di archiviazione che a disposizione per il successivo esame a fini di indagine.

Il quinto e ultimo fenomeno è dato dall'affinamento delle metodologie difensive ed investigative a disposizione del difensore il quale, per svolgere il suo compito, deve confrontarsi con indagini e investigazioni ad oggetto informatico e telematico o svolgerne di propria iniziativa nell'ambito delle facoltà di investigazione difensiva previste dalla L. 7 dicembre 2000 n. 397, per cui a sua volta ha, o deve sviluppare profonde competenze nell'ambito dell'Informatica forense.

In conclusione sul punto, il comune denominatore dei fenomeni appena rassegnati è costituito dal fatto che l'attività di indagine e investigativa, anche solo difensiva, svolta dalle parti del procedimento è incentrata sui dati digitalizzati e, quindi, sui bit dai quali le parti del procedimento (e del processo) traggono informazioni costituenti, sotto il profilo giuridico, indizi ed elementi di prova.

Tuttavia, la disciplina dell'Informatica forense, lentamente affermatasi in Italia solo a partire dalla prima metà del 2000, e quindi con grande ritardo rispetto agli Stati Uniti, ad oggi non ha ancora trovato pieno riconoscimento teorico e pratico.

Sul piano più eminentemente pratico, i motivi del ritardo sono dipesi da diversi fattori.

Innanzitutto la più lenta diffusione delle tecnologie informatiche e quindi il minor numero di reati informatici hanno comportato una minor domanda di analisi di dati a fini giudiziari.

Inoltre, un ruolo preponderante è stato giocato dalla diversa tradizione processuale, quella italiana basata ancora su schemi e ideologie processuali di tipo inquisitorio che non agevolano, e talvolta ostacolano, l'affermazione di elementi e schemi più aderenti al processo di parte.

In terzo luogo, hanno avuto rilievo le endemiche ristrettezze del bilancio statale che non favoriscono la logistica, l'aggiornamento tecnologico, la formazione degli operatori pubblici rispetto alle nuove competenze richieste dall'evoluzione tecnologica.

Infine, la complessità della nuova disciplina, conseguente alla profonda commistione di elementi tecnico-informatici e giuridici, ha costituito un ostacolo per tutti gli operatori forensi i quali, per converso, hanno assunto posizioni di resistenza passiva all'innovazione degli schemi normativi e tecnici.

Sul piano teorico, invece, rileva il diverso assetto processuale che caratterizza lo scenario giuridico italiano rispetto a quello statunitense.

Infatti, il sistema processuale civile italiano è caratterizzato dal principio della disponibilità della prova e da un tradizionale *favor* per le prove costituite rispetto a quelle costituende. Per quanto i dati informatici possano rientrate nel novero delle prove costituite o precostituite rispetto al momento celebrativo del processo, la loro corretta acquisizione, presupposto della corretta valutazione, è soggetta a tempi e tecniche che richiedono l'intervento di un ausiliare del

giudice, previo giudizio riguardante i presupposti di ammissibilità del mezzo istruttorio[38].

Tuttavia, la facile modificabilità dei dati, l'inadeguatezza degli strumenti processuali, e l'innegabile arretratezza culturale o insensibilità verso il problema da parte degli attori processuali e degli organi giudicanti, fanno si che tali acquisizioni corrano spesso il rischio di essere infruttuose o addirittura controproducenti. Pertanto, predomina ancora una certa tendenza a privilegiare i surrogati e i sottoprodotti dei dati digitali, come ad esempio le copie semplici di file, le stampe di file, finche di pagine web (magari con la variante tranquillizzante dell'autentica di un notaio), le copie di copie di file e quant'altro possa far luogo dei documenti digitali originari.

Tali surrogati di mezzi di prova sono magari valutati in modo difforme dal modello legale, così scavalcando a piè pari – e a dire il vero con una certa approssimazione – molti problemi di ammissibilità del mezzo istruttorio.

Lo stesso fenomeno è invalso per diverso tempo nell'ambito del processo penale.

La dottrina d'oltreoceano e nazionale[39] hanno già dimostrato come ogni insieme di bit, e quindi ogni documento informatico digitalizzato in base a processi di registrazione su supporti (chip, hard disk, floppy disk, flash memory, ecc.), sia assiomaticamente soggetto a multiple e ampie modifiche ad ogni avvio del sistema[40] e ad ogni minima interazione con il dispositivo, anche non volutamente modificativo dell'insieme dei file. In particolare, sono soggetti a profonde modifiche proprio quei dati esterni ai file e generati dal sistema informatico, i c.d. metadati[41], ovvero proprio quei dati dai quali vengono tratte le informazioni utilizzate nella ricostruzione processuale dei fatti. Nonostante ciò, larga parte della giurisprudenza continua invece a ritenere che un sistema informatico (e finanche quello telematico) sia progettato e utilizzato proprio per

---

[38] Sulle prove digitali in ambito processual civilistico, cfr. NOVARIO F., Le prove informatiche nel processo civile, Giappichelli, Torino, 2014.

[39] Cfr. MAIOLI C., Dar voce alle prove: elementi di Informatica forense, in POZZI P., MASOTTI R., BOZZETTI M., (a cura di), Crimine virtuale, minaccia reale. Francoangeli, 2004, p. 66 e ss..

[40] Ai fini della presente disamina:
- per sistema digitale, per quanto differenziato, intendo l'archetipo di sistema informatico e telematico composto da uno o più sistemi di input di dati, da una memoria primaria, da una memoria secondaria, da uno o più sistemi di output o di trasmissione dati, da un sistema operativo che ne gestisce le varie funzionalità, da uno o più eventuali programmi applicativi, dai dati in formato digitale e da un sistema di ricerca dati; dalla variegata ingegnerizzazione di tali componenti e funzioni nei vari dispositivi più o meno differenziati secondo il servizio cui è dedicato, sono derivate le molteplici forme di dispositivi;
- per dispositivo digitale, intendo l'insieme dei dati digitali e dello strumento di elaborazione e/o archiviazione sul quale essi sono archiviati;
- per reperto digitale, intendo un uno o più componenti del sistema informatico o un dispositivo rilevante a fini processuali;

[41] I dati esterni ai file, o metadati, sono quei dati accessori ai file, generati automaticamente dal sistema informatico e telematico, quali il tipo di file, (ad es. .doc, .PDF, .TXT), le dimensioni, le date di creazione, di modifica, di ultimo accesso, ecc..

mantenere inalterati i dati memorizzati, ignorando come invece vi siano molti dati che vengono modificati, e più volte, direttamente dal sistema e senza che l'utente se ne accorga.

Solo verso i primi anni del 2000, le tecniche della Computer forensics hanno iniziato a prendere piede nell'ambito delle attività investigative relative ad alcuni gravi fatti di terrorismo e, successivamente, per le attività di contrasto alla diffusione della pedopornografia.

In tali circostanze, muovendo dall'acquisizione e analisi dei dispositivi informatici e dei dati in essi registrati sono state adottate nuove tecniche di ricerca di indizi ed elementi di prova utili alla ricostruzione dei fatti oggetto di indagine.

Quale materia di insegnamento universitario, infine, mentre negli Stati Uniti la Computer forensics è prevista in numerose Università maggiori e minori con articolati percorsi di perfezionamento e produce migliaia di laureati all'anno, in Italia sono ancora sparute le Università che contemplano un corso di studi o di perfezionamento in Informatica forense[42].

2.1 La definizione di Informatica forense

Mentre l'inquadramento scientifico e metodologico risultava già delineato dall'esperienza d'oltreoceano, in Italia si poneva la particolare relativa alla traduzione dell'espressione Computer forensics, per non incorrere nel rischio di ricorrer ad espressioni inadeguate come Informatica legale o Infortunistica informatica.

La prima espressione appariva scarsamente descrittiva e fuorviante in quanto avrebbe richiamato un senso di conformità dell'informatica alla legge in contrapposizione del concetto di "informatica illegale"; la seconda appariva riduttiva in quanto richiamava la limitazione dell'oggetto all'attività di accertamento e liquidazione dei danni derivanti dagli "infortuni informatici" (?), al pari dell'analogo fenomeno registratosi negli ultimi due decenni circa le tecniche di determinazione dei danni da circolazione stradale (c.d. infortunistica stradale).

Entrambe le espressioni apparivano comunque riduttive in quanto incapaci di cogliere appieno l'ampio oggetto di studio e pratica proprio della Computer forensics.

[42] Sull'insegnamento dlel'informatica forense, v. MAIOLI C., CANESTRARI S., On the preparation of better law graduates and ICT jurist, in Eleventh International Conference on Substantive Technology in Legal Education and Practice, (atti del Convegno SubTech 2010, Saragozza, 1-3 luglio 2010) University of Zaragoza Press, Saragozza, 2010, pp. 24 – 33; sullo specifico riferimento all'insegnamento dell'Informatica forense presso l'Università di Bologna, cfr. MAIOLI C., L'insegnamento dell'informatica giuridica: il contributo dell'Università di Bologna, in PERUGINELLI G., RAGONA M., (a cura di), L'informatica giuridica in Italia, ESI, Napoli, 2014, pp. 109.

Invero, poiché in Italia le prime esperienze teoriche e applicative dei principi e delle tecniche della Computer forensics si erano sviluppate in ambito penalistico, l'Informatica forense apparve naturalmente inquadrabile tra le scienze ausiliare all'applicazione del diritto penale e processuale penale, secondo la tradizione classificatoria dei più autorevoli Autori di tali discipline[43].

Difatti, l'Informatica forense trovava naturale applicazione operativa nell'alveo delle procedure dell'investigazione criminale, ovvero in quel particolare metodo investigativo che, secondo una tradizione ormai consolidata, si basa sull'applicazione delle conoscenze scientifiche e della tecnologia per lo studio delle tracce finalizzato all'accertamento dei fatti costituenti oggetto di investigazione e indagine[44]. Inoltre, per la diretta rilevanza processuale che assumono gli atti e gli effetti delle attività investigative in materia informatica, l'Informatica forense è indissolubilmente intrecciata al diritto processuale penale.

Tuttavia, ciò che rimane predominante nell'Informatica forense è l'intreccio tra il diritto e l'informatica che si rinviene trasversalmente anche in altri ambiti dell'ordinamento, quali il diritto sostanziale e processuale civile, il diritto del lavoro, il diritto amministrativo e il diritto tributario, motivo per il quale l'Informatica forense trovava sviluppo teorico proprio nell'ambito dell'Informatica giuridica[45].

---

[43] Cfr. ANTOLISEI F., Manuale di diritto penale, Parte generale, Giuffrè, Milano, 1987, p. 26, dove è delineata la sistematica delle scienze ausiliarie al diritto penale, ovvero le scienze criminalistiche (antropologia criminale, psicologia criminale, sociologia criminale la medicina legale (medicina legale, psichiatria forense, psicopatologia forense, tossicologia forense, psicologia giudiziaria), sia tra quelle di polizia scientifica. In tale sistematica, l'Informatica forense sarebbe collocabile tra le scienze criminalistiche e tra quelle di polizia scientifica; nell'ambito di analoga sistematica, cfr. MANTOVANI F., Diritto Penale, Parte generale, Padova, 1992, p. 10, tra le c.d. scienze criminali (diritto penale, criminologia, filosofia e storia del diritto penale, diritto penale processuale, politica criminale), viene collocata la tecnica dell'investigazione criminale e nell'ambito di questa si annoverano altre scienze quali medicina legale, dattiloscopia, antropometria, balistica giudiziaria, Grafometria, tossicologia forense, psicologia giudiziaria, psichiatria forense, al fianco delle quali può essere classificata anche l'Informatica forense.

[44] Per gli aspetti giuridici delle investigazioni e indagini scientifiche, v. CHELO A., Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria, Cedam, Padova, 2014.

[45] Sui prodromi dell'Informatica giuridica, v. FROSINI V., Cibernetica, diritto e società, Edizioni di comunità, Milano, 1968; per l'oggetto ed il metodo dell'informatica giuridica, v. FROSINI V., Informatica, diritto e società, II ed., Giuffrè, Milano, 1982; LOSANO M., Informatica per le scienze sociali. Corso di informaticca giuridica, Einaudi, Torino, 1985; GIANNANTONIO E., Manuale di diritto dell'informatica, II ed., Cedam, Padova, 1997; BARBARISI M., Diritto e informatica, Edizioni Simone, Napoli, 1997, p.7 e ss.; HANCE O., Internet e la legge, McGraw-Hill, Milano, 1997; NESPOR S., Internet e la legge, Hoepli, Milano, 1999; TADDEI ELMI, G., Corso di informatica giuridica, Simone, Napoli 2003; CEVENINI C., DI COCCO, C., SARTOR, G., Lezioni di informatica giuridica, Gedit, Bologna, 2005; SARTOR, G. L'informatica giuridica e le tecnologie dell'informazione, Giappichelli, Torino, 2012; più di recente, sul diritto del'informatica, v. PATTARO E., (a cura di), Manuale di diritto dell'informatica e delle nuove tecnologie, Cedam, Padova, 2000; CIACCI G., Le fonti del diritto dell'informatica, in VALENTINO, D., (a cura di) Manuale di diritto dell'informatica, II ed., ESI, Napoli, 2011, p. 7 e ss.; FINOCCHIARO G., DELFINI F.,

2.2 L'oggetto e gli scopi dell'Informatica forense

La trasversalità delle problematiche studiate all'Informatica forense rispetto a molti altri ambiti diversi dal diritto penale e processuale penale è resa attuale dalla pervasività dei cambiamenti tecnologici e sociali, nonchè dalle recenti riforme legislative verificatesi in vari settori del diritto processuale.

Tuttavia, le riflessioni e le tecniche maturate nell'ambito dell'Informatica forense si prestano, previo opportuni adattamenti, ad essere mutuati in altri settori della scienza giuridica stante proprio il carattere trasversale dei temi presupposti, comuni a qualsiasi ambito nel quale si renda necessario trattare dati digitalizzati a fini processuali.

Per questo, quando nel maggio 2003 ebbi modo di esporre per la prima volta i tratti salienti dell'Informatica forense[46], lo sforzo definitorio necessario a sintetizzarne l'ampiezza e la complessità dell'oggetto di studio non fu molto efficace se fu necessario descriverla come: "*la scienza che concerne le attività di individuazione, conservazione, protezione, estrazione, documentazione ed ogni altra forma di trattamento ed interpretazione del dato informatico memorizzato su supporto informatico, al fine di essere valutato come prova nel processo. L'Informatica Forense si occupa altresì di studiare a fini probatori i processi, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici (memorie, hard disk, dischetti, nastri, cartaceo, etc.), nonché l'analisi forense di ogni sistema informatico e telematico (computer, rete di computer, ed ogni altro dispositivo per il trattamento di dati in formato digitale), l'esibizione della prova elettronica, l'esibizione del dato digitale, il recupero di dati e la loro esibizione, l'analisi ed esame del sistema informatico e telematico".*

Si trattava di un primo tentativo di comporre in un unico quadro definitorio sia i molteplici aspetti tecnico-informatici delle nuove metodologie, sia il quadro giuridico della disciplina, in una fase storica nella quale, essendo la dottrina rara e ignorando la giurisprudenza tali fenomeni, l'ordinamento italiano non conosceva tale materia né le sue ampie e raffinate potenzialità a fini conoscitivi e processuali.

Da allora sono passati molti anni e soprattutto sono intervenuti tutti i molteplici fattori evolutivi già esposti, che hanno portato ad una diversa e più efficace circoscrizione dell'ambito di operatività dell'Informatica forense.

A seguito di miglior rielaborazione che ha portato ad una definizione sintetica dei temi in esame, si può affermare che "**L'informatica forense**

(a cura di), Diritto dell'informatica, Utet Giuridica, Milano, 2014; PERUGINELLI G., RAGONA M., (a cura di), op.cit.

[46] La prima definizione dell'oggetto dell'Informatica forense fu esposta nel maggio 2003, nel corso della presentazione dal titolo "Dalla Computer Forensics all'Informatica forense" svolta nell'ambito della seconda edizione del Master in Diritto delle nuove tecnologie organizzato dal Centro Studi di Informatica Giuridica di Bari, come da GALEOTTI P., Master-Post eventum 12.05.03, in *http://www.avvocatiacquavivacassano.it* .

studia le norme giuridiche e le tecniche informatiche per il trattamento dei dati digitali a fini processuali."

L'espressione "Informatica forense" è stata mutuata da quella che i latinoamericani usano per indicare la Computer forensics e che fa riferimento all'applicazione dei principi e delle tecniche proprie della scienza informatica e delle sue articolazioni al procedimento di accertamento giudiziale dei fatti per l'applicazione della legge.

Secondo tale definizione, l'oggetto di studio dell'Informatica forense è costituito dai seguenti elementi:

1. dalle norme di diritto sostanziale e processuale che talvolta, anche solo latamente, riguardano l'utilizzo di sistemi informatici e telematici nonché i dati digitali; tali norme possono essere di diritto interno e internazionale, di diritto dell'Unione Europea, diritto costituzionale, diritto penale e processuale penale, diritto civile, commerciale, processuale civile, diritto amministrativo, e da ultimo di diritto tributario, ma non è esclusa nessuna branca del diritto, anche extra ordinamentale[47];
2. dalle tecniche informatiche in senso ampio[48] con particolare riguardo alla scienza dell'informazione, alle tecniche di rappresentazione e trattamento dell'informazione codificata, all'architettura e funzionamento dei computer, delle reti telematiche e ai sistemi di telecomunicazioni, ai dispositivi digitali, anche telefonici, ai sistemi operativi, alle basi di dati, alla programmazione, alla crittografia e crittoanalisi, purché finalizzate al trattamento dei dati digitali per trarne informazioni utili alla ricostruzione dei fatti processualmente rilevanti e con modalità complianti con le norme giuridiche;
3. dagli standard internazionali pubblicati dall'ISO/IEC[49], organismi sovranazionali a composizione mista, pubblico-privato, che perseguono l'obiettivo della standardizzazione di beni, servizi e procedure. Proprio in relazione al trattamento dei dati digitali a fini probatori, l'ISO/IEC ha recentemente intrapreso un'ampia produzione di standard per l'informatica Forense aventi ad oggetto norme tecniche discusse e riconosciute a livello internazionale, versate nei seguenti documenti[50]:

[47] Si pensi alla rilevanza dell'informatica forense nei casi di procedimenti a struttura contenziosa previsti ad es. dagli ordinamenti professionali per l'applicazione dei codici deontologici, o dall'ordinamento sportivo, o addirittura dagli ordinamenti diversi da quello statale come nel caso del processo previsto dall'ordinamento canonico, o di quello previsto dagli organismi arbitrali, pubblici o privati, statali e internazionali.

[48] L'oggetto ricomprende l'ampio ambito dell'ICT.

[49] Organizzazione Internazionale per la Standardizzazione (ISO) e Commissione Elettrotecnica Internazionale (IEC).

[50] In linea di prima approssimazione, va rilevato che tali Standard sono costituiti da linee guida che non fanno riferimento nè alle norme giuridiche di singoli paesi, nè a specifici prodotti o strumenti per il compimento delle operazioni.

- “ISO/IEC 27037:2012 Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence” pubblicato in versione definitiva il 15 ottobre 2012 (Linee guida per l’identificazione, raccolta, acquisizione e conservazioni delle prove digitali);
- “ISO/IEC 27038:2014 Information technology - Security techniques - Specification for digital redaction” pubblicato in versione definitiva il 13 marzo 2014 (Linee guida per le specifiche di redazione digitale);
- “ISO/IEC 27041:2015 Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative method” pubblicato in versione definitiva il 15 giugno 2015 (Linee guida sulla garanzia di idoneità e adeguatezza dei metodi di investigazione);
- “ISO/IEC 27042:2015, su “Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence” pubblicato in versione definitiva il 19 giugno 2015 (Linee guida per l’analisi e l’interpretazione di prove digitali);
- “ISO/IEC 27043:2015 “Information technology - Security techniques - Incident investigation principles and processes” pubblicato in versione definitiva il 1 marzo 2015 (Principi e processi per l’investigazione di incidenti informatici).

Ampliando i limiti della definizione sintetica, nello spettro di indagine dell’Informatica forense rientrano lo studio sia delle tecniche, metodologie, procedure e strumenti per l’individuazione, estrazione, conservazione, protezione, analisi, documentazione, interpretazione e valutazione dei dati digitali a fini processuali, sia lo studio delle norme dell’ordinamento giuridico che ne regolano l’ammissione, l’assunzione e la valutazione in qualsivoglia procedimento.

Inoltre, quanto all’oggetto specifico di indagine, rientra lo studio del trattamento dei dati digitali sia nella loro condizione statica, allorquando sono memorizzati su un supporto (Computer Forensic), sia nella loro condizione dinamica allorquando vengano trasmessi tra due dispositivi (Network forensic).

In quanto scienza che studia le applicazioni dell’informatica all’accertamento dei fatti processualmente rilevanti, ed essendo caratterizzata dalla compenetrazione tra le problematiche di natura tecnica (informatica) e giuridica, sia a livello empirico che epistemologico, l’Informatica forense rientra a pieno titolo nel novero delle scienze forensi quali la medicina legale, la biologia forense, la balistica forense, e le altre scienze le cui tecniche e metodologie sono utilizzate per l’applicazione del diritto.

Circa il metodo di approccio alle questioni oggetto di studio, l'Informatica forense, al pari delle altre scienze forensi, si giova dell'applicazione delle tecniche e delle metodologie delle branche coinvolte, e quindi delle scienze giuridiche per quanto riguarda la componente giuridica e dal metodo scientifico per quanto riguarda la componente informatica, avvinte da una stretta interdisciplinarietà. Nell'ambito del rapporto dialettico tra scienze di diversa natura, ciascuna componente apporta un contributo di conoscenza, per quanto il fine ultimo sia costituito dall'applicazione della legge (o delle norme previste dal diverso ordinamento), cosicché la funzione dello strumento scientifico, fermo restando il rispetto dei propri principi e metodi, resta ancillare rispetto allo scopo giuridico.

Secondo la tradizione ereditata dalla Computer forensics, tali tecniche trovano campo privilegiato di applicazione nell'ambito criminale, per cui la sede scientifica elettiva dell'Informatica forense sarebbe quella processual penalistica.

Per quanto attiene all'ambito processual penalistico, le tecniche dell'Informatica forense trovano più frequente applicazione alle seguenti tipologie di reati:

1. reati comuni in cui il dispositivo digitale, le cui funzioni di produzione e/o trasmissione di dati digitali, e/o i dati stessi, costituiscono lo strumento per la realizzazione di tutta o di parte della condotta e/o dell'evento del reato, o di una sua circostanza (ad es. l'art. 612 bis, c. 2, c.p. Atti persecutori, nel caso in cui *"...il fatto è commesso attraverso strumenti informatici o telematici"*);
2. reati informatici in senso stretto, in cui il dispositivo digitale, le sue funzioni di produzione e/o trasmissione di dati digitali, o il sistema informatico e/o i dati stessi, costituiscono l'oggetto della tutela penale ex L. 547/93 e L. 48/08[51];
3. reati comuni e/o speciali, per le cui indagini vengono acquisiti e analizzati dati generati dai dispositivi digitali che costituiscono indizi, o elementi di prova.

Nonostante l'ambito penale costituisca il terreno elettivo per l'Informatica forense, l'approccio scientifico alla gestione dei dati digitali ad uso giudiziale sviluppato in tale ambito è mutuabile, con gli opportuni adattamenti, agli altri

[51] Sui reati informatici, v. oltre; in prima approssimazione, fra tutti, v. GALDIERI P., Teoria e pratica nell'interpretazione del reato informatico, op.cit.; PICA G., Diritto penale delle tecnologie informatiche, op.cit.; PECORELLA C., Il diritto penale dell'informatica, Cedam, Padova, 2000; PICOTTI L., Reati informatici in Enciclopedia giuridica, op.cit., p. 1-33; SARZANA DI S. IPPOLITO, C., Informatica, Internet e diritto penale, Giuffrè, Milano, 2003; BUFFA F., Informatica, internet e diritto penale, II ed., Giuffrè, Milano, 2003; CUOMO L., RAZZANTE R., La nuova disciplina dei reati informatici, Giappichelli, Torino, 2009, AMATO G., DESTITO V. S., DEZZANI G., SANTORIELLO, C., I reati informatici, Cedam, Milano, 2010; LUPARIA L., (a cura di), Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest, Giuffrè, Milano, 2009.

sistemi processuali previsti dall'ordinamento giuridico, in quanto interessati dalle medesime problematiche quale portato del progresso tecnologico e delle recenti riforme legislative.

Inoltre, l'Informatica forense può e dovrebbe trovare applicazione anche nei procedimenti amministrativi nei quali ai dati in formato digitale viene riconosciuto valore probatorio, come ad es. ai procedimenti per accertamento delle violazioni amministrative[52]

Infine, come si è già accennato, l'Informatica forense trova applicabilità a tutti i casi di procedimenti a struttura contenziosa, pubblici o privati, statali e internazionali, nei quali il dato digitale viene assunto come elemento di prova.

Il riconoscimento dell'Informatica forense in Italia come autonomo oggetto di studio ha attraversato tre distinte fasi.

Durante la prima fase, durata sino agli inizi del 2000, circa, nonostante l'introduzione nell'ordinamento dei crimini informatici ad opera della L. 547/93, l'Informatica forense ha conosciuto teorizzazioni prevalentemente finalizzate all'applicazione pratica[53]. Difatti, la dottrina italiana si è concentrata sullo studio dei reati informatici, gettando le basi del diritto penale dell'informatica, trascurato completamente il momento applicativo delle norme procedurali.

Tuttavia, i nuovi *input* investigativi incentrati sulla ricerca di informazioni utili al procedimento partendo dai sistemi informatici e telematici hanno

---

[52] Vi sono numerosi casi nei quali dati digitali prodotti da sistemi informatici e telematici vengono usati a fini probatori nell'ambito di procedimenti formalmente amministrativi ma sostanzialmente contenziosi quali, ad esempio: le procedure di accertamento automatizzato delle violazioni al Codice della Strada effettuato mediante dispositivi digitali come i sistemi di rilevazione automatizzata della velocità (ad es. sistemi Photored, Autovelox, Tutor), nei quali l'accertamento della violazione è mediato da sistemi digitali ed il cui risultato ha valore di mezzo di prova nell'ambito del procedimento sanzionatorio; i prelievi e analisi di campioni di sostanze mediante sistemi digitali ai fini dell'applicazione della normativa sugli alimenti e bevande; infine, le rilevazioni di dati delle presenze dei dipendenti pubblici sul posto di lavoro effettuate con dispositivi digitali e utilizzati ai fini dei procedimenti disciplinari e sanzionatori. In tali casi e altri analoghi, la funzione sostanzialmente probatoria dei dati digitalizzati impone, a chi intende servirsene, l'onere di preventiva adozione delle tecniche di Informatica forense.

[53] È emblematico come sul piano sociologico-criminologico, era già da tempo avvertita l'esigenza di coniugare le esigenze di indagine con i diritti fondamentali e le garanzie previste dall'ordinamento processuale; ad es. v. CHICCARELLI S., MONTI A., Spaghetti hacker - Storie, tecniche e aspetti giuridici dell'hacking in Italia, Apogeo, 1997, pp. 260 e ss. e GUBITOSA C., ASSOCIAZIONE PEACELINK, Italian crakdown, BBS amatoriali, volontari telematici, censure e sequestri nell'Italia degli anni '90, Apogeo, 1999, pp. 50 e ss. . Tuttavia, sino ai primi anni del 2000, non sembrano esservi contributi di diritto penale dell'informatica (v. sopra) o di manuali di informatica giuridica nei quali compaia l'espressione Informatica forense; a tal proposito, v. GIANNANTONIO E., Manuale di diritto dell'informatica, op.cit., p. 441 e ss.; VETTORI, G., Reati connessi a Internet: profili processuali penali e tutela dell'indagato, in GAUDENZI SIROTTI, A., (a cura di), Internet e diritto. Problemi e soluzioni, Gedit, Bologna, 2001, p. 125. CASSANO G., (a cura di), Diritto delle nuove tecnologie informatiche e dell'Internet, Ipsoa, Milano, 2002, p. 1375 e ss.; RUGGIERI F., Profili processuali nelle indagini sui reati informatici, in PASCUZZI G. (a cura di), Diritto e informatica, Giuffrè, Milano, 2002, p. 147 e ss.; TADDEI ELMI G., Corso di informatica giuridica, Simone, Napoli, 2003, p. 123 e ss..

iniziato a compulsare l'evoluzione di nuovi approcci difensivi. Durante tale fase, l'applicazione di tecniche rudimentali ha portato risultati che, sottoposti al vaglio dibattimentale nelle successive fasi decisorie del processo (*de libertate*, dibattimentali, di legittimità), hanno evidenziato un'ampia serie di problematiche giuridiche e tecniche relative alla legittimità delle modalità di trattamento dei dati digitali e dall'attendibilità dei risultati stessi[54]. Gli operatori forensi hanno così iniziato a dedicare maggiore attenzione sia alle problematiche informatiche, sia a quelle procedimentali, al fine di evidenziare i profili di (il)legittimità e/o di (in)adeguatezza tecnica delle operazioni di ricerca, analisi, acquisizione e valutazione delle prove informatiche e, in senso più ampio, digitali.

Pertanto, l'Informatica forense si è sviluppata soprattutto a seguito dell'attività dei pratici forensi[55] che, sulla scia dell'esperienza tecnico-giuridica d'Oltreoceano, hanno sopperito alle ampie lacune normative, dottrinali e giurisprudenziali mediante tensioni e torsioni esegetiche delle norme esistenti[56].

La seconda fase si avvia idealmente nel 2001 con l'adesione dell'Italia alla Convenzione di Budapest sul Cybercrimine. Tale atto rappresenta un punto di svolta in quanto prevedeva a carico dei Paesi aderenti l'obbligo di dotarsi di un *corpus* normativo che comprendesse le principali figure di reato, gli strumenti processuali per il loro accertamento, gli organi e le procedure di coordinamento e cooperazione transnazionale tra organi investigativi statali per rendere più efficace l'attività di contrasto.

Nella sostanza, il provvedimento prevedeva che i paesi aderenti adottassero, tra le altre cose, gli strumenti tecnici, le procedure e le tutele per le parti coinvolte nei procedimenti con oggetto informatico che, in via esegetica, erano stati invocati dai pratici e dagli studiosi che, nel frattempo, avevano iniziato ad insegnare l'Informatica forense.

La fase di *vacatio legis* in pendenza di ratifica della Convenzione di Budapest evidenziava come l'embrionale disciplina introdotta dalla dibattuta L. 547/93 sui crimini informatici[57] fosse rimasta priva di correlati strumenti processuali[58]. Inoltre, lo strumentario concettuale e dommatico a disposizione degli studiosi e dei pratici confermava la sua inadeguatezza a qualificare

[54] Cfr. GAMMAROTA A., Danneggiamento di sistema informatico della P.A. e informatica forense: un caso, op.cit., *passim.*

[55] La prima esposizione pubblica delle problematiche dell'Informatica forense venne effettuata nel 2003 nel corso della conferenza dal titolo "Dalla Computer Forensics all'Informatica forense", svolta durante la prima edizione del Master in Diritto delle nuove tecnologie organizzato dal Centro Studi di Informatica Giuridica di Bari.

[56] Tale approccio costituisce la naturale evoluzione del metodo sviluppatosi presso lo Studio bolognese con Irnerio, Graziano ed i Glossatori, ed in qualche modo conferma il principio *ex facto ius oritur.*

[57] PICA G., Diritto penale delle tecnologie informatiche, op.cit., *passim.*

[58] Cfr. RUGGIERI F., Profili processuali nelle indagini sui reati informatici, in PASCUZZI, G. (a cura di), Diritto e informatica, Giuffrè, Milano, 2002, p. 147 e ss..

correttamente le nuove tecniche di indagine sui nuovi fenomeni criminali della società dell'informazione; infine, evidenziava la sostanziale arretratezza della ricerca accademica e la difficoltà a colmare la lacuna normativa, dottrinale e giurisprudenziale sul trattamento della prova informatica, anche negli altri settori dell'ordinamento giuridico.

Nonostante ciò, i principi tecnici e soprattutto le procedure per il corretto trattamento dei dati digitali evocate dalla Convenzione di Budapest, in quanto non ancora trasfusi nella normativa nazionale, venivano ignorati.

Pertanto, le impellenti necessità applicative continuavano ad essere tamponate dall'elaborazione teorica basata sugli schemi normativi del *corpus* giuridico esistente al fine di adattarli alle esigenze di inquadramento giuridico dei "fatti digitali", raggiungendo apprezzabili risultati attestati dalla giurisprudenza di merito.

Ad eccezione di qualche altra sporadica esperienza accademica, la maggior parte delle altre realtà di insegnamento conservava sulla materia una posizione evidentemente arretrata rispetto all'esigenza di ammodernamento concettuale ed esegetico compulsato dal progresso tecnologico.

Agli inizi del 2003, inoltre, per la prima volta in Italia, l'insegnamento dell'Informatica forense veniva formalizzato presso la facoltà di Giurisprudenza dell'Alma Mater di Bologna[59].

E proprio a motivo della profonda interdisciplinarietà tra diritto e informatica, l'insegnamento dell'Informatica forense si sviluppava tra le materie che trovano il loro alveo naturale nell'Informatica giuridica, quale luogo scientifico che negli anni precedenti aveva già sviluppato la ricerca e la didattica fondata sull'approccio interdisciplinare tra diritto e informatica. Sulla scia di tali precedenti esperienze, l'Informatica forense trovava a Bologna terreno fecondo per il suo sviluppo e insegnamento[60], caratterizzato dall'approccio interdisciplinare, informatico e giuridico, diventando così stabile punto di riferimento nazionale e internazionale per lo studio e la pratica di tale disciplina[61].

La terza fase va idealmente identificata con l'entrata in vigore della L. 18 marzo 2008 n. 48, (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)[62], con la quale l'Italia,

---

[59] MAIOLI C., (2002) Elementi di Informatica per l'Informatica Giuridica, Pioda, Roma, 2002 e dello stesso Autore, Dar voce alle prove: elementi di Informatica forense, op.cit., p. 66 e ss.

[60] La circostanza è indicata da Ziccardi in LUPARIA L., ZICCARDI G., Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali, Giuffrè, Milano, 2007 , p. 22 e ss..

[61] Cfr. GAMMAROTA A., MAIOLI C., A steganography based proposal for the detection of hidden data, Convegno Internazionale RIS su Indagini in Internet, Roma, 2005, in *http://www.carabinieri.it/Internet/Arma/Oggi/Convegni/Roma23052005/May+23/04_p.htm*.

[62] Pubblicata in Gazzetta Ufficiale n. 80 del 4 aprile 2008 – S.O. n. 79 ed entrata in vigore il giorno successivo; si considerino anche le successive modifiche introdotte dalla L. 24 luglio

simultaneamente a molti altri Paesi aderenti, ratificava la Convenzione di Budapest.

Con tale novella, il legislatore introduceva i principi di armonizzazione degli ordinamenti dei Paesi firmatari previsti dalla Convenzione di Budapest nel codice penale, nel codice di procedura penale, nel codice per la tutela dei dati personali, nonché in altri provvedimenti dell'ordinamento italiano.

Il legislatore, ritenendo che il diritto processuale penale non delineasse a sufficienza la disciplina delle investigazioni ad oggetto informatico, interpolava gli istituti preesistenti e in particolare quelli del Codice di procedura penale.

Durante tale fase ancora in corso, muovendo dall'individuazione delle problematiche tecniche e giuridiche più evidenti, le questioni di maggiore rilevanza hanno conosciuto migliore sistematizzazione, soprattutto per ciò che attiene agli strumenti e alle tecniche informatiche da adottarsi.

Sul piano giuridico, invece, venivano sviluppate nuove risposte esegetiche in chiave proattiva che innescavano un movimento di idee che negli anni immediatamente successivi maturavano nella giurisprudenza italiana quantomeno una presa di coscienza delle problematiche relative al rapporto tra diritto processuale e informatica[63].

In particolare, mediante l'analisi di *case study* sempre più frequenti e complessi, venivano sviluppati nuovi strumenti concettuali per l'analisi della prova digitale, delle tecniche investigative e di indagine, delle problematiche relative alle tecniche difensive e alla tutela dei dati personali che, all'esito, evidenziavano perduranti lacune sistematiche e giurisprudenziali.

Sul piano accademico, l'Informatica forense iniziava a prendere piede in varie Università[64].

Il processo in atto è irreversibile e condurrà alla prevalenza della rappresentazione digitale su tutte le altre forme di documentazione[65], con conseguenze rivoluzionarie anche in ambito processuale, connotate dalla necessità di garantire un elevato livello di certezza alle informazioni che verranno utilizzate per decidere la sorte di un imputato.

2008 n. 125, di conv. con modif. del D. L. 23 maggio 2008 n. 92 (in G.U. n. 122, 26 maggio 2008, S.G.) – Misure urgenti in materia di sicurezza pubblica (c.d. "Pacchetto sicurezza"), dal D.L. 7 aprile 2000, n. 82, convertito, con modificazioni, nella L. 5 giugno 2000, n. 144, dal D.L. 18 ottobre 2001, n. 374, convertito, con modificazioni, nella L. 15 dicembre 2001, n. 438.

[63] Cfr. Trib. Vigevano, sent. 17 novembre 2009, op.cit., *passim.*

[64] Cfr. LOSANO M. G, La computer forensics e l'insegnamento dell'informatica giuridica in NERHOT P., (a cura di), "L'identità plurale della filosofia del diritto, Atti del XXVI Congresso della Società Italiana di Filosofia del Diritto" (Torino, 16-18 settembre 2008), Napoli, ESI, 2009, pp. 115-123.

[65] "*...tutto il diritto sarà diritto informatico così come finora, in particolare a partire dalla diffusione della stampa, tutto il diritto è stato diritto scritto...Come la scrittura nel corso di cinquanta secoli è divenuta trama essenziale del tessuto sociale, e quindi oggetto del diritto oltre che sua precipua modalità espressiva, così l'informatica si avvia a diventare nei prossimi decenni la nuova trama essenziale di un tessuto sociale destinato a soppiantare quello sorretto dalla scrittura...*" così PATTARO E., Diritto, scrittura, informatica, in PATTARO E., (a cura di), Manuale di diritto dell'informatica e delle nuove tecnologie, Cedam, Padova, 2000, p. 30.

L'effetto della pandigitalizzazione delle azioni umane, sociali e produttive, e del conseguente incremento delle attività criminose si riverbererà anche nel processo, e in particolare quello penale, che sarà sempre più sarà basato solo su dati, documenti e tecniche digitalizzate, sino a quando la digitalizzazione diventerà nuova forma dello stesso processo[66].

A seguito di tali dinamiche, l'Informatica forense sta trovando ambiti applicativi sempre più numerosi e impensabili sino qualche anno fa: dalla tutela delle opere dell'ingegno a quella delle invenzioni, dall'e-care, e in particolare dai sistemi digitali HIS[67], RIS-PACS[68], LIS[69] sino alla telemedicina, dalla bioingegneria alla bioinformatica e alla bioetica, dall'ingegneria civile alla telematica finanziaria. Non esistono settori della vita sociale investiti dalla rivoluzione digitale che restino estranei ad accertamenti giudiziari sulla base di informazioni tratte da dati digitali.

Infine, non può sottacersi che, come spesso è accaduto nella storia del progresso delle idee, l'Informatica forense ha trovato impulso grazie all'attività di diverse associazioni di cultori, specialisti e pratici della disciplina, i cui risultati hanno agevolato la diffusione, la condivisione della conoscenza e il progresso della materia[70] prima ancora che dell'iniziativa accademica avviata solo successivamente e con ritmi incompatibili con il progresso tecnologico, e che solo da ultimo vede la materia inserita in corsi stabili o in percorsi di perfezionamento.

---

[66] Sul punto, v. MOFFA S., Verso il processo penale telematico, in MAIOLI C., (a cura di), Questioni di Informatica forense, Aracne, Ariccia, 2015, p. 155 e ss..

[67] I sistemi informativi ospedalieri (*HIS, Hospital Information System*) integrano gli strumenti informatici utilizzati in ambito sanitario per gestire i flussi amministrativi e clinici di un ospedale; per l'Informatica forense applicata ai dati digitali sanitari, v. GAMMAROTA A., CACCAVELLA D. E., "L'Informatica forense per l'E-Healt", in FARALLI C., BRIGHI R., MARTONI M., (a cura di), Strumenti, diritti, regole e nuove relazioni di cura, Giappichelli, Torino, 2015, p. 205 e ss..

[68] Il sistema informatico radiologico *RIS (Radiology Information System)* integra gli strumenti hardware e software dedicati all'acquisizione delle immagini diagnostiche digitali, ed è strettamente collegato al Sistema di archiviazione e trasmissione di immagini (*PACS, Picture Archiving and Communication System*) che integra gli strumenti hardware e software dedicati all'archiviazione, trasmissione, visualizzazione e stampa delle immagini diagnostiche digitali.

[69] Il sistema informativo di laboratorio (*LIS, Laboratory Information System)* integra gli strumenti hardware e software dedicati alla gestione del laboratorio di analisi.

[70] A tal proposito va segnalata l'attività svolta da varie associazioni, tra le quali il Centro Studi di Informatica Giuridica (CSIG), nella sua articolazione locale degli Osservatori CSIG, cui va riconosciuto un ruolo pionieristico sulla promozione Informatica forense; l'International Information Systems Forensics Association (IISFA) Italian Chapter, che negli ultimi anni ha contribuito alla diffusione della conoscenza dell'Informatica forense nelle sue varie articolazioni; l'Osservatorio Nazionale per l'Informatica Forense (ONIF), che ha come fine la promozione a livello nazionale della figura e del ruolo professionale dell'informatico forense (*http://www.onif.it/*).

2.3 L'autonomia scientifica dell'Informatica forense

Non vi è dubbio che l'Informatica forense abbia assunto una propria maturità e completezza tale da poterle riconoscersi autonomia scientifica nel più ampio ambito dell'Informatica giuridica[71].

Il riconoscimento teorico e pratico deriva non solo dallo studio e pratica che a livello internazionale è dedicato alla Computer (Digital) forensics, ma per quanto riguarda l'Europa e l'Italia, rileva anche la formazione di un ampio *corpus* normativo omogeneo che, per quanto connesso al diritto penale processuale da un lato e all'informatica dall'altro, ne travalica i limiti essendo i suoi principi caratterizzati da peculiarità di oggetto, finalità e metodo che la differenziano dalle sue componenti e la rendono indispensabile e trasversale a tutte le altre branche dell'ordinamento giuridico.

A ciò si aggiunga la formalizzazione del suo insegnamento in corsi di studi universitari stabilmente strutturati e ampiamente diffusi in tutto il mondo, che trovano riscontro a livello europeo e, da alcuni anni, anche in Italia.

Sono quindi circoscritti lo scopo e l'oggetto di studio sulla base sia di una propria metodologia interdisciplinare basata su quella delle scienze afferenti, sia di un corpus normativo ampio e articolato, sia di un vasto riconoscimento dottrinale che si traduce in una letteratura ampia e con posizioni articolate, e spesso divergenti, oltre ad una vasta letteratura tecnica.

Pertanto, all'Informatica forense non può negarsi autonomia scientifica al pari delle altre scienze forensi di più antica tradizione quali ad esempio la medicina legale, la chimica forense e la balistica forense.

2.4 I rapporti tra l'Informatica forense e le altre discipline

Poiché in Italia le prime esperienze teoriche e applicative dei principi e delle tecniche della Computer forensics si sono sviluppate in ambito penalistico, l'Informatica forense appare naturalmente inquadrabile tra le scienze ausiliare all'applicazione del diritto penale e processuale penale, secondo la tradizione classificatoria dei più autorevoli Autori di tali discipline[72].

---

[71] Per tale collocazione sistemica in ambito accademico, v. MAIOLI C., ORTOLANI C., La cyber law non è la horse law. L'informatica giuridica nelle Facoltà di Giurisprudenza, Gedit, Bologna, 2007, pp. 185-186.

[72] Cfr. ANTOLISEI F., Manuale di diritto penale, op.cit., p. 26, dove è delineata la sistematica delle scienze ausiliarie al diritto penale, ovvero le scienze criminalistiche (antropologia criminale, psicologia criminale, sociologia criminale la medicina legale (medicina legale, psichiatria forense, psicopatologia forense, tossicologia forense, psicologia giudiziaria), sia tra quelle di polizia scientifica. In tale sistematica, l'Informatica forense sarebbe collocabile tra le scienze criminalistiche e tra quelle di polizia scientifica; nell'ambito di analoga sistematica, cfr. MANTOVANI F., Diritto Penale, op.cit., tra le c.d. scienze criminali (diritto penale, criminologia, filosofia e storia del diritto penale, diritto penale processuale, politica criminale), si classifica la tecnica dell'investigazione criminale e nell'ambito di questa si annoverano altre scienze quali medicina legale, dattiloscopia, antropometria, balistica giudiziaria, grafometria,

Tuttavia, sin dalle prime esperienze teoriche, si è posta la questione di delimitare l'area di studio e l'operatività dell'Informatica forense rispetto alle altre discipline dell'area informatico-giuridica.

Durante la prima presentazione delle questioni terminologiche[73], ebbi modo di differenziare il campo di azione dell'Informatica forense da quello delle altre discipline aventi ad oggetto lo studio del rapporto tra diritto e informatica.

A mio parere, l'Informatica forense si distingueva dalla Giuscibernetica, avente ad oggetto l'impiego dell'elaboratore nel campo del diritto[74], dall'Informatica giuridica, quale disciplina che si occupa della trattazione delle attività informatiche tecnico-pratiche applicate al diritto[75], dal Diritto dell'informatica, quale complesso delle norme legislative, delle decisioni giurisprudenziali e della letteratura giuridica in materia di informatica[76], dall'Informatica documentaria, quale scienza della memorizzazione dei fatti giuridici, dall'Informatica decisionale o modellistica giuridica o metadocumentaria o intelligenza artificiale nel diritto, intesa quale disciplina che si occupa dell'algoritmizzazione di procedure giurisdizionali al fine di automatizzare le attività degli operatori del diritto per riprodurre le attività proprie dell'operatore quali pareri, consulenze, decisioni[77], e infine dalI'Informatica giudiziaria, che si occupa dell'uso dell'informatica a supporto dell'organizzazione delle attività svolte negli uffici giudiziari e negli studi legali e notarili.

La trasversalità delle problematiche studiate all'Informatica forense rispetto a molti altri ambiti diversi dal diritto penale e processuale penale, è resa attuale dalla pervasività dei cambiamenti tecnologici e sociali e dalle recenti riforme legislative verificatesi in vari settori del diritto processuale.

Si pensi alle implicazioni delle molte riforme che in questi ultimi anni stanno rivoluzionando vari settori della pubblica Amministrazione, centrale e locale.

In ambito tributario, il riconoscimento della centralità dell'informatica quale strumento di svolgimento delle procedure contabili e di assolvimento

tossicologia forense, psicologia giudiziaria, psichiatria forense, al fianco delle quali può essere classificata anche l'Informatica forense.

[73] La prima esposizione pubblica delle problematiche dell'Informatica forense venne effettuata nel 2003 nel corso della conferenza dal titolo "Dalla Computer Forensics all'Informatica forense" nell'ambito della prima edizione del "Master in Diritto delle nuove tecnologie" organizzato dal Centro Studi di Informatica Giuridica di Bari.

[74] Sull'evoluzione della giurimetria in giuscibernetica, cfr. LOSANO M., Informatica per le scienze sociali, Torino, 1985, pp. 45-53.

[75] Cfr. FROSINI V., Informatica diritto e società, Giuffrè, Milano, 1992, p. 229 e ss.

[76] Sul contenuto del diritto dell'informatica, cfr. GIANNANTONIO E., Manuale di diritto dell'informatica, op.cit., p. 1.

[77] Cfr. BARBARISI M., Diritto e informatica, op.cit. e da ultimo, SARTOR, G., L'informatica giuridica e le tecnologie dell'informazione, op.cit., p. 11 e ss.

degli obblighi fiscali, comporta un'ampia ricaduta del fenomeno nell'ambito del processo tributario anch'esso riformato.

In ambito amministrativo, i processi di dematerializzazione della documentazione e gli istituti del Codice dell'Amministrazione Digitale (CAD), sposteranno il baricentro dell'attività istruttoria del processo amministrativo nella direzione imposta dalla dematerializzazione dei mezzi di prova, fenomeno peraltro che i nuovi strumenti istruttori previsti dal nuovo processo amministrativo potranno solo in parte assecondare.

In ambito civile, i nuovi strumenti, forme e ambiti di esercizio dei diritti, quali ad esempio gli strumenti di firma digitale, i contratti dematerializzati e gli scambi nell'ambito di mercati sempre più globalizzati e anch'essi dematerializzati, pongono esigenze di tipo processuale che nessuna riforma ha sino ad oggi ha affrontato in modo ampio ed esaustivo[78].

Per questo motivo, le riflessioni e le tecniche maturate nell'ambito dell'Informatica forense si prestano, previo opportuni adattamenti, ad essere mutuati in altri settori della scienza giuridica stante proprio il carattere trasversale dei presupposti comune a qualsiasi ambito nel quale si renda necessario trattare dati digitalizzati a fini processuali.

2.5 Gli utilizzatori dell'Informatica forense

Gli aspetti teorici e operativi dell'Informatica forense trovano applicazione in molteplici settori pubblici e privati.

Le procedure e le tecniche di indagine informatica costituiscono la base dell'attività della polizia giudiziaria sia nella fase delle investigazioni ad iniziativa che, successivamente all'assunzione della loro direzione da parte del pubblico ministero durante le indagini[79]. In particolare, l'Informatica forense

[78] L'estensibilità dell'approccio scientifico alle prove proprio dell'Informatica forense ad altre tipologie di processi, quali quello civile, amministrativo, tributario, è stata evidenziata sin dal 2005 da VILLECCO BETTELLI A., Appunti sul nuovo processo tecnologico, in CEVENINI C., DI COCCO C., SARTOR G., Lezioni di informatica giuridica, Gedit, Bologna, 2005, p. 264; da ultimo, v. NOVARIO F., Le prove informatiche nel processo civile, op.cit.

[79] In tale prospettiva, si veda l'ampia opera di ATERNO S., CAJANI F., COSTABILE G., MATTIUCCI M., MAZZARACO G., (a cura di), Computer forensics e indagini digitali, Experta, 2011; v. anche SOI, G., Tracce informatiche, in Polizia Moderna, novembre 2010, p. 30; ESPOSITO G., Un PC per Sherlock Holmes, 2012, in *http://www.carabinieri.it/editoria/il-carabiniere/anno-2012/febbraio/scienza/un-pc-per-sherlock-holmes*; CURTOTTI NAPPI D., SARAVO L., Le indagini sulla scena del crimine. Discrasia legislativa, 2011, in *http://www.carabinieri.it/editoria/rassegna-dell-arma/anno-2011/n-2---aprile-giugno/studi/le-indagini-sulla-scena-del-crimine-discrasia-legislativa-*; SPECCHIO G., Attività Investigativa in Internet, in *http://www.carabinieri.it/editoria/rassegna-dell-arma/anno-2012/n-1---gennaio-marzo/studi/attivit%C3%A0-investigativa-in-internet*; DONATO F., Indagini e acquisizione di dati probatori sulla scena del crimine. Protocolli operativi e utilizzabilità della prova: aspetti criminalistici , in Archivio penale, n. 2, 2012; BOVIO, L., Prova informatica e processo penale, inserto in Polizia Moderna, marzo 2015;

costituisce il nucleo delle attività svolte dai diversi corpi di polizia giudiziaria[80], e in particolare dai reparti specializzati in indagini per reati informatici o con implicazioni informatiche[81].

L'attività di polizia giudiziaria trova poi naturale esito, come si è detto, nell'attività di indagine svolta sotto la direzione del pubblico ministero o, nel caso di diverso procedimento, dall'organo che conduce la fase inquirente.

Quindi, l'Informatica forense trova applicazione privilegiata nell'ambito giudiziario, inquirente e giudicante penale ordinario, contabile, militare, ma anche nell'ambito giudiziario civile ordinario, amministrativo e tributario.

Tuttavia, vi è un'ampia serie di addetti e operatori che, svolgendo attività di rilevante importanza per quanto ausiliaria all'amministrazione della giustizia, sono coinvolti nella gestione dei dati a fini processuali e quindi tenuti ad adottare le tecniche dell'Informatica forense.

Tra questi, vanno annoverati gli addetti alle Segreterie degli Uffici del Pubblico Ministero e alle Cancellerie degli uffici delle magistrature giudicanti, di tutti i gradi di giudizio (Giudice di Pace, Tribunale, Monocratico e Collegiale, Corte di Assise, Corte di Appello, Corte di Assise di Appello, Cassazione). Sono gli addetti consegnatari e custodi dei fascicoli e dei corpi di reato sempre più spesso comprendenti supporti con dati digitali acquisiti ai fini del procedimento. In tali attività rilevano soprattutto le norme giuridiche e tecniche riguardanti la correttezza della gestione dei supporti contenenti i dati e del trattamento degli stessi.

Le stesse considerazioni valgono anche per gli Ufficiali giudiziari che, nel corso della loro attività, possono essere chiamati a svolgere funzioni per le quali sono tenuti a custodire o comunque svolgere funzioni di consegnatari di supporti e dispositivi digitali contenenti dati.

Un'altra particolare figura di ausiliario è quella del custode giudiziario, al quale può essere affidata la custodia di dispositivi digitali, supporti, sistemi informatici e telematici e quant'altro possa contenere dati rilevanti per il procedimento. A seguito della loro nomina, anche tali operatori vengono gravati

[80] Le funzioni di polizia giudiziaria possono essere svolte dagli appartenenti alle polizie statali, quali l'Arma dei Carabinieri, la Polizia di Stato, la Guardia di Finanza, il Corpo forestale dello Stato, la Guardia forestale, la Polizia penitenziaria, il Corpo nazionale dei vigili del fuoco, il Corpo delle capitanerie di porto - Guardia costiera, dalle numerose polizie locali, quali i Corpi di polizia municipale e provinciale, ma anche da altre figure a disciplina intermedia come ad es. le Guardie zoofile. Data la pervasività della tecnologia informatica in tutti i settori oggetto dell'attività di tali Corpi, almeno le istituzioni dell'Informatica forense dovrebbero far parte integrante del bagaglio formativo e professionalizzante dei loro appartenenti.

[81] Tra i reparti specializzati in indagini informatiche o che si avvalgono di particolari strumenti informatici si ricordano il RAggruppamento Carabinieri Investigazioni Scientifiche (RaCIS), articolato a livello territoriale nei Reparti di Investigazione Scientifica (RIS), in *http://www.carabinieri.it/arma/oggi/indagini-scientifiche/indagini-scientifiche*, nonchè i Raggruppamenti Operativi Speciali (ROS) dell'Arma dei Carabinieri, in *http://www.carabinieri.it/arma/oggi/reparti/organizzazione-mobile-e-speciale/ros*; il Servizio di Polizia Postale e delle Comunicazioni della Polizia di Stato; il Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza.

di rilevanti obblighi giuridici relativi alla correttezza della custodia e trattamento dei dispositivi digitali, supporti, sistemi informatici e telematici e quant'altro possa contenere dati rilevanti per il procedimento e temporaneamente affidati alla loro custodia.

Vi è poi una categoria di ausiliari che assume una particolare rilevanza e attinenza con gli ambiti oggetto di rilevanza dell'Informatica forense, e che comprende le figure del consulente tecnico[82] del pubblico ministero e delle altre parti del procedimento, e del perito nominato dal giudice. Tali figure svolgono funzioni di importante rilievo nell'ambito del procedimento in quanto costituiscono lo strumento conoscitivo in ambito tecnico-scientifico dei protagonisti del procedimento che consentono a questi ultimi di poter svolgere con miglior consapevolezza la propria funzione sugli aspetti tecnico-scientifici in materia informatica oggetto di cognizione. È evidente che soprattutto a tali figure è richiesta un'ampia e profonda conoscenza di tutti gli aspetti giuridici e tecnici che costituiscono oggetto di studio dell'Informatica forense[83].

È evidente che l'ignoranza della normativa riguardante gli obblighi e le responsabilità derivanti dal (mal)trattamento dei dati digitali, nonché l'omessa adozione delle tecniche tecniche previste a tal fine, sono motivo di responsabilità degli ausiliari responsabili ma soprattutto possono arrecare gravi pregiudizi all'efficacia dell'attività processuale.

---

[82] Sulla consulenza tecnica e sull'attività del consulente nel processo penale, v. MENDOZA R., MARCON G., MARCON L., La perizia e la consulenza nel processo penale, Padova, Cedam, 1994; FOCARDI F., La consulenza tecnica extraperitale delle parti private, Cedam, Padova, 2003; BRESCIA G., Il consulente tecnico e la perizia nel processo civile e penale, IV ed., Maggioli, Rimini, 2006; ATERNO S., MAZZOTTA P., La perizia e la consulenza tecnica. Cedam, Padova, 2006, e in particolare, CACCAVELLA D., E., Gli accertamenti tecnici in ambito informatico, ivi, p. 195.

[83] In Italia, il problema della professionalizzazione dei consulenti tecnici e dei periti di Informatica forense sconta la generale arretratezza della teoria e pratica di quest'ultima disciplina e di un sistema selettivo che non premia la specializzazione. Mentre negli USA l'iter formativo, selettivo e professionalizzante dei Digital forenser è 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, elenchi o sezioni dedicati alla specifica figura dell'esperto di Informatica forense. Ne deriva che chiunque può svolgere l'attività di consulente tecnico in materia di informatica forense su incarico di una parte privata (e talvolta anche pubblica) anche se non ha seguito un percorso accademico nel quale abbia acquisito una formazione sia giuridica che informatica. Pertanto, è dato assistere ancora a casi di improvvisazione da parte di chi non sia in possesso di specifiche competenze. Infatti, chiunque sia in possesso di laurea in Ingegneria (e di qualunque tipo), Informatica, Scienza dell'informazione, ma anche in Economia e Commercio o in Agraria, può chiedere l'iscrizione agli albi dei Tribunali, civili e penali, ed essere incaricato Consulente tecnico del PM o Perito per il compimento di attività di Informatica forense. Non è quindi irrazionale assistere alla nomina da parte di un Giudice di Pace, di un Dottore Commercialista come Consulente Tecnico d'Ufficio (CTU) in una causa dove si controverteva in tema di inadempimento del contratto di fornitura di un software per la gestione dello studio di consulente tributario e della nomina di un Dottore Agronomo come CTU in un'altra causa nella quale si controverteva sui vizi del software di gestione di un'azienda agricola. La conclusione è che proprio l'esperto che dovrebbe essere di ausilio alle parti in attività dai risvolti processuali estremaente delicati, può essere motivo di rilevante pregiudizio per la qualità degli accertamenti.

Sempre per rimanere in ambito forense, l'Informatica forense occupa ormai un posto di grande rilievo nel patrimonio professionale e culturale sia dell'avvocato che dei suoi collaboratori e ausiliari chiamati a svolgere le funzioni a supporto dell'attività professionale (segretari, consulenti, investigatori privati).

In particolare, l'Informatica forense consente all'avvocato un approccio molto più attento alle problematiche relative alla corretta ricostruzione delle fattispecie oggetto del procedimento e a tutte le problematiche relative all'uso probatorio dei dati digitali. Semplificando, si può senz'altro affermare che se l'attività professionale dell'avvocato consisteva tradizionalmente nella qualificazione giuridica e applicazione di norme ad una realtà fatta di atomi, nelle ultime decadi l'attività professionale ha ad oggetto una realtà dematerializzata e fatta di bit. Per quanto poi attiene alla particolare attività processuale, di qualunque natura essa sia, e in particolare dell'attività di quella finalizzata all'applicazione della legge penale oggetto della presente disamina, la tradizionale attività di difesa si confronta continuamente con procedure aventi ad oggetto il trattamento di dispositivi e dati digitali tratti da dispositivi informatici e telematici dai quali vengono assunte le informazioni oggetto del procedimento. Inoltre, tali informazioni vanno correlate con le altre informazioni derivate dalle attività investigative e di indagine svolte secondo gli schemi tradizionali. Tutto ciò comporta che gli avvocati sono, al pari della polizia giudiziaria e dei magistrati, i destinatari naturali dei contenuti dell'Informatica forense[84].

Va infine rilevato che, se la disciplina processual penale ha trovato nella L. 48/08 alcuni principi innovatori, per quanto incompleti, incoerenti ancora poco attuati, tutti gli altri sistemi processuali, sottosistemi e riti speciali che affollano il nostro ordinamento giuridico[85], per quanto presentino analoghe problematiche a quelle già rassegnate, sono rimasti ancora privi di una disciplina delle tecniche e procedure di trattamento della prova informatica.

---

[84] Anche a tal proposto non si può evitare di notare come né l'attuale percorso di studi obbligatorio per coloro i quali intendano svolgere la libera professione forense, al pari delle altre due classiche attività professionali forensi (magistratura e notariato), né gli esami abilitanti all'esercizio della professione, né i percorsi professionalizzanti e di formazione continua obbligatoria, prevedano la conoscenza della normativa e delle regole tecniche per la corretta gestione dei dispositivi, dei sistemi informatici e telematici e dei dati digitali oggetto di attività procedimentale. Ad eccezione delle iniziative già citate, nella maggior parte dei casi, l'approccio all'Informatica forense resta ancora relegato ad iniziative ristrette ed estemporanee.

[85] Nell'ordinamento giuridico italiano si rinviene un'ampia tipologia di processi: si va dal processo civile, nel cui ambito si rinvengono almeno quindici diversi sottosistemi, al processo penale, nel quale il regime probatorio è caratterizzato da un regime ordinario e da diversi regimi speciali dipendenti da vari schemi di giudizi alternativi, al procedimento arbitrale, al processo amministrativo, al contabile, al tributario, al penale militare di pace e di guerra, ma anche ai sistemi disciplinari e ai sistemi processi extraordinamentali come, ad esempio, il processo sportivo.

Tale carenza diventa tanto più ampia ed evidente, quanto più aumenta la necessità di analisi di dati digitali a fini processuali nell'ambito dei più svariati tipi di processo[86].

Pertanto, lo spettro di studio dell'Informatica forense non è limitato all'ambito processuale penale, e come le acquisizioni teoriche e pratiche delle altre scienze forensi hanno rilevanza anche negli altri processi di diverso tipo, anche quelle dell'informatica forense possono trovare adeguata declinazione in molteplici ambiti, ovviamente adattandole ai diversi contesti.

Inoltre, in Italia, come altrove, l'Informatica Forense trova applicazione anche in molti settori privati.

In ambito aziendale, l'Informatica forense costituisce un efficace strumento da affiancare alle altre tecniche di risk & data *management*[87], in quanto consente di implementare forme organizzative e strumenti operativi a supporto di politiche di prevenzione e gestione dei casi che possono trovare esito processuale, come ad es. nei casi di fatti costituenti reato commessi da dipendenti e amministratori ai danni della stessa azienda o di terzi[88]. Inoltre, l'Informatica forense, sviluppatasi nell'ambito della migliore gestione degli elementi di prova a contenuto digitale, fornisce i paradigmi e gli strumenti per la migliore prevenzione e gestione dell'eventuale contenzioso insorgente tra azienda e concorrenti, dipendenti, fornitori e clienti, la cui soluzione dipenda da elementi di prova digitale[89]. L'adozione delle misure di Informatica forense risulta più rilevante ed efficace nei settori ad alto il livello di dematerializzazione mediante digitalizzazione dei processi produttivi: dall'ambito bancario, finanziario e assicurativo, a quello dei media e design, alle società di servizi e consulenza.

Ad analoghe considerazioni non si sottrae l'ampio settore delle libere professioni, i cui protagonisti, avvocati, commercialisti, ingegneri, architetti e da ultimo, sempre più, i medici, usualmente utilizzano sistemi informatici e telematici che creano dati digitali per lo svolgimento della propria attività professionale[90].

---

[86] Cfr. VILLECCO BETTELLI A., L'efficacia delle prove informatiche, Giuffrè, Milano, 2004.

[87] Cfr. AA.VV, Inside attack. Tecniche di intervento e strategie di prevenzione.Manuale di ricerca e di intervento sul computer crime nelle organizzazioni. Nuovo studio tecna, Roma, 2005; per l'implementazione dell'Informatica forense nei processi di *risk management* in ambito sanitario (pubblico e privato), v. CACCAVELLA D. E., FERRAZZANO M., BONORRI F., L'implementazione dei processi organizzativi finalizzati alla gestione del rischio nell'ambito di strutture sanitarie, in FARALLI C., BRIGHI R., MARTONI M., (a cura di), Strumenti, diritti, regole e nuove relazioni di cura, Giappichelli, Torino, 2015, p. 221 e ss..

[88] Va sin d'ora rilevato che le aziende vengano spesso condotte dai soggetti rientranti tra quelli indicati dall'art. 1 del Decreto legislativo, 08/06/2001 n° 231 (in G.U. 19/06/2001) (enti forniti di personalità giuridica, società e associazioni anche prive di personalità giuridica) sui quali grava la responsabilità per gli illeciti amministrativi dipendenti da reato.

[89] LUPARIA L., ZICCARDI G., op.cit. pp., 89 e ss.

[90] Sull'applicabilità dell'Informatica forense ai processi sanitari digitalizzati, v. GAMMAROTA A., CACCAVELLA D. E., op.cit., p. 205 e ss.

Tale impostazione conferma da un lato la natura strettamente interdisciplinare dell'Informatica forense, la cui pratica diventa strutturale rispetto a quella del diritto e dell'ICT ovunque quest'ultima presenti attitudine ad esitare in scenari processuali.

2.6 Le prospettive di convergenza tra Informatica forense e Informatica giudiziaria penale

Come si è visto, la digitalizzazione delle varie forme di processo è un processo ormai irreversibile.

A seguito dell'esperienza del Processo Civile Telematico[91], non scevra da ombre, da poco ha visto l'avvio anche il Processo Amministrativo Telematico, ma ci si attende la progressiva estensione dell'esperienza anche agli altri tipi di processo operanti nel nostro ordinamento.

In particolare, l'attenzione è suscitata dalla progressiva informatizzazione delle procedure del processo penale.

In tale ambito, il Processo Penale Telematico, oggetto di studio dell'Informatica giudiziaria penale[92], è ancora in fase embrionale, essendo l'informatizzazione limitata alla gestione di spezzoni di procedure e di operazioni elementari[93].

Tuttavia, per quanto allo stato non sia prefigurabile sino a dove potrà giungere tale evoluzione, è sicuro che all'esito della progressiva sostituzione delle attuali forme di gestione del processo penale, il processo penale sarà molto diverso da quello attualmente conosciuto.

Non è peregrino prefigurare che, prima di quanto si pensi, il legislatore possa introdurre nel sistema una sorta di Rito o Giudizio Telematico, caratterizzato dal solo fatto di essere celebrato a distanza e in forma telematica. Un meta-rito alternativo alla celebrazione del processo con le parti tutte fisicamente presenti, e quindi cumulabile anche con gli altri riti alternativi, facoltativo, incentivato con le forme di premialità già note al nostro sistema processuale o anche diverse. Tale opzione potrebbe essere prevista soprattutto per determinate categorie di processi, ad esempio per quelli relativi ad

[91] Sull'informatizzazione della gestione delle procedure giudiziarie in ambito civile e penale, v. BUFFA F., Il processo civile telematico. La giustizia informatizzata, Giuffrè, Milano, 2002; ZAN S., (a cura di), Tecnologia, Organizzazione e Giustizia. L'evoluzione del Processo Civile Telematico. Il Mulino, Bologna, 2004; ASARO C., Ingegneria della conoscenza giuridica applicata al diritto penale, Aracne, Ariccia, 2012; DE RUGGERIIS, Effetti delle innovazioni tecnologiche sul processo penale, in MAIOLI C., (a cura di), Questioni di Informatica forense, Aracne, Ariccia, 2015, p. 89 e ss.

[92] In ambito internazionale, l'informatizzazione delle procedure di giustizia è nota come E-Justice, sulle cui problematiche, v. FALLETTI E., E-Justice. Esperienze di diritto comparato, Giuffrè, Milano, 2008; CARNEVALI D., CONTINI F., FABRI M., (a cura di) Tecnologie per la Giustizia. Isuccessi e le false promesse dell'E-Justice, Giuffrè, Milano, 2006.

[93] Sulle alcune esperienze di informatizzazione di procedure di gestione di dati in ambito giudiziario penale, v. MOFFA S., op.cit.

imputazioni per reati meno gravi, o per i processi a più elevata complessità dipendente dalla presumibile durata, dal numero delle parti coinvolte, dai costi di gestione per l'organizzazione, svolgimento, logistica e trasferimento di persone.

Tali prospettive, più realistiche di quanto si pensi in un contesto di bilancio soggetto a continui tagli e ridimensionamenti di spesa, non vanno demonizzate aprioristicamente, ma vanno pensate e governate con strumenti che riconoscano e attuino i principi e i diritti di difesa secondo logiche che non cedano nulla alla rivoluzione digitale ma, anzi, vengano da questa "aumentati".

Il presupposto indefettibile è costituito dalla reingegnerizzare del diritto processuale penale, Affinché la digitalizzazione delle procedure e delle forme del processo siano soggette ai principi e alle garanzie fondamentali a presidio del diritto di difesa, all'interno della cornice costituzionale del Giusto Processo Telematico.

Non da meno, sarà imprescindibile realizzare l'innovazione al di fuori di un'infrastruttura informatica e telematica all'altezza della delicatezza della funzione, e quindi dedicata, stabile e sicura, al cui uso sarà fondamentale formare tutti gli operatori forensi.

In tale prospettiva, l'Informatica giuridica penale e in particolare l'Informatica giudiziaria penale dovranno tener conto delle tecniche messe a punto dall'Informatica forense nel campo delle modalità di trattamento e gestione dei dati processualmente rilevanti.

3 La questione dei postulati tecnici dell'Informatica forense

3.1 La definizione ontologica e giuridica dei dati informatici

Se gli attori del processo intendono trarre dai dispositivi digitali e dai sistemi informatici e telematici dati digitali che abbiano alta capacità rappresentativa dalla quale desumere informazioni utili ai fini del procedimento, allora l'idoneità dei dati informatici a costituire elemento di prova e le relative tecniche di trattamento deve sottostare al vaglio della metodologia e delle tecniche scientifiche studiate dall'Informatica forense.

Ma la ricostruzione degli aspetti giuridici caratterizzanti l'attività processuale ad oggetto informatico non può prescindere dalla preliminare definizione dei concetti fondamentali di informatica che costituiscono il presupposto indefettibile per una corretta impostazione su base scientifica delle questioni esegetiche che si intende affrontare nel prosieguo della trattazione.

3.2 Dato, informazione, bit

Nella normativa di settore, europea e italiana, si incontrano spesso i termini di dato, informazione, documento informatico, ma raramente quello di bit. Si tratta di termini utilizzati nella dalla giurisprudenza investita del suo momento applicativo delle norme, nonché dagli autori che in sede dottrinale hanno trattato la materia.

In verità, tali termini vengono usati in modo non univoco e spesso come sinonimi, causando confusione nei casi meno gravi e antinomie in alcuni casi eclatanti.

L'origine dell'uso disinvolto di tali termini va senza dubbio individuata nella legislativa nazionale che, da come li accosta o li utilizza nell'ambito delle novelle di settore, rivela di ignorarne le profonde differenze ontologiche tra i termini, al punto di provocare una eterogenesi di fini rispetto alla *ratio legis*.

Per tale motivo, prima di inoltrarci nella disamina giuridica, si rende imprescindibile il tentativo di differenziare la portata dei termini compresi nel glossario tecnico pregiuridico.

La prima questione da affrontare riguarda un postulato dell'informatica forense, attinente alla individuazione dell'oggetto ultimo dello studio e delle tecniche di Informatica forense, ovvero il dato.

Per "dato" si intende la rappresentazione originaria, non interpretata di un fatto, fenomeno o evento, effettuata attraverso simboli (numeri, lettere, segni).

Un dato può essere analogico, cioè rappresentato da simboli distinti e continui o variabili con continuità (ad esempio la temperatura di un corpo rilevata da un termometro a mercurio), oppure digitale, cioè rappresentato secondo un codice di simboli o segnali ben definiti e discontinui che non mutano con continuità e che può essere letto da un elaboratore.

Dal dato va a sua volta tenuta distinta l'informazione: mentre il primo è una "*rappresentazione originaria, cioè non interpretata, di un fenomeno, evento o fatto, effettuate attraverso simboli o combinazioni di simboli (numeri, lettere, segni) o di qualsiasi altra forma espressiva (vocale, visuale ecc.) legate a un qualsiasi supporto (carta, dischi magnetici o ottici, pellicola fotografica ecc.)".*[94] In quanto tale, il dato non costituisce di per sé l'informazione, la quale, per essere desunta, necessita di un ulteriore attività che si rapporti al dato.

L'**informazione**, invece, **"***...deriva da un dato, o più verosimilmente da un insieme di dati, che sono stati sottoposti ad un processo di interpretazione, derivante dalla conoscenza orientata in una materia, che li ha resi significativi per il destinatario, e realmente importanti agli scopi prefissi."*[95]

Tali definizioni consentono di individuare una serie di differenze tra il dato e l'informazione[96]:

- il dato è l'input di un sistema informatico, l'informazione è l'output del dato;
- il dato è fatti e cifre non processati, l'informazione è un dato processato;
- il dato non dipende dall'informazione, l'informazione dipende dal dato;
- il dato non è specifico, l'informazione è specifica;
- il dato è una singola unità, informazione è chiamata un gruppo di dati che porta notizie e significato;
- il dato non porta significato, l'informazione deve portare un significato logico;
- il dato è il materiale grezzo, l'informazione è il suo prodotto.

Orbene, la definizione di dato contiene tre elementi importanti:

1. il dato è una rappresentazione non interpretata, e quindi oggettiva, di fenomeni, eventi o fatti;
2. viene realizzato tramite simboli o combinazioni di simboli di altra forma di espressione sensorialmente apprezzabile;

[94] BONI M., Informatica, Apogeo, 2005, p. 7.
[95] BONI M., *ibidem.*
[96] *http://www.differencebetween.info/difference-between-data-and-information*.

3. il dato è talvolta legato ad un supporto che può essere di diversi materiali, purché utile a fissare i dati e trasmetterli al destinatario.

Pertanto, la peculiarità del rapporto tra dato e supporto sta nel fatto che il dato può essere contenuto su un supporto adeguato e deve essere composto da simboli comprensibili al destinatario.[97]

L'utilità di tale costruzione del dato, allorquando sia legato ad un supporto che lo contiene, deriva dalla possibilità di leggerlo dal supporto grazie ad un dispositivo che sappia elaborarlo.

L'informazione, invece, è caratterizzata dal fatto che la sua utilità si rivela solo a chi si occupa della materia specifica e sa interpretare i simboli costituenti i dati.

Pertanto, le informazioni, proprio perché sono il risultato di un processo interpretativo che presuppongono un'attività intellettiva, prescindono dal supporto e invece dipendono:

- dal destinatario o a colui il quale svolge l'attività interpretativa, tant'è che la stessa sequenza di dati può essere interpretata da persone differenti in modi differenti;
- dal contesto e dal tempo in cui viene creata;
- dal luogo di creazione o di destinazione;
- dalla fonte di emissione dei dati originari.

Quindi, l'informazione è strettamente legata al contesto nel quale viene creata, utilizzata e fruita.

Il processo interpretativo dei dati, soprattutto quelli legati ai simboli, viene facilitato seguendo vari livelli di regole che danno origine ad un linguaggio[98].

Nell'ambito della teoria dell'informazione, con il termine *bit* si indica la più piccola unità di informazione esistente e immaginabile che un sistema può gestire[99]. Il termine ha altresì una doppia notazione: la prima, fa riferimento all'unità più piccola che, secondo la numerazione binaria, può avere valore di 0 o 1[100]; la seconda, indica la più piccola unità di dato che un sistema può gestire[101]. In informatica l'uso del termine, derivato da *BInary digiT*[102], identifica la quantità minima indivisibile di informazione e la scelta elementare tra sole due possibilità come, ad es.vero/falso, acceso/spento, tensione

[97] BONI M., *ibidem.*
[98] Così in BONI M., *ibidem*, p. 8.
[99] Cfr. BONI M., *ibidem*, p. 18.
[100] Cfr. TANENBAUM A. S., AUSTIN T., Structured Computer Organization, VI ed., Pearson, Milano, 2013, p. 74.
[101] Cfr. COLLIN S.M.H., Dictionary of Computing, Teddington, 1988: "*bit = (a) smallest unit in binary number notation , wich can have the value 0 or 1 (b) smallest unit of data that a system can handle (...)*.
[102] Cfr. TANENBAUM A. S., AUSTIN T., *ibidem;* il termine bit, che letteralmente significa "un poco, un pezzettino, un bocconcino, viene anche derivato come acronimo di Basic Indissoluble Information Unit; cfr. LOSANO M., Informatica per le scienze sociali. Corso di informatica giuridica, Einaudi, Torino, 1985, p. 128.

presente/tensione assente[103] e qualunque altra dimensione duale come ad esempio si/no, bianco/nero, pieno vuoto, destra sinistra.

Un insieme di bit è detto *stringa.* Una stringa di otto bit costituisce un *byte*[104], ovvero una sequenza utilizzata per codificare un singolo carattere alfanumerico in un computer[105].

L'insieme delle convenzioni e regole con le quali si utilizzano configurazioni prestabilite di bit per rappresentare in modo univoco i numeri, lettere, simboli, si chiama *codice*[106], mentre *codifica* è detta l'operazione di trasformazione di lettere, numeri, simboli in stringhe di bit che un calcolatore (o altro dispositivo) può memorizzare o elaborare.

Un insieme di byte che costituiscono un agglomerato logico (testo, suoni, immagini, filmati…) è detto *file.*

Si definisce *digitalizzazione* il processo di trasformazione di un dato analogico in dato digitale, ovvero la sua rappresentazione mediante la codifica binaria.

Se ad esempio si fa riferimento al *codice ASCII*, questo codifica i caratteri alfanumerici, ovvero l'insieme di tutte le cifre decimali, delle lettere dell'alfabeto, utilizzando 8 bit per ogni carattere per cui, essendo 2 il numero di simboli disponibili (0 e 1) e otto i bit utilizzati per ogni carattere, i caratteri rappresentabili dal codice a 8 bit saranno $2^8 = 256$[107].

[103] Cfr. voce "Bit", in ANTOLA A., MEZZALIRA L., NEGRINI R., SCARABOTTOLO N., Nuovo dizionario di informatica, Mondadori, Milano, 1996.

[104] Termine coniato per assonanza con bite, che letteralmente significa "morso, boccone", e modificato in byte per non confonderlo con bit.

[105] Il byte è formato da 8 bit ed è pertanto in grado di assumere $2^8 = 256$ possibili valori decimali (da 0 a 255); 4 bit, metà di byte, invece, formano un nibble costituito da 4 bit, che consente di rappresentare $2^4 = 16$ valori diversi, cioè le cifre esadecimali 0,1,2,3,4,5,6,7,8,9, a,b,c,d,e,f che consentono la leggibilità umana delle immagini (dump) delle memorie, in particolare dei digest; vi sono poi altri valori multipli del byte, che è diventato anche l'unità di misura della capacità di memoria.

[106] Esistono altri codici standard, tra i quali i più usati sono il codice BCD (Binary Coded Decimal), il codice EBCDDIC (Extended BCD Interchange Code), il codice ASCII (American Standard Code for Information Interchange), il Codice Binario, così in DE ROSSO, L'ABC dell'informatica, Arnoldo Mondandori, Milano, 1988, pp. 61.

[107] Questo è l'attuale sistema di codifica chiamato extended ASCII o high ASCII introdotto da IBM PC che raddoppia la capacità di codifica del codice US-ASCII introdotto nel 1961 e basato su una codifica a 7 bit per un totale di $2^7 = 127$ caratteri; nel 1968 il sistema diventava standard.

Byte	Cod.	Char
00000000	0	Null
00000001	1	Start of heading
00000010	2	Start of text
00000011	3	End of text
00000100	4	End of transmit
00000101	5	Enquiry
00000110	6	Acknowledge
00000111	7	Audible bell
00001000	8	Backspace
00001001	9	Horizontal tab
00001010	10	Line feed
00001011	11	Vertical tab
00001100	12	Form Feed
00001101	13	Carriage return
00001110	14	Shift out
00001111	15	Shift in
00010000	16	Data link escape
00010001	17	Device control 1
00010010	18	Device control 2
00010011	19	Device control 3
00010100	20	Device control 4
00010101	21	Neg. acknowledge
00010110	22	Synchronous idle
00010111	23	End trans. block
00011000	24	Cancel
00011001	25	End of medium
00011010	26	Substitution
00011011	27	Escape
00011100	28	File separator
00011101	29	Group separator
00011110	30	Record Separator
00011111	31	Unit separator

Byte	Cod.	Char
00100000	32	Spc
00100001	33	!
00100010	34	"
00100011	35	#
00100100	36	$
00100101	37	%
00100110	38	&
00100111	39	'
00101000	40	(
00101001	41	)
00101010	42	*
00101011	43	+
00101100	44	,
00101101	45	-
00101110	46	.
00101111	47	/
00110000	48	0
00110001	49	1
00110010	50	2
00110011	51	3
00110100	52	4
00110101	53	5
00110110	54	6
00110111	55	7
00111000	56	8
00111001	57	9
00111010	58	:
00111011	59	;
00111100	60	<
00111101	61	=
00111110	62	>
00111111	63	?

Byte	Cod.	Char
01000000	64	@
01000001	65	A
01000010	66	B
01000011	67	C
01000100	68	D
01000101	69	E
01000110	70	F
01000111	71	G
01001000	72	H
01001001	73	I
01001010	74	J
01001011	75	K
01001100	76	L
01001101	77	M
01001110	78	N
01001111	79	O
01010000	80	P
01010001	81	Q
01010010	82	R
01010011	83	S
01010100	84	T
01010101	85	U
01010110	86	V
01010111	87	W
01011000	88	X
01011001	89	Y
01011010	90	Z
01011011	91	[
01011100	92	\
01011101	93	]
01011110	94	^
01011111	95	_

Byte	Cod.	Char
01100000	96	`
01100001	97	a
01100010	98	b
01100011	99	c
01100100	100	d
01100101	101	e
01100110	102	f
01100111	103	g
01101000	104	h
01101001	105	i
01101010	106	j
01101011	107	k
01101100	108	l
01101101	109	m
01101110	110	n
01101111	111	o
01110000	112	p
01110001	113	q
01110010	114	r
01110011	115	s
01110100	116	t
01110101	117	u
01110110	118	v
01110111	119	w
01111000	120	x
01111001	121	y
01111010	122	z
01111011	123	{
01111100	124	|
01111101	125	}
01111110	126	~
01111111	127	Del

Figura 1 – Codice US-ASCII a 7 bit

Byte	Cod.	Char	Byte	Cod.	Char	Byte	Cod.	Char	Byte	Cod.	Char
10000000	128	Ç	10100000	160	á	11000000	192	+	11100000	224	Ó
10000001	129	ü	10100001	161	í	11000001	193	-	11100001	225	ß
10000010	130	é	10100010	162	ó	11000010	194	-	11100010	226	Ô
10000011	131	â	10100011	163	ú	11000011	195	+	11100011	227	Ò
10000100	132	ä	10100100	164	ñ	11000100	196	-	11100100	228	õ
10000101	133	à	10100101	165	Ñ	11000101	197	+	11100101	229	Õ
10000110	134	å	10100110	166	ª	11000110	198	ã	11100110	230	µ
10000111	135	ç	10100111	167	º	11000111	199	Ã	11100111	231	þ
10001000	136	ê	10101000	168	¿	11001000	200	+	11101000	232	Þ
10001001	137	ë	10101001	169	®	11001001	201	+	11101001	233	Ú
10001010	138	è	10101010	170	¬	11001010	202	-	11101010	234	Û
10001011	139	ï	10101011	171	½	11001011	203	-	11101011	235	Ù
10001100	140	î	10101100	172	¼	11001100	204	¦	11101100	236	ý
10001101	141	ì	10101101	173	¡	11001101	205	-	11101101	237	Ý
10001110	142	Ä	10101110	174	«	11001110	206	+	11101110	238	¯
10001111	143	Å	10101111	175	»	11001111	207	¤	11101111	239	´
10010000	144	É	10110000	176	_	11010000	208	ð	11110000	240	-
10010001	145	æ	10110001	177	_	11010001	209	Ð	11110001	241	±
10010010	146	Æ	10110010	178	_	11010010	210	Ê	11110010	242	_
10010011	147	ô	10110011	179	¦	11010011	211	Ë	11110011	243	¾
10010100	148	ö	10110100	180	¦	11010100	212	È	11110100	244	¶
10010101	149	ò	10110101	181	Á	11010101	213	i	11110101	245	§
10010110	150	û	10110110	182	Â	11010110	214	Í	11110110	246	÷
10010111	151	ù	10110111	183	À	11010111	215	Î	11110111	247	¸
10011000	152	ÿ	10111000	184	©	11011000	216	Ï	11111000	248	º
10011001	153	Ö	10111001	185	¦	11011001	217	+	11111001	249	¨
10011010	154	Ü	10111010	186	¦	11011010	218	+	11111010	250	·
10011011	155	ø	10111011	187	+	11011011	219	_	11111011	251	¹
10011100	156	£	10111100	188	+	11011100	220	_	11111100	252	³
10011101	157	Ø	10111101	189	¢	11011101	221	¦	11111101	253	²
10011110	158	×	10111110	190	¥	11011110	222	Ì	11111110	254	■
10011111	159	ƒ	10111111	191	+	11011111	223	_	11111111	255	

Figura 2 – Codice extended ASCII a 8 bit

Tuttavia, il codice ASCII, anche in formato esteso, non ha simboli e capacità sufficiente per rappresentare tutti i caratteri alfanumerici dei vari alfabeti usati nel mondo (arabo, cirillico, ebraico, ecc.). Per questo, è nato l'Unicode Consortium[108], un consorzio formato da società produttrici di computer che hanno creato un nuovo sistema di codifica chiamato Unicode, poi divenuto standard nel 2012 (IS 10646), basato prima su una codifica a 16 bit e poi a 21 bit[109].

Poiché anche Unicode presenta dei limiti, la codifica viene effettuata anche con altri codici, la cui logica elementare è analoga a quelle dei codici già esaminati[110].

[108] http://www.unicode.org/consortium/consort.html .
[109] TANENBAUM A. S., AUSTIN T., op.cit., pp. 138 e ss..
[110] TANENBAUM A. S., AUSTIN T., op.cit., p. 141.

3.2.1 La codifica di immagini, suoni e filmati

I dati riguardanti rappresentazioni di testo sono stati solo i primi esempi di contenuti ad essere stati codificati, ma non sono rimasti gli unici.

L'aumento della capacità di calcolo dei computer e della capacità delle memorie ha reso possibile gestire le grandi quantità di dati necessarie alla codifica di immagini, suoni e filmati[111].

Infatti, anche le immagini e i suoni vengono rappresentati grazie alla codifica binaria.

La codifica delle immagini è possibile grazie ad un processo diverso da quello del procedimento di codifica dei testi. Infatti, la codifica delle immagini può essere di tipo *vettoriale* oppure *raster* (o *bitmap*).

Nel primo caso, l'immagine è descritta mediante elementi primitivi quali punti, linee o poligoni, per ognuno dei quali è definita una colorazione o una sfumatura, che poi vanno a comporre l'immagine.

Nel secondo l'immagine è composta da una matrice di punti, detti *pixel*, la cui colorazione è codificata tramite uno o più bit.

Nelle immagini monocromatiche in scala di grigio, il valore indica l'intensità del grigio, che varia dal nero al bianco[112].

Nelle immagini a colori, invece, il pixel assume il livello di intensità dei colori fondamentali[113].

Per la codifica dei suoni, invece, bisogna considerare che dal punto di vista fisico, il suono è rappresentato da un'onda (*onda sonora*) che descrive la variazione della pressione dell'aria, rispetto alla pressione atmosferica, nel tempo, e che graficamente può essere rappresentato ponendo sull'asse delle ordinate la variazione di pressione, cioè il suono stesso e sull'asse delle ascisse il tempo.

Tale rappresentazione è detta *analogica* e descrive esattamente il fenomeno continuo dell'onda sonora. La rappresentazione digitale dell'onda avviene mediante una serie di bit che ne forniscono una descrizione discreta: maggiore è il numero di bit usati, più fedele sarà la rappresentazione dell'audio (e maggiore la dimensione del file).

La digitalizzare di un'onda sonora si basa sul campionamento: si misura l'ampiezza dell'onda a intervalli costanti nel tempo; più frequenti sono i

[111] Per le tecniche di codifica delle immagini, v. GONZALEZ R. C., WOODS R. E., Elaborazione delle Immagini, III ed., Pearson, 2008; per le tecniche di codifica dei suoni, v. LOMBARDO V., VALLE A., Audio e multimedia, ed. 4. Apogeo, 2014; per le tecniche di codifica video, GONZALEZ R. C., WOODS R. E., Digital Image Processing, op.cit.

[112] Un caso particolare di immagine in scala di grigio è l'immagine in bianco e nero, per il quale si utilizza un solo bit per pixel per rappresentare il bianco oppure il nero.

[113] Nel modello di colore RGB, uno dei più usati, i colori base utilizzati sono il rosso, il verde e il blu. Nel modello CMYK, usato per la stampa, i colori base sono il ciano, il magenta, il giallo e il nero.

campionamenti, più precisa sarà la sua rappresentazione. Ogni misurazione sarà poi convertita mediante il codice binario[114].

La codifica dei video, infine, avviene secondo tecniche che si dividono in due grandi famiglie: la codifica *intraframe* e la codifica *interframe*.

Con la codifica intraframe viene codificato e decodificato un flusso video descrivendo ogni singolo fotogramma che compone la sequenza video, secondo l'approccio tradizionale che quantizza il video come sequenza di immagini statiche. Tale tecnica è più adatta a video con sequenze particolarmente movimentate.

Con la codifica interframe invece, partendo da un fotogramma iniziale condificato secondo la tecnica intraframe, vengono descritti i cambiamenti che si verificano tra un fotogramma ed il successivo. Tale tecnica è più adatta a sequenze video più statiche[115].

3.2.2 La natura fisica e la dimensione del bit

Tornando all'elemento costitutivo dei bit, la connessione tra questi e la memoria sulla quale sono archiviati dà luogo ad una problematica di rilevante importanza ai fini della definizione delle metodologie tecniche e delle regole per il corretto trattamento dei dati a fini giuridici e processuali: i bit sono elementi materiali o immateriali?

Sul piano strettamente giuridico, la questione assume un'ampia rilevanza in quanto le implicazioni derivanti dalla definizione della "sostanza" di cui sono fatti i bit costituisce il presupposto per la corretta qualificazione giuridica dei fatti informatici. Infatti, come si vedrà nel prosieguo, per il giurista chiamato ad applicare le norme alle fattispecie concrete, è importante stabilire se un oggetto abbia un dimensione materiale o immateriale. Alcune norme, infatti, per la loro applicazione alla fattispecie, presuppongono la materialità dell'oggetto come elemento indefettibile; altre norme, invece, ove vengano applicate ad oggetti immateriali, implicano l'adozione diretta o indiretta di iniziative volte a salvaguardare le caratteristiche di completezza e affidabilità delle informazioni derivanti dai bit.

Il problema della materialità o immaterialità del bit si muove innanzitutto sul piano ontologico-filosofico, tanto da costituire per alcuni un elemento fondamentale per elevare il bit a paradigma e strumento di conoscenza del reale[116].

---

[114] FERRAZZANO M., Seminario su Aspetti tecnici di Informatica forense, a.a. 2015-2016, Scuola di Giurisprudenza, Alma Mater - Università di Bologna, Bologna.

[115] Cfr. voce Codec video in *https://it.wikipedia.org/wiki/Codec_video*.

[116] Sugli aspetti filosofico-ontologici dei fenomeni digitali, v. LONGO G. O., VACCARO A., Bit Bang, La nascita della filosofia digitale, Maggioli, Santarcangelo di Romagna, 2013, p. 107 e ss., i quali ripercorrono la storia del pensiero degli autori che indagando il rapporto tra informazione e bit, giungono ad individuare nell'informazione l'*archè* nell'accezione dei

In un saggio fondamentale sui temi digitali, alla domanda "*Ma che cos'è un bit ?*", l'Autore dava una risposta inequivocabile:" *Un bit non ha colore, dimensioni o peso, e può viaggiare alla velocità della luce. È il più piccolo elemento atomico del DNA dell'informazione. È un modo di essere: si o no, vero o falso, su o giù, dentro o fuori, nero o bianco. Per praticità noi diciamo che un bit è 1o 0 Che cosa significhi l'1 o lo 0 è un altro discorso. Ai primordi dell'era del computer una stringa di bit generalmente rappresentava informazioni di tipo numerico (...)*"[117].

Tuttavia, su un piano più pratico, allo stato della tecnologia, la questione della materialità dei bit impone di considerare, seppur sommariamente, gli aspetti tecnici riguardanti la stessa dimensione fisica dei bit in rapporto con la memoria sulla quale sono registrati.

Sin dai primi passi dell'informatica, la tecnologia di registrazione dei bit sulle memorie e le stesse tipologie di memorie hanno subito una costante evoluzione[118].

I tipi di memorie vengono classificate in primarie (o centrale) e secondarie (o di massa)[119].

La memoria primaria è quella usata in fase di esecuzione del programma, ha tempi di accesso rapidi, di poche decine di nanosecondi, per assecondare la velocità del processore. Grazie al progresso tecnologico, le memorie primarie[120] si sono evolute dalle valvole termoioniche, a quelle a nuclei di ferrite, alle memorie a circuiti integrati sempre più miniaturizzati, sino alle attuali memorie dai tempi di accesso, costo per bit e potenza dissipata sempre più ottimizzati[121].

Le memorie secondarie, invece, hanno tempi di accesso molto più lunghi di quelli delle memorie primarie, millisecondi o più, che dipendono dalla necessità

filosofi presocratici, e a qualificare il bit da elemento essenziale ontologico a noumeno dell'informazione alla base dell'essere e quindi immateriale per definizione.

[117] NEGROPONTE, N., Essere digitali, Sperling e Kupfer, Milano, 1995, p. 3 e ss..

[118] Per una storia dell'evoluzione dei computer, v. http://www.computerhistory.org/timeline/computers/ ; v. anche http://www.tecnoteca.it/museo/introduzione/document_view .

[119] Per i diversi tipi di memorie, v. TANENBAUM A. S., AUSTIN T., Structured Computer Organization, VI ed., Pearson, 2013, pp. 73 e ss..

[120] Per una breve rassegna dell'evoluzione tecnologica delle memorie primarie, v. http://www.tecnoteca.it/museo/15 .

[121] A tal proposito, assumono rilevante importanza due notizie di questi giorni: la prima riguarda la crisi per motivi industriali dell'evoluzione dei processi produttivi dei chip annunciata dalla più grande azienda produttrice di microprocessori al mondo (v. http://punto-informatico.it/4307925/PI/News/intel-addio-al-tick-tock.aspx); tale crisi potrebbe riverberarsi sulla legge di Moore secondo la quale il numero di transistor in un microchip raddoppia ogni due anni circa, con un incremento proporzionale nelle performance raggiungibili, nel risparmio dei costi e nella riduzione dell'energia necessaria al funzionamento delle CPU al silicio (http://punto-informatico.it/4301666/PI/News/legge-moore-fine-un-era.aspx); la seconda notizia, invece, riguarda il rilascio del microprocessore free ed opensource PULPino (v. http://www.pulp-platform.org/ e http://iis-projects.ee.ethz.ch/images/d/d0/Pulpino_poster_riscv 2015.pdf), i cui sviluppi nel campo della tecnologia dei microprocessori potrebbero assumere rilevanza analoga a quella avuta dal sistema operativo GNU/Linux nel campo del software, sul quale v. https://www.gnu.org/gnu/linux-and-gnu.html .

di collocare in bit in lettura o scrittura. La tecnologia delle memorie secondarie si è evoluta passando dai sistemi a schede perforate ai nastri magnetici, memorie flash, al disco magneto-ottico, ai dischi ottici (CD-ROM, DVD, Blu-Ray Disc)[122]. I dischi magnetici possono essere di vario tipo: IDE, SCSI, RAIDs. Nel genere dischi ottici sono inclusi i CD-ROMs, i CD-Rs, i DVDs e i Blu-Rays.

Allo stato del progresso tecnologico, un bit, nella sua fase statica, non può prescindere dalla memoria sul quale sia registrato.

Pertanto, anche la dimensione fisica di un bit dipende dalla tecnologia della memoria, primaria o secondaria che sia[123], e dal tipo di materiale di cui è composta la stessa.

La dimensione fisica del bit può essere anche visualizzata e misurata con l'utilizzo di potentissimi microscopi o apparecchiature microelettroniche. Nella Figura 3[124] sono visibili delle sequenze di bit registrati su un hard disk e rilevati con una sonda MFM (Magnetic Force Microscope). I bit sono di dimensione di circa 180 nm (nanometro; 180 miliardesimi di metro cioè milionesimi di millimetro) distanziati di cerca 370 nm, dando origine quindi a una densità di cerca 5 Gbits/pollice cioè 5 miliardi di bit per 2.3 cm.

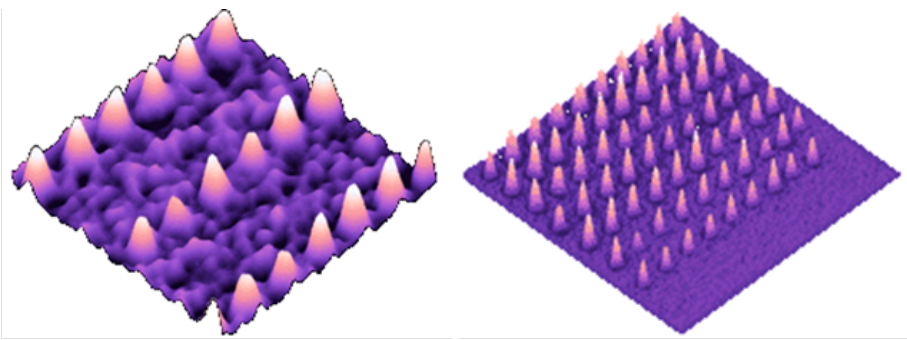

Figura 3 – Bit magnetici rilevati con una sonda MFM (Magnetic Force Microscope)

E tuttavia, le dimensioni raggiunte dalle nanotecnologie in tale settore non costituiscono ancora il limite ultimo. Infatti, le ricerche compiute negli ultimi

[122] Per una breve rassegna dell'evoluzione tecnologica delle memorie secondarie, v. http://www.tecnoteca.it/museo/16/document_view .

[123] TANENBAUM A. S., AUSTIN T., op.cit., pp. 74 e ss..

[124] Tratte da http://chemistry.oregonstate.edu/courses/ch448/CH448Images/VEECO%20AFM-%20Images.htm; per comprendere le grandezze di cui si sta trattando si deve pensare che non esistono esseri viventi rapportabili alla scala dei 10 nanometri (un nanometro = 1.000.000.000mo di metro = 1.000.000mo di millimetro), mentre a tali dimensioni possono rapportarsi le più grandi macromolecole come il DNA di una cellula umana; www.treccani.it/scuola/.html , per cui nell'uomo il codice genetico è formato da circa tre miliardi di nucleotidi; poiché la distanza media tra due nucleotidi successivi in un filamento è dell'ordine di circa 0.2 nanometri (nm; 1 m = 1 miliardo di nm), il DNA contenuto in ogni cellula ha una lunghezza di circa 1 m ed è spesso solo 2 nm. Per poter essere contenuto in una cellula grande 10 micron (1m = 1 milione di micron) questo lunghissimo filamento deve necessariamente ripiegarsi su se stesso e formare strutture di complessità crescente che siano adatte a mantenerlo in forma compattata, con una lunghezza pari a circa 500 milioni di volte il suo diametro.

anni, dopo aver superato il traguardo della modellazione di tecnologie basate sul principio "un bit per molecola"[125], si sono inoltrate sia nella realizzazione di tecniche di archiviazione dei dati che utilizzano come supporto un filamento di DNA[126], sia nella modellazione di bit a dimensione atomica, per poi giungere alla modellazione di bit che, basandosi sui principi e proprietà della meccanica quantistica[127], ha consentito la costruzione di computer quantistici (o quantici)[128] che superano la logica stessa del calcolo binario basato sulla materialità del bit.

Pertanto, le considerazioni che seguiranno sono valide solo in relazione alle procedure di codifica e memorizzazione dei bit secondo la tecnologia attualmente diffusa sul mercato, e andranno riviste in conseguenza della futura evoluzione tecnologica.

I bit, oltre a trovarsi staticamente archiviati su memoria, possono anche essere teletrasmessi mediante tecniche di commutazione a pacchetto.

In tale situazione i bit vengono trasmessi attraverso una rete associando ogni bit ad un fenomeno fisico che può essere riprodotto a distanza attraverso un mezzo di trasmissione. In tal caso, i bit vengono sottoposti ad un'ulteriore codifica piuttosto complessa. In base al tipo di fenomeno fisico utilizzato, i mezzi trasmissivi utilizzati nelle reti si suddividono attualmente in tre categorie:

- mezzi elettrici: sono i mezzi utilizzati nel passato e che, sfruttando la proprietà dei metalli di condurre energia elettrica, consentono la trasmissione dei dati associando i bit a particolari valori di tensione o di corrente, o determinate variazioni di tali grandezze;
- onde radio (c.d. mezzi wireless): sono mezzi intervenuti successivamente alle tecniche basate sulla trasmissione elettrica e

[125] Cfr. MIYAMACHI T., GRUBER M., DAVESNE M., BOWEN M., BOUKARI S., JOLY L., SCHEURER F., ROGEZ G., KAZU YAMADA T., OHRESSER P., BEAUREPAIRE E., WULFHEKE W., Robust spin crossover and memristance across a single molecule, 3/7/2012, in *http://www.nature.com/ncomms/journal/v3/n7/full/ncomms1940.html*.

[126] v. CHURCH G. M, GAO Y., KOSURI S., Next-Generation Digital Information Storage in DNA, in http://arep.med.harvard.edu/pdf/Church_Science_12.pdf, e supplementi in *http://science.sciencemag.org/content/sci/suppl/2012/08/15/science.1226355.DC1/Church.SM.pdf*; gli Autori avrebbero codificato il contenuto di un libro su base quaternaria anzichè binaria e sfruttando le quattro diverse basi azotate (Adenina, Citosina, Guanina, Timina), lo avrebbero trascritto in un filamento di DNA, riuscendo poi a recuperarne il contenuto, asserendo che tale metodo consentirebbe l'aumento della capacità di archiviazione e una maggiore durata della stessa nel tempo.

[127] Branca della fisica moderna che descrive il comportamento controintuitivo di particelle microscopiche come fotoni, elettroni e quark.

[128] I computer quantistici elaborano i *qubit*, codificazione dello stato quantistico di una particella, o di un atomo, che può assumere più valori diversi nello stesso istante. Per un'introduzione al tema, v. *https://it.wikipedia.org/wiki/Computer_quantistico*; per le ultime ricerche nel campo dei materiali da utilizzarsi per nuove tipologie di computer quantici, v. il recente BANERJEE A., BRIDGES C.A., YAN J.-Q., ACZEL A. A., LI L., STONE M. B., GRANROTH G. E., LUMSDEN M. D., YIU Y., KNOLLE J., BHATTACHARJEE S., KOVRIZHIN D. L., MOESSNER R., TENNANT D. A., MANDRUS D. G., NAGLER S. E., Proximate Kitaev quantum spin liquid behaviour in a honeycomb magnet, 2016, in *http://www.nature.com/nmat/journal/vaop/ncurrent/full/nmat4604.html#access*.

che hanno conosciuto molte e diverse applicazioni (reti locali, collegamenti via ponte radio o satellite per le reti geografiche). In tali tecnologie, lo strumento fisico sfruttato per la trasmissione dei dati associati ai bit è l'onda elettromagnetica, ovvero la combinazione di un campo elettrico e un campo magnetico variabili, che ha la proprietà di di propagarsi nello spazio e di riprodurre a distanza una corrente elettrica di un dispositivo ricevente (antenna);

- mezzi ottici: fibre ottiche e da ultimo laser, ovvero tecnologie trasmissive molto recenti che sfruttano il fenomeno fisico della luce[129].

Tali mezzi trasmissivi si basano tutti sul trasporto di una qualche forma di energia che codifica i bit (così chiamato *segnale)* al quale si oppone il sistema fisico attraversato determinando così un'attenuazione dell'energia trasmessa. Tale attenuazione è altresì diversa a seconda della frequenza, cosicché per ogni sistema fisico si avrà una banda passante, ovvero l'insieme delle frequenze che possono essere trasmesse senza attenuazione eccessiva[130].

Per trasmettere le informazioni codificate in formato digitale, la tecnica più elementare è quella di associare i bit a determinati valori per lo zero e altri per l'uno, mentre la tecnica più complessa è quella che garantisce la corretta sincronizzazione del ricevitore con il trasmettitore che permettono di ridurre la banda necessaria alla trasmissione[131].

Tornando al quesito iniziale, ovvero se i bit siano materiali o immateriali, la disamina appena svolta ci induce a ritenere che, allo stato attuale della tecnologia:

1. i bit, e quindi i dati codificati, vengono letti dalla memoria e archiviati sulla stessa (o diversa) mediante modifica della materia di cui è composto il supporto sul quale sono archiviati
2. i bit elaborati dal sistema sono successivamente rappresentati dal sistema;
3. i bit teletrasmessi, a prescindere dalla tecnologia e dalla tecnica utilizzata, sono disgunti da qualunque supporto materiale e quindi sono immateriali.

3.2.3 I rapporti tra bit, memorie e strumenti di trasmissione

Tornando al dilemma iniziale circa la materialità o immaterialità del bit, questo non può essere risolto in via unitaria, univoca e definitiva in quanto, allo stato attuale, esso dipende dal tipo di tecnologia con la quale esso viene trattato.

---

[129] Così in GAI S., MONTESSORO P.L., NICOLETTI P., Reti Locali. Dal cablaggio all'internetworking, Scuola Superiore G. Reiss, L'Aquila, 1995, pp. 27-28.
[130] *Ibidem,* p. 28.
[131] *Ibibem,* p. 29 e ss..

Infatti, se si considera un bit archiviato su una memoria secondaria costituita da una base materiale, (nastro magnetico, floppy disk, hard disk, memoria ottica), il bit si configura come la risultante della deformazione o meno della materia della base materiale sulla quale esso viene archiviato, per cui la materialità del bit dipenderà proprio dalla stretta connessione tra lo stesso e la memoria secondaria sulla quale esso è archiviato.

Allorquando invece il bit venga elaborato dalla memoria primaria, in quanto impulso tensionale elettrico, si trova, come dire, separato dalla materia della memoria secondaria, per cui in tale fase è propriamente dematerializzato.

Ad analoga conclusione si perviene anche allorquando i bit si trovino nella fase dinamica di trasmissione telematica, per i motivi tecnici già esposti sopra.

La disamina appena svolta induce a ritenere che, allo stato attuale della tecnologia:

1. i dati codificati in codice binario, e per completezza le informazioni codificate, non possono prescindere dai bit che li rappresentano;
2. i bit, e quindi i dati codificati, vengono letti dalla memoria e archiviati sulla stessa mediante modifica della materia di cui è composto il supporto sul quale sono archiviati;
3. i bit elaborati dal sistema e quelli teletrasmessi attraverso le reti sfruttando le proprietà fisiche dell'elettricità, delle onde elettromagnetiche e della luce, sono immateriali.

Alla struttura materiale o immateriale dei bit conseguono alcune considerazioni che vanno sempre tenute presenti per una corretta impostazione del metodo di trattamento dei dati a fini processuali:

1. necessità di una memoria[132] (hard disk, floppy disk, flash memory): nei casi in cui i bit si trovano in fase statica, la loro dimensione fisica impone che non si possono ipotizzare documenti che per la cui fruibilità non necessitino di una memoria; allorquando invece si trovino in fase dinamica, la corretta formazione del quadro informativo derivante dai bit impone che vengano elaborati o acquisiti tutti i bit (o la loro maggior parte) che fanno parte del flusso;
2. riproducibilità in numero infinito di copie: grazie alla loro codifica digitale, le stringhe di bit più o meno lunghe possono essere replicate uguali a se stesse in un numero infinito di stringhe sempre perfettamente uguali tra loro, come verificabile mediante calcolo e confronto dei rispettivi hash[133];

[132] La dottrina giuridica e spesso anche la giurisprudenza non prestano molta attenzione al rigore definitorio proprio dell'informatica, preferendo così l'uso del termine "supporto" in luogo di quello più corretto di "memoria".

[133] Per una definizione di hash, v. https://it.wikipedia.org/wiki/Hash, secondo la quale:"*Nel linguaggio matematico e informatico, l'hash è una funzione non iniettiva (e quindi non*

3. volatilità: la tecnologia sulla quale si basa il funzionamento delle memorie primarie[134], dette anche memorie volatili, richiede una continua alimentazione elettrica, cosicché i bit da esse elaborati non sono permanentemente archiviati, ma si perdono nel caso in cui l'alimentazione elettrica si interrompa;
4. deteriorabilità: i bit archiviati sulle memorie secondarie solo apparentemente sembrano essere destinati a rimanere disponibili per tempi prolungati; in realtà, la capacità di rimanere leggibili nel tempo, dipende dalla tecnologia utilizzata per la costruzione e l'utilizzo delle memorie secondarie e per la fissazione del dato alla memoria. Su un piano strettamente fisico, le memorie secondarie risentono dei limiti intrinseci al materiale di cui esse sono composte. Tali parametri condizionano il degrado dei bit e quindi dei dati e delle informazioni desumibili, cosicché i bit archiviati sulle stesse sono soggetti a fenomeni di deteriorabilità e illeggibilità che vanno sotto il nome di "obsolescenza digitale"[135]. Tale fenomeno si manifesta per tutti i documenti digitalizzati, fino a renderli inutilizzabili in tempi relativamente brevi;
5. modificabilità (quasi) anonima: in virtù della mediazione dell'hardware e del software nel processo di creazione e archiviazione di bit, questi ultimi non presentano in sé e per sé elementi fisici che consentano di risalire univocamente all'operatore che li ha creati, modificati, trasferiti o cancellati, nè alle caratteristiche che instaurino un rapporto tra bit e operatore, rapporto che può essere inferito sulla base di informazioni desumibili *aliunde* rispetto alle caratteristiche fisiche specifiche dei bit.

Le considerazioni esposte costituiscono non solo la base ontologica e fisica minimale per una corretta qualificazione giuridica dei fatti informatici processualmente rilevanti, ma consentono di poter svolgere le successive considerazioni in merito alle migliori tecniche per l'acquisizione dei bit e quindi dei dati sia in fase statica (Computer forensics) che dinamica (Network forensics).

Inoltre, tale inquadramento fattuale del fenomeno informatico consentirà anche la verifica di correttezza dei presupposti di fatto posti dalla

invertibile) che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita. Esistono numerosi algoritmi che realizzano funzioni hash con particolari proprietà che dipendono dall'applicazione." Tale funzione è stata sviluppata in ambito crittografico.

[134] Sulle memorie primarie, v. TANENBAUM A. S., AUSTIN T., op.cit., pp. 73 e ss..

[135] Sul deterioramento dei supporti digitali sull'evoluzione degli strumenti informatici utilizzati per crearli, modificarli e leggerli, cfr. voce "Obsolescenza digitale" in http://www.treccani.it/ enciclopedia/ obsolescenza-digitale_%28Lessico-del-XXI-Secolo%29/

giurisprudenza a fondamento delle decisioni che interessano il trattamento dei dati informativi a fini processuali.

3.2.4 La natura giuridica dei bit

L'approfondimento delle caratteristiche fisiche del dato digitale e delle sue componenti, i bit, costituisce il principio e il fondamento di una corretta comprensione del fenomeno informatico quale presupposto indefettibile per la sua corretta qualificazione giuridica.

L'approccio scientifico alla definizione della natura fisica del dato e del bit consente al giurista:

1. di comprendere le caratteristiche "materiali" degli elementi di prova costituiti dai bit e dalle successioni di bit;
2. di stabilire una base conoscitiva che, nella fase attuale del progresso tecnologico, sia utile alla ricostruzione del quadro esegetico e applicativo degli istituti processuali secondo principi più appropriati e rispettosi della realtà fattuale di quelli attualmente in voga;
3. di ridelineare le aree e i limiti di applicabilità delle norme sui dati digitali e in particolar modo quelle riguardanti mezzi di prova e di ricerca della prova ad oggetto informatico (si pensi ad es. alle norme sull'ispezione informatica, sul sequestro di dati e corrispondenza informatici e telematici, sull'intercettazione di flussi telematici).

Se si esclude la tutela del dato come opera dell'ingegno o come dato personale soggette a particolari presupposti oggetti e soggettivi, il dato digitale in sé e per sé non è classificato come autonomo oggetto tutelato dal diritto. Infatti, l'art. 810 del Codice civile, nell'ambito della nozione di beni mobili, prevede che "*Sono beni le cose che possono formare oggetto di diritti*".

Tradizionalmente si ritiene che poiché i bit in sé non hanno una materialità tale da consentirne la qualificazione come "cose" – rientrando in tale concetto al più la memoria sulla quale i dati sono archiviati – essi non possono essere ritenuti "cose", mancando del requisito della materialità. Pertanto, i bit non vengono ricompresi tra i beni mobili[136].

In realtà nell'ambito del diritto civile, la materialità dei beni non costituisce un elemento indefettibile tant'è che vi sono innumerevoli beni immateriali – come le opere dell'ingegno e i diritti di credito – che, pur non essendo "cose" in senso stretto o materiale, rientrano nella categoria dei beni mobili a tutti gli effetti e sono oggetto di atti dispositivi, di *traditio* e finanche di abbandono.

[136] Di parere contrario è PICA G., Diritto penale delle tecnologie informatiche, op.cit., p. 27, il quale correttamente allerta dal pericolo di estendere ai dati la qualità di beni immateriali, che invece è attributo proprio del diritto sull'oggetto, come ad esempio un software.

Inoltre, il codice civile conosce anche la particolare categoria delle energie naturali[137] che, pur tradizionalmente ritenute immateriali[138], rientrano nella categoria dei beni mobili prevista dall'art. 814 c.c., secondo il quale: "*Energie. Si considerano beni mobili le energie naturali che hanno valore economico*".

Ciò che rileva ai fini della presente trattazione è che la questione della classificabilità dei bit e dei dati come beni mobili ricorda molto l'analoga questione della qualificazione giuridica dell'energia elettrica e della sua sussumibilità all'interno della più ampia categoria dei beni mobili affrontata già negli anni 30[139], a seguito dell'ingravescenza del fenomeno delle sottrazioni di energia elettrica non punibili a titolo di furto stante la mancata qualificabilità delle energie come beni mobili.

Il legislatore del 1930, superando con una *fictio juris* le discussioni intervenute sotto la vigenza del Codice penale Zanardelli, introdusse nel codice penale la fattispecie del furto di energie annoverandole espressamente fra i beni mobili, per cui l'attuale lettera del reato di furto, all'art. 624 (Furto) c.p., prevede che: "*(...) Agli effetti della legge penale, si considera cosa mobile anche l'energia elettrica e ogni altra energia che abbia valore economico*[140].

Quella stessa questione, portato dell'evoluzione tecnologica, si pone oggi anche in relazione al concetto di bit senza che tuttavia sia possibile un'applicazione analogica dell'espressa previsione relativa alle energie, ostando a ciò il principio di legalità della legge penale e, nell'articolazione del principio di tassività, il divieto di applicazione analogica di norme penali a casi diversi non ricompresi nella fattispecie penale espressa.

Nonostante la mancata previsione normativa dei dati e dei bit come beni mobili, la dimensione "reale" dei bit sembra invece essere presupposta dalla previsione dell'art. 392 c.p. (Esercizio arbitrario delle proprie ragioni con violenza sulle cose)[141] il quale prevede che:"*Chiunque, al fine di esercitare un preteso diritto, potendo ricorrere al giudice, si fa arbitrariamente ragione da sé medesimo, mediante violenza sulle cose, è punito, a querela della persona offesa (120 ss.; 336 ss. c.p.p.), con la multa fino a euro 516.*

---

[137] Nella categoria delle energie naturali vengono annoverate l'energia elettrica, radioelettrica, termica o cinetica.

[138] Cfr. PARDOLESI R., voce Energia, in *Digesto delle Discipline Privatistiche,* sez. civ., vol VIII, Torino, 1991.

[139] Sulle energie come oggetto di rapporti giuridici, v. CARNELUTTI, F., Studi sulle energie come oggetto di rapporti giuridici, in Studi di diritto civile, Roma, Atheneum, 1916, p. 117 e ss..

[140] Cfr. AMARELLI G., Furto (art. 624 c.p.), in FIORE, S., (a cura di), Reati contro il patrimonio, Utet, Torino, 2010.

[141] Il testo in esame è quello dell'art. 324 c.p. come modificato dalla L. 347/93 che ha introdotto nel sistema penale i reati informatici. La norma in esame realizza una discrasia rispetto al diverso ambito giuridico costituito dal diritto d'autore, non distinguendo la componente immateriale costituente il *corpus mysticum* dal *corpus mechanicum* costituito dal supporto materiale che incorpora il software.

Agli effetti della legge penale, si ha «violenza sulle cose» allorché la cosa viene danneggiata o trasformata, o ne è mutata la destinazione.

Si ha, altresì, violenza sulle cose allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico". In tale norma, l'illiceità della "violenza sulle cose" è specificamente prevista come consumabile anche anche in relazione al "programma informatico" che, essendo notoriamente composto di bit, mal si presta ad essere annoverabile nel concetto di "cose"[142].

Sulla questione, le posizioni non sono concordi.

In dottrina, alcuni Autori[143] propendono espressamente per la materialità dei bit.

In giurisprudenza, invece, si registrano diversi orientamenti, per cui alcune decisioni propendono per la materialità dei dati[144], altre, invece, per la loro immaterialità[145].

3.3 La rilevanza dell'integrità dei bit ai fini delle indagini

I rilievi appena esposti confermano uno dei postulati dell'Informatica forense, ovvero la necessità di preservare l'integrità dei bit che compongono i dati ove se ne intenda trarre informazioni da utilizzarsi in sede processuale.

La necessità di applicare tutti i principi elaborati dall'Informatica forense in tema di trattamento dei dati ad uso processuale hanno come unica finalità quella di preservare l'integrità delle sequenze di bit Affinché le informazioni derivate dalle parti del procedimento possano essere attendibili per tutte le parti.

In via esemplificativa, i seguenti esperimenti[146] mirano a verificare se vi sia e quale sia la variazione dell'informazione alla variazione di un solo bit o di un solo byte di una stringa di dati.

Esperimento A: variazione di date (nascita, incontro, attentato, ecc.) mediante posposizione di un solo bit:

1) si prenda una data espressa in valori decimali e simboli (.) e la si codifichi;
2) se alla data 2**5**.07.1966 espressa dalla seguente sequenza di bit:

[142] Cfr. PICA, op.cit., p. 33.
[143] Tra questi cfr. GIANNANTONIO, E., op.cit., p. 462 1e PICA, *ibidem.*
[144] Cfr. Cass. Sez. Un. 9 ottobre 1996 (Giust. Pen. 1998, III, 65 e ss.), Trib. ries. Alessandria, ord. 14-15/11/2001.
[145] Cfr. Cass., Sez. II, sent. 13/01/2005 n. 308, Buzzoni, Non è configurabile il reato di ricettazione a carico di soggetto che si sia limitato a ricevere dati, informazioni e notizie tratti da materiale documentario che sia stato oggetto di furto, mancando, in siffatta ipotesi, l'esistenza di una "res" suscettibile di apprensione e possesso.
[146] Gli esperimenti sotto riportati sono stati eseguiti con il traduttore di testo in codice binario liberamente disponibile in *http://binarytranslator.com/* e possono quindi essere replicati e verificati.

00110010 00110**01** 00101110 00110000 00110111 00101110 00110001 00111001 00110110 00110110
si pospongono i due bit in grassetto, da 01 a 10,
00110010 00110**10** 00101110 00110000 00110111 00101110 00110001 00111001 00110110 00110110
si avrà la diversa data 2**6**.07.1966.

<u>Esperimenti B</u>: **variazioni di date mediante variazione di un bit**:

<u>Esperimento B.1)</u>

1) si prenda una data espressa in valori decimali e simboli (.) e la si codifichi
2) se alla data 26.07.19**6**6 espressa dalla seguente sequenza di bit:
00110010 00110110 00101110 00110000 00110111 00101110 00110001 00111001 00110**1**10 00110110
varia il bit in grassetto, da 1 a 0,
00110010 00110110 00101110 00110000 00110111 00101110 00110001 00111001 00110**0**10 00110110
la data cambierà in 26.07.19**4**6.

<u>Esperimento B.2)</u>

1) si prenda una data espressa in valori decimali e simboli (.) e la si codifichi
2) se alla data 26.07.19**6**6 espressa dalla seguente sequenza di bit:
00110010 00110110 00101110 00110000 00110111 00101110 00110001 00111001 00110110 00110110
cambia il bit in grassetto, da 0 a 1,
00110010 00110110 00101110 00110000 00110111 00101110 00110001 00111001 00110111 00110110
la data cambia in 26.07.19**7**6

<u>Esperimento B.3)</u>

1) si prenda una data espressa in valori decimali e simboli (.) e la si codifichi
2) se alla data 26.07.19**6**6 espressa dalla seguente sequenza di bit:
00110010 00110110 00101110 00110000 00110111 00101110 00110001 00111001 00110110 00110110
varia il bit in grassetto, da 0 a 1,
00110010 00110110 00101110 00110000 00110111 00101110 00110001 00111001 00110110 00110111
la data cambia in 26.07.196**7**

<u>Esperimento C)</u>: variazione del senso di un messaggio mediante posposizione di un byte

1) si prenda il messaggio: “Michele, oggi ti ammazzerò ciao” e lo si codifichi
01001101 01101001 01100011 01101000 01100101 01101100 01100101 00101100 00100000 01101111 01100111 01100111 01101001 00100000 01110100 01101001 00100000 01100001 01101101 01101101 01100001 01111010 01111010 01100101 01110010 11000011 10110010 00001010 01100011 **01100001 01101001** 01101111

c **i** **a** o

2) se si pospone un byte, il messaggio si trasformerà nel messaggio: “Michele, oggi ti ammazzerò caio”

01001101 01101001 01100011 01101000 01100101 01101100 01100101
00101100 00100000 01101111 01100111 01100111 01101001 00100000
01110100 01101001 00100000 01100001 01101101 01101101 01100001
01111010 01111010 01100101 01110010 11000011 10110010 00001010
01100011 **01101001 01100001** 01101111

c **a** **i** o

Ebbene, questi semplici e banali esperimenti, compiuti su pochissimi bit rispetto ai miliardi di bit che compongono i documenti complessi, consentono di comprendere come in relazione ai dati di un file, siano essi anche solo metadati, il cambiamento di anche un solo bit non determina solo il cambio di un dato, ma può comportare anche un completo stravolgimento dell’informazione derivante.

Il cambio di una data, di un saluto in una firma, di un punto esclamativo in un punto interrogativo, stravolgono la portata rappresentativa e il patrimonio informativo di un messaggio, di una email, di un documento, di una tabella di calcolo, finanche di una foto digitale e di un file audio.

Ove tale informazione venga usata in un contesto comunicativo ludico, familiare, aziendale, può determinare un difetto di comunicazione più o meno rilevante.

Ove la medesima informazione sia invece rilevante o addirittura determinante per la ricostruzione in un contesto giudiziario del quadro probatorio, spesso basato su elementi indiziari, tale cambio può provocare un completo travisamento dei fatti e la pronuncia di provvedimenti errati per una parte, ingiusti se favorevoli ad un colpevole o aberranti se sfavorevoli ad un innocente.

Le variazioni sono molto più rilevanti e gravi ove siano più numerose e diffuse tra miliardi di stringhe di dati normalmente registrate su un supporto.

4 Processo penale e prova informatica

4.1 La questione terminologica in tema di prova digitale

Come si è detto, l'Informatica forense studia le norme che riguardano il trattamento dei dati digitali ad uso processuale, e in particolar modo la loro rilevanza a fini probatori in un procedimento.

Una delle questioni terminologiche sulle quali deve preliminarmente farsi chiarezza, attiene proprio alla definizione di termini come prova, mezzo di prova[147], prova informatica che, per quanto frequentemente ricorrenti nell'ambito dell'Informatica forense, sono erroneamente utilizzati come sinonimi.

Tale specificazione si pone come momento indefettibile del consolidamento della base terminologica, soprattutto in considerazione dell'eterogenea formazione e provenienza degli studiosi e pratici della materia.

Da un punto di vista giuridico, e secondo la migliore classificazione[148], il termine "prova" può avere almeno quattro diversi significati: fonte di prova, mezzo di prova, elemento di prova e risultato probatorio.

Per "fonte di prova" si intende "tutto ciò che è idoneo a fornire risultati apprezzabili per la decisione del giudice, come ad es. una persona, un documento, una cosa", e talvolta la fonte di prova è all'origine dell'elemento di prova (v. ad es. art. 65, c.1[149]).

---

[147] Motivi di economia espositiva impediscono di ripercorrere le tematiche legate alla prova, per cui si rimanda all'ampia bibliografia in tema di prova civile e penale, per la quale si rinvia a CARNELUTTI F., Principi del processo penale, Morano, Napoli, 1960 e La prova civile (1915), Giuffrè, Milano; FERRAJOLI L., Diritto e ragione. Teoria del garantismo penale, Laterza, Bari, 1989; SIRACUSANO D., Prova, in Enc. Giur. Treccani, XXIV, Roma, 1991; TARUFFO M., La prova dei fatti giuridici, Giuffrè, Milano, 1992; UBERTIS G., La prova penale. Profili giuridici ed epistemologici. Utet, Torino, 1995, TONINI P., La prova penale, V ed., Cedam, Padova, 2000, FERRUA P., GRIFANTINI F. M., ILLUMINATI G., ORLANDI R., La prova nel dibattimento penale, Giappichelli, Torino, 2005; APRILE E., SILVESTRI P., La formazione della prova penale, Giuffrè, Milano, 2002; DE FRANCESCO A., Il principio del contraddittorio nella formazione della prova nella costituzione italiana, Giuffrè, Milano, 2005; MOSCARINI P., Principi delle prove penali, Giappichelli, Torino, 2014; TONINI P., CONTI C., Il diritto delle prove penali, II ed., Giuffrè, Milano, 2014; sulle prove atipiche, v. LARONGA A., Le prove atipiche nel processo penale, Cedam, Padova, 2002; per l'analisi delle patologie in ambito probatorio, v. ANGELETTI R., Le invalidità delle prove e dei mezzi di prova, Giappichelli, Torino, 2005.

[148] Si riprende l'articolazione di TONINI, P., La prova penale, Padova, Cedam, 2000, pp. 32 e ss.

[149] Art. 65, c. 1, c.p.p.: *"Interrogatorio nel merito. L'autorità giudiziaria contesta alla persona sottoposta alle indagini in forma chiara e precisa il fatto che le è attribuito, le rende noti gli elementi di prova esistenti contro di lei e, se non può derivarne pregiudizio per le indagini, gliene comunica le fonti.(...)"*.

Per "mezzo di prova", si intende invece lo strumento con il quale si acquisisce al processo un elemento di prova che serve per la decisione, come ad es. una testimonianza[150].

Per "elemento di prova", si intende il dato grezzo che si ricava dalla fonte di prova, quando ancora non è stato valutato dal giudice (v. ad es. art. 68, disp. att. [151]).

Per "risultato probatorio" si intende quanto ottiene il Giudice all'esito della valutazione della credibilità della fonte e dell'attendibilità dell'elemento ottenuto (art. 192. c. 1, [152]).

La prova tout court può essere quindi definita come il processo logico che dal fatto noto ricava l'esistenza del fatto da provare.

Ciò che deve essere oggetto di prova è indicato dall'art. 187[153], e sono: i fatti che si riferiscono all'imputazione, alla punibilità e alla determinazione

---

[150] Art. 194 c.p.p.: "*Oggetto e limiti della testimonianza. 1. Il testimone è esaminato sui fatti che costituiscono oggetto di prova[187]. Non può deporre sulla moralità dell'imputato, salvo che si tratti di fatti specifici, idonei a qualificarne la personalità in relazione al reato [c.p. 133] e alla pericolosità sociale [c.p. 203].*

2. L'esame può estendersi anche ai rapporti di parentela e di interesse che intercorrono tra il testimone e le parti o altri testimoni nonché alle circostanze il cui accertamento è necessario per valutarne la credibilità [236]. La deposizione sui fatti che servono a definire la personalità della persona offesa dal reato è ammessa solo quando il fatto dell'imputato deve essere valutato in relazione al comportamento di quella persona.

3. Il testimone è esaminato su fatti determinati [499]. Non può deporre sulle voci correnti nel pubblico né esprimere apprezzamenti personali salvo che sia impossibile scinderli dalla deposizione sui fatti".

[151] L'art. 38 disp. att., così recitava: "*Facoltà dei difensori per l'esercizio del diritto alla prova. 1. Al fine di esercitare il diritto alla prova previsto dall'articolo 190 del codice, i difensori, anche a mezzo di sostituti e di consulenti tecnici, hanno facoltà di svolgere investigazioni per ricercare e individuare elementi di prova a favore del proprio assistito e di conferire con le persone che possano dare informazioni.*

2. L'attività prevista dal comma 1 può essere svolta, su incarico del difensore, da investigatori privati autorizzati.

2-bis. Il difensore della persona sottoposta alle indagini o della persona offesa può presentare direttamente al giudice elementi che egli reputa rilevanti ai fini della decisione da adottare.

2-ter. La documentazione presentata al giudice è inserita nel fascicolo relativo agli atti di indagine in originale o in copia, se la persona sottoposta alle indagini ne richiede la restituzione" .; l'articolo è stato abrogato dalla L. 7 dicembre 2000, n. 397.

[152] Art. 192, c. 1, c.p.p.: "*Valutazione della prova. 1. Il giudice valuta la prova dando conto nella motivazione dei risultati acquisiti e dei criteri adottati [546 1 lett. E].*

2. L'esistenza di un fatto non può essere desunta da indizi a meno che questi siano gravi, precisi e concordanti [2729].

3. Le dichiarazioni rese dal coimputato del medesimo reato o da persona imputata in un procedimento connessoa norma dell'articolo 12 sono valutate unitamente agli altri elementi di prova che ne confermano l'attendibilità [210, 238bis, 500 4].

4. La disposizione del comma 3 si applica anche alle dichiarazioni rese da persona imputata di un reato collegato a quello per cui si procede, nel caso previsto dall'articolo 371 comma 2 lettera b)".

[153] Art. 187 c.p.p. "*1. Sono oggetto di prova i fatti che si riferiscono all'imputazione, alla punibilità e alla determinazione della pena o della misura di sicurezza .*

2. Sono altresì oggetto di prova i fatti dai quali dipende l'applicazione di norme processuali.

della pena o della misura di sicurezza, ma anche, "*i fatti dai quali dipende l'applicazione di norme processuali"*. Proprio quest'ultima norma ha particolare rilevanza ai fini dell'Informatica forense in quanto proprio sui dati digitali e sui fatti informatici in senso lato si basa la prova dei fatti dai quali dipende l'applicazione delle norme processuali.

Infine, se vi è costituzione di parte civile, devono essere oggetto di prova anche i fatti inerenti alla responsabilità civile derivante dal reato[154]. Per quanto tale eventualità diventi effettiva solo con l'atto di costituzione di parte civile, atto che ai sensi dell'art. 79 si colloca di norma per l'udienza preliminare o prima del compimento degli adempimenti di cui all'art. 484, c. 1, e quindi molto tempo dopo l'avvio delle indagini, la semplice prospettiva che vi possa essere una o più parti civili, fa sì che le attività di indagine debbano tener conto della possibilità – o dell'alta probabilità - che i risultati delle indagini ad oggetto informatico possano servire anche a provare i fatti inerenti la responsabilità civile.

Inoltre, si distingue tra prova e "indizio", ove la prova, più propriamente detta "prova rappresentativa", si riferisce al procedimento logico attraverso il quale dal fatto noto si deduce per rappresentazione l'esistenza del fatto da provare[155]. È il caso in cui ad esempio un testimone rappresenta direttamente un certo accadimento.

Con il termine "indizio", più propriamente detta "prova logica", ci si riferisce al procedimento in virtù del quale, muovendo da un fatto provato, appunto la circostanza costituente indizio, attraverso massime di esperienza o leggi scientifiche si ricava il fatto storico da provare[156]. Gli indizi sono quindi prove che devono essere verificate, e per esserlo devono soddisfare l'art. 192, c. 2, in tema di valutazione della prova, per cui "*2. L'esistenza di un fatto non può essere desunta da indizi a meno che questi siano gravi, precisi e concordanti",* ove per gravi si intendono gli indizi consistenti che resistono alle obiezioni e che quindi sono attendibili e convincenti; precisi sono gli indizi non generici, e concordanti sono quelli che non contrastano con altri indizi o con altri dati certi[157] e che convergono tutti verso la medesima conclusione.[158]

3. Se vi è costituzione di parte civile [76], sono inoltre oggetto di prova i fatti inerenti alla responsabilità civile derivante dal reato [c.p. 185]".

[154] Per quanto l'eventualità diventi effettiva solo con l'atto di costituzione di parte civile, atto che ai sensi dell'art. 79 si colloca di norma per l'udienza preliminare o prima del compimento degli adempimenti di cui all'art. 484 comma 1 c.p.p.., e quindi molto tempo dopo l'avvio delle indagini, la semplice prospettiva che vi sia una o più persone offese dal reato e che in seguito possa esservi una o più parti civili, fa sì che le attività di indagine debbano tener conto della possibilità – o dell'alta probabilità - che i risultati delle indagini ad oggetto informatico possano servire anche anche ad altre parti diverse da quelle necessarie.

[155] Così, TONINI P., (2000), op.cit., p. 32.

[156] *Ibidem*, p. 33.

[157] Cfr. Cass. sez. I, 30 gennaio 1991, Bizantino, in Cass. pen. 1992, p. 2795.

[158] Cfr. TONINI P., (2000), op.cit., p. 40.

I "mezzi di prova" sono quegli strumenti processuali che permettono di acquisire un elemento di prova; il codice ne prevede sette che costituiscono i mezzi di prova tipici[159] di cui la legge regolamenta le modalità di assunzione (artt. 194-243)[160]. Tuttavia, il codice ammette anche mezzi di prova atipici, previsti dall'art. 189 il quale, in tema di "*Prove non disciplinate dalla legge"* prevede che "*1. Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti [187] e non pregiudica la libertà morale della persona [642, 188]. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova"*. Si tratta quindi di strumenti di acquisizione di un elemento di prova non regolamentato dalla legge, ma consentiti se idonei ad assicurare l'accertamento del fatto e non pregiudicano la libertà morale dell'imputato. Sono i casi in cui il progresso tecnologico mette a disposizione nuovi strumenti che consentano di accertare i fatti[161]. In tal caso, ai sensi della prefata norma, Il giudice provvede all'ammissione del mezzo di prova atipico non secondo uno schema legale, che per definizione non è previsto dalla legge, bensì dopo aver sentito le parti le quali sono chiamate ad un contraddittorio su tale punto.

Per "mezzi di ricerca della prova", infine si intende l'attività strumentale per consentire di acquisire al procedimento un mezzo di prova preesistente[162].

Pertanto, dal punto di vista qualificatorio, il nostro ordinamento processual penalistico, la dottrina e la giurisprudenza definiscono i fenomeni suddetti con una precisione molto maggiore rispetto a quella che è dato verificare tra gli operatori i quali, a causa delle assonanze, sono più spesso soggetti ad incertezze.

Sta di fatto che gli indizi e i mezzi di prova, che nella fase anteriore al vaglio valutativo del Giudice sono solo tali, assumono il termine di "prova" tout court solo all'esito dell'iter di ricerca, ammissione, assunzione e valutazione del mezzo di prova e quindi posteriormente al vaglio valutativo del Giudice, successivamente al completamento del sillogismo decisionale compiuto dal Giudice e trasfuso nel suo provvedimento, sentenza, ordinanza, decreto che siano[163].

In secondo luogo, il nostro codice non conosceva una (sotto)categoria definibile come mezzo di prova informatica o prova digitale o prova

[159] Sono mezzi di prova la testimonianza, l'esame delle parti, il confronto, la ricognizione, l'esperimento giudiziale, la perizia, i documenti.
[160] *Ibidem*, p. 91.
[161] Si pensi ad esempio alla scoperta di una nuova procedura idonea a recuperare le tracce di altre sostanze disperse e ritenute non recuperabili.
[162] Sono mezzi di ricerca della prova, l'ispezione, la perquisizione, il sequestro probatorio, le intercettazioni di conversazioni e comunicazioni.
[163] Sul sillogismo giudiziario e sul sillogismo probatorio, v. TONINI P., 2000, pp. 27 e ss.

documentale informatica, categoria isolata dalla dottrina più attenta[164]. Dal 2015, a seguito dell'introduzione dell'art. 234 bis rubricata come "*Documenti e dati informatici*"[165], salvo quanto si dirà oltre a proposito della prova documentale ex art. 234 e della prova documentale informatica ex art. 234 bis, nel nostro ordinamento è possibile ora parlare, anche formalmente, di mezzo di prova documentale informatica.

Il concetto di "prova digitale" è derivato dalla trasposizione del concetto rinvenibile nel sistema di Common Law il quale, prevedendo la categoria giuridica dell'*evidence,* ove questa abbia ad oggetto un insieme di dati digitali, può annoverare anche la sottocategoria della *digital evidence.* Tale espressione, di non recente introduzione, per effetto dell'osmosi giuridica in atto in tema di indagini informatiche si è fatta largo travalicando il sistema originario e approdando nel nostro sistema[166].

Tuttavia, le incertezze del legislatore consentono agevolmente di annoverare un'ampia e variegata serie di "manifestazioni" del dato digitale nell'ambito di un procedimento che non consente di sussumere un concetto onnicomprensivo di prova digitale.

Prova ne sia che il dato digitale può costituire oggetto di prova documentale ex artt. 234, oppure prova documentale acquisibile all'estero ex art. 234 bis, o ancora oggetto di corrispondenza digitale da sequestrare, o risultato dell'intercettazione di flussi informatici e telematici ex art. 266 bis.

Pertanto, ad oggi, l'espressione prova digitale potrebbe rilevare al più come espressione atecnica che semplifica il riferimento alle categorie sussunte.

E tuttavia, poiché potente è la forza suggestiva dei termini, il rischio di trasposizione nel nostro sistema di espressioni che non trovano corrispettivo nelle norme rischia di ammantare della qualifica di prova quello che, nella fase anteriore alla sua valutazione, è solo un elemento, rectius: un mezzo di prova.

4.2 La prova informatica come prova scientifica

Sempre da un punto di vista giuridico, ai fine dell'utilizzo che gli operatori forensi intendono fare dei dati digitali tratti da dispositivi e sistemi informatici e

[164] TONINI P., Documento informatico e giusto processo, in "Diritto penale e processo", 2009, p. 401 e ss. e TONINI P., CONTI C., Il diritto delle prove penali, op.cit.

[165] Articolo inserito dall'art. 2, comma 1 bis del D.L. 18 febbraio 2015 n. 7, convertito con modificazioni nella L. 17 aprile 2016, n. 43, "Integrazione delle misure di prevenzione e contrasto delle attività terroristiche".

[166] Sulla prova informatica, v. PESCI S., L'ingresso nel proceso della prova informatica, Atti dell'Incontro di formazione decentrata C.S.M., Ufficio referente distrettuale formazione magistrati Bologna, su "Criminalità informatica: profili sostanziali e di ricerca e formazione della prova", Bologna, 27.11.2006.

telematici, è innegabile che questi si collochino a pieno titolo nell'ambito della prova scientifica[167].

L'espressione prova scientifica, e quindi anche quella di prova informatica, frequentemente utilizzata con intento classificatorio, e più frequentemente con intento semplificatorio, presenta molti profili di atecnicismo e può risultare se non fuorviante, almeno suggestiva.

Infatti, da un punto di vista di qualificabilità sistematica, il nostro ordinamento processual penalistico conosce i mezzi di prova, gli indizi e i mezzi di ricerca della prova, che assumono valore di prova *tout court* solo all'esito del vaglio valutativo del Giudice.

In secondo luogo, nel nostro ordinamento non si rinviene una (sotto)categoria definibile come mezzo di prova di prova scientifica, e tantomeno informatica (tantomeno in contrapposizione con una non meglio definibile "prova analogica"[168].

Da ultimo, vi è stato chi, nell'ambito della teoria del documento come mezzo di prova, ha correttamente differenziato tra prova documentale analogica e prova documentale digitale, ma al fine di meglio definire le differenze tra rappresentazione e incorporamento.

Inoltre, l'esperienza consente agevolmente di annoverare un'ampia e variegata serie di "manifestazioni" del dato digitale nell'ambito di un procedimento che non consente di sussumere un concetto onnicomprensivo di prova digitale.

Il realtà il contenuto scientifico relativo ai dati informatici attiene alle modalità con le quali essi devono essere trattati al fine di conservare integro il patrimonio informativo utile al procedimento.

A tal proposito rileva tutta la questione del metodo utilizzato nel trattamento dei dati e quindi delle migliori modalità, chiamate anche best practice, protocolli, linee guida, standard che annoverano le migliori tecniche di trattamento dei dati a fini processuali, tema che verrà affrontato nel prosieguo della presente trattazione.

---

[167] Sulla prova scientifica nel processo penale, DOMINIONI O., La prova penale scientifica, Giuffrè, Milano, 2005 ; STELLA F., Il giudice corpuscolariano. La cultura delle prove, Giuffrè, Milano, 2005; AA.VV. Decisione giudiziaria e verità scientifica, Giuffrè, Milano, 2005; CHIAVARIO M. (a cura di), Nuove tecnologie e processo penale, Giappichelli, Torino, 2006 ; PUTIGNANO D. S., L'errore scientifico nel processo penale, Giuffrè, Milano, 2007; DE CATALDO NEUBURGER, L. (a cura di) La prova scientifica nel processo penale, Cedam, Padova, 2007 ; TONINI P. (a cura di) La prova scientifica nel processo penale, Dossier di Diritto e processo penale, Milano, 2008 ; CONTI C. (a cura di), Scienza e processo penale. Nuove frontiere e vecchi pregiudizi, Giuffrè, Milano, 2011; sui rapporti tra scienza e processo, v. JASANOFF S., La scienza davanti ai giudici, Giuffrè, Milano, 2001.

[168] TONINI P. (2009), Documento informatico e giusto processo, in "Diritto penale e processo", 2009, p. 401 e ss..

4.3 La L. 547/93 sui reati informatici

I reati informatici sono stati introdotti nel nostro ordinamento per la prima volta dalla L. n. 547 del 1993[169].

La prima novella in materia di reati informatici[170], intervenendo mediante interpolazione del codice, accanto alle norme preesistenti previste a protezione dei beni giuridici tradizionali, inseriva una serie di nuove fattispecie per "aggiornare" gli ambiti tradizionali di tutela dalle aggressioni ai beni informatici o mediante strumenti informatici.

Particolare rilevanza avevano le seguenti previsioni:

- l'esercizio arbitrario delle proprie ragioni con violenza sulle cose, veniva integrata dalla previsione della violenza sul programma informatico e sul sistema informatico o telematico (art. 392, c. 2, c.p.);
- in tema di danneggiamento, venivano introdotte le norme sul danneggiamento di sistemi informatici o telematici (art. 635 bis c.p.) e sulla diffusione di programmi diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.), per quanto questa seconda sia stata inopinatamente accostata alla tutela del domicilio informatico;
- la norma che già puniva l'attentato ad impianti di pubblica utilità (art. 420 c.p.) veniva integrata dalla previsione relativa ai sistemi informatici e telematici;
- la tutela del domicilio veniva ampliata a quella del domicilio informatico, prevedendo reati quali l'accesso abusivo a un sistema informatico o telematico (art. 615 ter c.p.), la detenzione e diffusione abusiva di codici di accesso a sistemi informatici (art. 615 quater c.p.);
- la frode informatica (art. 640 ter c.p.), veniva delineata sul modello della truffa;
- la falsificazione del documento informatico (art. 491 bis c.p.) ampliava i casi di falso documentale;

---

[169] Legge 23 dicembre 1993 n. 547, in G. U. n. 305 del 30 dicembre 1993, Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica.

[170] Le problematiche esegetiche sui reati informatici sono troppo ampie perché in questa sede se ne possa dare anche solo un resoconto sommario. Le notazioni critiche all'impianto superano ampiamente quelle adesive; fra tutti, v. GALDIERI P., Teoria e pratica nell'interpretazione del reato informatico, op.cit.; PICA G., Diritto penale delle tecnologie informatiche, op.cit.; PECORELLA C., Il diritto penale dell'informatica, op.cit.; PICOTTI L., Reati informatici in Enciclopedia giuridica, Aggiornamento VIII, Istituto della Enciclopedia italiana, Roma, 2000, p. 1-33; AMMIRATI D., (a cura di), Internet e la legge penale, Giappichelli, Torino, 2001; SARZANA DI S. IPPOLITO, C., Informatica, Internet e diritto penale, op.cit.; BUFFA F., Informatica, internet e diritto penale, op.cit.; per la disamina successiva alle modifiche introdotte ai reati informatici dalla L. 48/08, v. CUOMO L., RAZZANTE R., La nuova disciplina dei reati informatici, op.cit; AMATO G., DESTITO V. S., DEZZANI G., SANTORIELLO, C., I reati informatici, op.cit.; LUPARIA L., (a cura di), Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest, Giuffrè, Milano, 2009.

- i reati di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.), di installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.), e di falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617 sexies c.p.), al fine di tutelare la corrispondenza e le comunicazioni telematiche;
- l'estensione dell'applicabilità delle norme previste dagli artt. da 617 a 617 sexies c.p. alle trasmissioni a distanza di suoni, immagini o altri dati (623 bis 6 c.p.).

L'unica norma introdotta nel codice di procedura penale è stata quella riguardante l'intercettazione di flussi telematici prevista all'art. 266 bis c.p..

Pertanto, la L. 547/93 non ha inciso sul regime della prova, né ha previsto alcunchè in tema di prova digitale; non vi è luogo in cui se ne parli.

Sotto il profilo sistematico, invece, la L. 547/93 se da un lato ha rappresentato il primo tentativo di adeguamento dell'ordinamento alle nuove esigenze imposte dalla rivoluzione digitale, dall'altro costituisce il primo segnale della scarsa comprensione dei nuovi fenomeni digitali da parte del nostro legislatore, comprovata dall'inclinazione ad adattare gli schemi normativi preesistenti a realtà del tutto nuove e solo apparentemente simili.

Tale inclinazione si è poi confermata nella successiva legge che ha modificato le norme procedurali.

4.4 La L. 48/08 e le nuove procedure ad oggetto informatico

Con la L. 18 marzo 2008, n. 48, avente ad oggetto la "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"[171], il legislatore ha confermato la propensione, già manifestatasi con la L. 547/93, ad impiantare nelle strutture preesistenti le nuove norme che dovrebbero dovuto dare risposta alle esigenze di ammodernamento normativo.

Questa volta, l'intervento normativo ha riguardato alcune norme del codice di procedura penale, con l'intento di contrastare il crimine informatico e telematico.

Al di là delle intenzioni, alla legge 48/08 va riconosciuto il pregio di aver acceso una luce sul problema del trattamento dei dati digitali a fini processuali e di aver sensibilizzato gli operatori forensi sulla necessità di adeguamento delle

[171] L. 18 marzo 2008, n. 48, "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" in G. U. n. 80 del 4 aprile 2008, S.O. n. 79.

restanti norme alle esigenze imposte dal progresso tecnologico in campo informatico.

Tuttavia, il legislatore non ha saputo evitare che l'operazione di *restyling* si rivelasse parziale e inadeguata, soprattutto rispetto all'area dei principi e delle garanzie difensive, dando luogo a problematiche di preoccupante rilevanza nei termini che si diranno in seguito.

Un altro obiettivo dichiarato era quello di attuare il principio di affidabilità della prova digitale, quale portato dell'integrità e incontestabile autenticità, come auspicato dalla Raccomandazione R (95) del 13 settembre 2001 del Comitato dei Ministri del Consiglio d'Europa[172].

E invece, oltre all'adeguamento di alcune norme di diritto penale sostanziale già introdotte dalla L. 547/93[173], il legislatore italiano si è limitato a modificare le norme processuali riguardanti la competenza, gli atti ad iniziativa di polizia giudiziaria e i mezzi di ricerca della prova, interpolando il codice e le norme preesistenti con aggiunte e incisi, ma senza alcun intervento sui mezzi di prova a contenuto informatico nella direzione dell'implementazione della *digital evidence*[174].

---

[172] Cfr. Art. 13 della Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology (Adopted by the Committee of Ministers on 11 September 1995 at the 543 meeting of the Ministers' Deputies) "*4. IV. Electronic Evidence 13. The common need to collect, preserve, and present electronic evidence in ways that best ensure and reflect their integrity and irrefutable authenticity, both for the purposes of domestic prosecution and international co-operation, should be recognized. Therefore, procedures and technical methods for handling electronic evidence should be further developed, and particularly in such a way as to ensure their compatability between states. Criminal procedural law provisions on evidence relating to tradition documents should similarly apply to data stored in a computer system (...)*".

[173] Va ricordato che gli articoli del codice penale interessati dalla L. 48/08 sono stati i seguenti: art. 491 bis c.p., (Documenti informatici), art. 495 bis c.p. (Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri), art. 615 quinquies c.p. (Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico), art. 640 quinquies c.p. (Frode informatica del soggetto che presta servizi di certificazione di firma elettronica), art. 635 bis c.p. (Danneggiamento di sistemi informatici o telematici di pubblica utilità), art. 635 ter c.p. (Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità), art. 635 quater c.p. (Danneggiamento di sistemi informatici o telematici), art. 635 quinqies c.p. (Danneggiamento di sistemi informatici o telematici di pubblica utilità), e con la simultanea abrogazione dei commi 2 e 3 dell'art. 420 c.p. (Attentato a impianti di pubblica utilità); va altresì ricordata l'introduzione dell'art. 24 bis (Delitti informatici e trattamento illecito di dati) del D. Lgs. 231/01 (c.d. Reponsabilità degli enti); su quest'ultimo tema, v. CORASANITI G., CORRIAS LUCENTE G., (a cura di), Cybercrime, responsabilità degli utenti, prova digitale, Cedam, Padova, 2009.

[174] V. PICOTTI L., La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto sostanziale, in Diritto penale e processo, n. 6, 2008, p. 700 e ss. ; LUPARIA, L., La ratifica della Convenzione Cybercrime del Consiglio d'Europa. I profili processuali, in Diritto penale e processo, n. 6, 2008, pp. 717 e ss. ; CAJANI F., La Convenzione di Budapest nell'insostenibile salto all'indietro del legislatore italiano: quello che le norme non dicono..... in "Ciberspazio e Diritto", 2010, Vol. 11, n. 1, pp. 185-210 ; PERRI P., voce Computer forensics (indagini informatiche), in Digesto delle discipline penalistiche, UTET, Torino, 2011, pp. 95-109; NERI G., Criminologia e reati informatici. Profili di diritto penale dell'economia, op.cit.

Inoltre, secondo l'art. 14 della Convenzione, ogni Parte aderente è tenuta ad adottare le misure legislative e di altro tipo necessarie a stabilire le procedure previste per le investigazioni e nei procedimenti penali imponendo il regime previsto per la digital evidence ai reati stabiliti nella Convenzione, ai reati commessi per mezzo di un sistema informatico e alla raccolta della prova in formato elettronico di un reato[175].

In definitiva, la Convenzione di Budapest ha imposto ai Paesi aderenti l'adozione delle tecniche per il trattamento dei dati oggetto di investigazione e procedimento senza imporre, come si dirà meglio in seguito, specifiche tecniche, purché fosse raggiunto il fine ultimo costituito dalla corretta gestione e del dato.

Quanto invece all'oggetto finale di tutto il provvedimento, vale a dire i dati informatici, la Convenzione ne dà una definizione sin dall'art. 1 costituente il fondamento di tutte le altre previsioni metodologiche del Consiglio d'Europa:"[176] "(...) *b (l'espressione) "dati informatici" indica ogni*

---

[175] Article 14 – *Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.*
2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
b other criminal offences committed by means of a computer system; and
c the collection of evidence in electronic form of a criminal offence.

[176] Ritenendo tale definizione centrale per la corretta comprensione della ratio dei diversi istituti previsti dalla Convenzione, per la migliore esegesi delle norme della L. 48/08 e per la corretta impostazione della metodologia ivi prevista, si riportano le Definizioni in entrambe le versioni ufficiali della Convenzione, al fine di verificare l'attendibilità delle vulgate in italiano: "*Chapter I – Use of terms Article 1 – Definitions For the purposes of this Convention:*
a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;
b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;
c "service provider" means:
i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;
d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."
Chapitre I – Terminologie Article 1 – Définitions - Aux fins de la présente Convention,
a l'expression «système informatique» désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données;
b l'expression «données informatiques» désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction;
c l'expression «fournisseur de services» désigne:

rappresentazione di fatti, informazioni o concetti in una forma adatta all'elaborazione informatica, compreso un programma adatto a far sì che un sistema informatico esegua una funzione;".

Orbene, tale definizione, unitamente alle altre registrate dall'art. 1, consentono di rassegnare alcune considerazioni di rilevante importanza:

1) l'uso del termine "dati informatici" al plurale indica la propensione della Convenzione a considerare rilevante l'insieme dei dati digitalizzati e aggregati, considerando quindi utili le informazioni derivanti dall'elaborazione di dati in tale formato;
2) i dati informatici rilevano in sé in quanto mezzo di "rappresentazione", senza la necessità o interferenza di ulteriori ammennicoli o superfetazioni;
3) i dati informatici fondano ogni ulteriore considerazione giuridica e tecnica, espressa o sottesa dalle norme della Convenzione da recepire e attuare negli ordinamenti;
4) i dati informatici costituiscono il baricentro dell'attività di modellazione delle fattispecie di reati, degli strumenti di indagine e investigazione, nonché degli strumenti di collaborazione internazionale e di ogni altra previsione della Convenzione.

Nonostante tutto ciò, lacuna tra le più gravi, il legislatore italiano ha omesso di riportare nel nostro ordinamento la definizione di dato o dati informatici, men che meno ha tipizzato il concetto, negandogli altresì il rango di autonomo bene giuridico meritevole di tutela.

Pertanto, la normativa da implementare nei sistemi nazionali si è limitata a prevedere le procedure cui deve sottostare il trattamento dei dati informatici oggetto di investigazione e indagine, nonché le modalità tecniche per la conservazione dei dati integri e affidabili, a tutela del patrimonio rappresentativo e quindi informativo che ne può derivare.

Da tali considerazioni discende che i dati di cui una parte del procedimento, polizia giudiziaria, pubblico ministero, o altra parte, intende avvalersi, hanno valenza probatoria solo se costituiscono una fedele "*rappresentazione di fatti, informazioni o concetti in una forma adatta all'elaborazione informatica*", e non se si risolvono in una rappresentazione parziale, erronea, fuorviante, o peggio travisante o, addirittura, alterata della realtà.

i toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et
ii toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.
d «données relatives au trafic» désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

Tale impostazione è l'unica che concilia le esigenze di accertamento e repressione dei reati con i presupposti tecnici che, se rispettati, possono attribuire affidabilità ai dati informatici utilizzati, nel rispetto dei diritti fondamentali delle parti.

La realizzazione di tale obiettivo è delimitata da due stipiti: il primo è costituito dalle norme processuali che disciplinano l'attività di investigazione e di indagine da applicarsi alla luce dei diritti riconosciuti dalle Convenzioni internazionali e dalla Costituzione[177]; l'altro stipite è invece costituito dalle norme tecniche basate su principi scientifici propri dell'Informatica e finalisticamente organizzate per garantire ai dati informatici l'integrità della capacità rappresentativa dei fatti, informazioni e concetti a fini probatori.

L'architrave è costituito dal metodo posto dall'Informatica forense che collega e stabilizza i due ambiti.

Le norme procedurali e di collaborazione previste dalla Convenzione, pur non imponendo o indicando specifici strumenti tecnici e scientifici che attuino le precauzioni imposte nel trattamento dei dati ad uso processuale, sottendono e compulsano la loro adozione. Si veda, ad esempio, l'art. 19 della Convenzione avente ad oggetto la ricerca e il sequestro di dati archiviati in un sistema informatico, poi trasfuso nelle norme relative all'ispezione, perquisizione e sequestro di dati informatici previsti dal codice di procedura penale:"*(...) Article 19 – Search and seizure of stored computer data*

---

[177] Cfr. i punti fermi posti dal Preambolo alla Convenzione di Budapest: "*(...) Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;*
Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; (...)" trasfusi nell'art. 15 della Convenzione:"*(...) Article 15 - Conditions and safeguards*
1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored in its territory.

2 Each Party shall adopt such ***legislative and other measures*** *as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.*

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. (...)"

Ebbene, le finalità poste dal 3° comma, lett. a), b), c), d), oltre ad essere oggetto di previsione normativa (*legislative ...measures*) possono essere attuate con "altre misure" (*other measures*) che non possono essere altro che misure tecniche.

Tali misure, essendo necessariamente informatiche, dovranno garantire le finalità poste dalle norme legislative, con le tecniche proprie della scienza informatica, e quindi con misure che poggiano la loro valenza tecnica sui principi scientifici dell'informatica.

Al contrario, ove quelle finalità poste dalle misure legislative fossero perseguite con strumenti non scientifici, le stesse finalità potrebbe non essere realizzate.

A tal proposito, il legislatore italiano non ha tipizzato specifiche tecniche di trattamento dei dati a fini processuali, scelta che, alla luce del continuo progresso tecnologico, appare condivisibile.

Pertanto, l'Informatica forense, tenuto conto delle finalità perseguite dal diritto, rivolge l'attenzione alla scienza informatica per acquisirne il metodo che le realizza su base scientifica per non deprimere la fedeltà rappresentativa e quindi l'efficacia probatoria dei dati informatici.

4.5 Gli atti a iniziativa della polizia giudiziaria e i mezzi di prova ad oggetto informatico

La L. 48/08, nel ratificare e dare esecuzione alla Convenzione del Consiglio d'Europa sulla criminalità informatica, tra le altre cose[178], ha integrato diverse norme del codice di rito penale con le previsioni relative al trattamento dei dati informatici a fini processuali[179].

In particolare, gli interventi hanno interessato sia le norme relative agli atti a iniziativa della polizia giudiziaria, sia le norme relative alle indagini e in particolare i mezzi di ricerca della prova, in genere estendendo la portata delle relative norme ai dati, programmi, informazioni, nonchè ai sistemi informatici e telematici.

Nell'ambito degli atti a iniziativa della polizia giudiziaria previsti dall'art. 347 e ss., sono state integrate le norme riguardanti le perquisizioni (art. 352, c. 1-bis), l'acquisizioni di plichi o di corrispondenza (art. 353, c. 2 e 3), gli accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro (art. 354, c. 2), nonché l'articolo 132 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196

Nell'ambito delle indagini, invece, sono state integrate le norme riguardanti i casi e le forme delle ispezioni (art. 244, c. 2), i casi e forme delle perquisizioni (art. 247, c. 1-bis), la richiesta di consegna (art. 248, c. 2), il sequestro di corrispondenza (art. 254) il sequestro di dati informatici presso fornitori di

[178] Va ricordata sin d'ora, in quanto rilevante ai fini della presente trattazione, la modifica apportata dalla L. 48/08 all'art. 491 bis. "*(Documenti informatici). Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, avente efficacia probatoria si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private.", attuata* mediante soppressione della seguente parte dal testo precedentemente introdotto dalla L. 547/93:"*A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.*".

[179] V. LUPARIA L., La ratifica della Convenzione Cybercrime del Consiglio d'Europa. I profili processuali, in Diritto penale e processo, n. 6, 2008, pp. 717 e ss.; CORASANITI G., CORRIAS LUCENTE G., (a cura di), Cybercrime, responsabilità degli utenti, prova digitale, op.cit.; PERRI P., voce Computer forensics (indagini informatiche), op.cit.; ATERNO S., CAJANI F., COSTABILE G., MATTIUCCI M., MAZZARACO G., (a cura di), Computer forensics e indagini digitali, op.cit.; VACIAGO G., Digital Evidence, Giappichelli, Torino, 2012.

servizi informatici, telematici e di telecomunicazioni (art. 254-bis), il dovere di esibizione e segreti (art. 256), la custodia delle cose sequestrate (art. 259, c. 2) e l'apposizione dei sigilli alle cose sequestrate (art. 260, c. 1 e 2).

Inoltre, è stata modificata la norma sulla competenza del pubblico ministero (art. 51)[180] e al fine di colmare il difetto di coordinamento con la competenza del giudicante, solo con ulteriori provvedimenti normativi è stata modificata la norma sulla competenza del giudice per le indagini preliminari[181].

---

[180] V. art. 51. "*(Uffici del pubblico ministero - Attribuzioni del procuratore della Repubblica distrettuale) (1).*
1. Le funzioni di pubblico ministero sono esercitate:
a) nelle indagini preliminari e nei procedimenti di primo grado dai magistrati della procura della Repubblica presso il tribunale [o presso la pretura] (2) (550) (3);
b) nei giudizi di impugnazione dai magistrati della procura generale presso la corte di appello o presso la Corte di cassazione.
2. Nei casi di avocazione (372, 412, 413), le funzioni previste dal comma 1 lett. a) sono esercitate dai magistrati della procura generale presso la corte di appello. Nei casi di avocazione previsti dall'art. 371 bis, sono esercitate dai magistrati della direzione nazionale antimafia (4).
3. Le funzioni previste dal comma 1 sono attribuite all'ufficio del pubblico ministero presso il giudice competente a norma del capo II del titolo I (4 ss.; att. 3).
3 bis. Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli artt. 416, sesto comma, 600, 601, 602, (8) 416 bis e 630 del codice penale, per i delitti commessi avvalendosi delle condizioni previste dal predetto art. 416 bis ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo, nonché per i delitti previsti dall'art. 74 del testo unico approvato con D.P.R. 9 ottobre 1990, n. 309, e dall'articolo 291 quater del testo unico approvato con decreto del Presidente della Repubblica 23 gennaio 1973, n. 43 (6) le funzioni indicate nel comma 1 lett. a) sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente (5).
3 ter. Nei casi previsti dal comma 3-bis, e dai commi 3-quater e 3-quinquies (2) se ne fa richiesta il procuratore distrettuale, il procuratore generale presso la corte di appello può, per giustificati motivi, disporre che le funzioni di pubblico ministero per il dibattimento siano esercitate da un magistrato designato dal procuratore della Repubblica presso il giudice competente (5).
3 quater. Quando si tratta di procedimenti per i delitti consumati o tentati con finalità di terrorismo le funzioni indicate nel comma 1, lettera a), sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente (2).
3-quinquies. Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 600-bis, 600-ter, 600-quater, 600-quater.1, 600-quinquies, 615-ter, 615-quater, 615-quinquies, 617-bis, 617-ter, 617-quater, 617-quinquies, 617-sexies, 635-bis, 635-ter, 635-quater, 640-ter e 640-quinquies del codice penale, le funzioni indicate nel comma 1, lettera a), del presente articolo sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente.".
(1) Articolo così modificato dall'art. 11 della L. 48/08, recante Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalita` informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno
(2) art. così modificato da art. 2 L. 24 luglio 2008 n. 125, di conv. con modif. del D. L. 23 maggio 2008 n. 92 (in G.U. n. 122, 26 maggio 2008, S.G.) – Misure urgenti in materia di sicurezza pubblica (c.d. "Pacchetto sicurezza").

[181] V. art. 328. "*(Giudice per le indagini preliminari). 1. Nei casi previsti dalla legge, sulle richieste del pubblico ministero, delle parti private (60, 61, 74, 83, 89) e della persona offesa dal reato (90), provvede il giudice per le indagini preliminari (22; att. 105; coord. 238; reg. 16).*
1 bis. Quando si tratta di procedimenti per i delitti indicati nell'art. 51 commi 3 bis e 3 quater, le funzioni di giudice per le indagini preliminari sono esercitate, salve specifiche disposizioni di

4.5.1 Gli atti a iniziativa della polizia giudiziaria

Le norme relative agli atti ad iniziativa della polizia giudiziaria previsti dall'art. 347 e ss., sono state integrate come segue:

Quanto alla perquisizione, così recita l'art. 352 "*(Perquisizioni) (1). 1. Nella flagranza del reato (382) o nel caso di evasione (385 c.p.), gli ufficiali di polizia giudiziaria (57) procedono a perquisizione personale o locale (247 ss.; coord. 225) quando hanno fondato motivo di ritenere che sulla persona si trovino occultate cose o tracce pertinenti al reato che possono essere cancellate o disperse ovvero che tali cose o tracce si trovino in un determinato luogo o che ivi si trovi la persona sottoposta alle indagini o l'evaso (103, 356; att. 113; 609 c.p.).*

1-bis. Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi.

2. (...)"

Orbene, molte osservazioni possono essere portate alla forma ed al contenuto di tale norma:

1) deve innanzitutto ricorrere la flagranza di reato o i casi previsti dal c. 1 e 2, sussistendo presupposti e condizioni;

---

legge, da un magistrato del tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente (1) (2).
1 ter. (4) abrogato)
1 quater. Quando si tratta di procedimenti per i delitti indicati nell'articolo 51, comma 3-quinquies, le funzioni di giudice per le indagini preliminari e le funzioni di giudice per l'udienza preliminare sono esercitate, salve specifiche disposizioni di legge, da un magistrato del tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente. (4)".

(1) Comma aggiunto dall'art. 12 del D.L. 20 novembre 1991, n. 367, istitutivo della Direzione Nazionale Antimafia, convertito, con modificazioni, nella L. 20 gennaio 1992, n. 8. Queste disposizioni, ai sensi dell'art. 15 del medesimo decreto, si applicano solo ai procedimenti iniziati successivamente alla data di entrata in vigore dello stesso.

(2) A norma dell'art. 4 bis del D.L. 7 aprile 2000, n. 82, convertito, con modificazioni, nella L. 5 giugno 2000, n. 144, la disposizione prevista da questo comma deve essere interpretata nel senso che quando si tratta di procedimenti per i delitti indicati nell'articolo 51, comma 3 bis, del codice di procedura penale, anche le funzioni di giudice per l'udienza preliminare sono esercitate da un magistrato del tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente.

(3) Questo comma è stato aggiunto dall'art. 10 bis del D.L. 18 ottobre 2001, n. 374, convertito, con modificazioni, nella L. 15 dicembre 2001, n. 438.

(4) art. 2 L. 24 luglio 2008 n. 125, di conv. con modif. del D. L. 23 maggio 2008 n. 92 (in G.U. n. 122, 26 maggio 2008, S.G.) – Misure urgenti in materia di sicurezza pubblica (c.d. "Pacchetto sicurezza").

2) alla perquisizione possono procedere gli ufficiali di polizia giudiziaria, quando hanno fondato motivo di ritenere che ne sussistano i presupposti; pertanto, non possono procedere arbitrariamente ma devono sussistere elementi obiettivi dai quali emerga con sufficiente probabilità, e non la mera possibilità, che si trovino i dati[182];

3) oggetto di perquisizione possono essere i sistemi informatici e telematici, per quanto sia arduo pensare a tali operazioni effettuate per rinvenire dati residenti nei sistemi telematici normalmente dedicati alla trasmissione dinamica dei dati;

4) nell'espressione "dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi" vengono ammassati elementi eterogenei quali i dati, unico termine sufficiente a descrivere l'intera gamma di elementi digitali rinvenibili, le informazioni, che invece derivano dal rapporto di interpretazione soggettiva, i programmi informatici di cui non si comprende la rilevanza, nonché le tracce pertinenti al reato che, in relazione alla dimensione digitale, mostra tutta la sua evanescenza[183];

5) inoltre, devono trovarsi "occultati", e quindi non meramente archiviati, ma nascosti e impediti al libero accesso;

6) "adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione", descrive l'obbligo per il procedente di rispettare il contesto, per cui vanno preventivamente adottate delle precauzioni di natura tecnica finalizzate a preservare l'integrità dei dati e la loro conservazione;

7) procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, per cui possono essere rimossi eventuali strumenti di protezione di natura logica e fisica; ma tale previsione, di per sé legittima al pari dell'abbattimento di ostacoli che si frappongono e ostacolano l'esecuzione di una perquisizione, non può essere traslata al settore dei dispositivi in quanto le attività necessarie a realizzarle, quali ad esempio ricerca di password e attacchi a forza bruta o con tesauri, interverrebbero direttamente sui file, modificando irreversibilmente i metadati. Pertanto, la previsione del superamento delle misure di sicurezza si pone in rapporto antinomico con l'obbligo di adottare preventivamente le precauzioni di natura tecnica finalizzate a preservare l'integrità dei dati e la loro conservazione. L'unico rimedio sarebbe quello di acquisire preventivamente copia bit per bit del dispositivo preservando i dati originari ed operare la perquisizione sulle copie originali ottenute. In merito agli strumenti software da utilizzarsi, al fine di consentire la verificabilità tecnico-scientifica dei trattamenti cui vengono

[182] Cfr. TONINI P., (2003), op.cit., p. 378.
[183] *Ivi*.

sottoposti i dati, è preferibile l'uso di strumenti a codice aperto (*open source)* rispetto agli strumenti software a codice chiuso, a prescindere se si tratti di software proprietari o meno, a pagamento o gratuiti[184].

Passando alla previsione sull'acquisizione di plichi o di corrispondenza, l'art. 353 così recita:"*(Acquisizione di plichi o di corrispondenza). 1. Quando vi è necessità di acquisire plichi sigillati o altrimenti chiusi, l'ufficiale di polizia giudiziaria (57) li trasmette intatti al pubblico ministero per l'eventuale sequestro (253 ss.).*

2. Se ha fondato motivo di ritenere che i plichi contengano notizie utili alla ricerca e all'assicurazione di fonti di prova che potrebbero andare disperse a causa del ritardo, l'ufficiale di polizia giudiziaria informa col mezzo più rapido il pubblico ministero il quale può autorizzarne l'apertura immediata (356) e l'accertamento del contenuto.

3. Se si tratta di lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza, anche se in forma elettronica o se inoltrati per via telematica, per i quali è consentito il sequestro a norma dell'art. 254, gli ufficiali di polizia giudiziaria, in caso di urgenza, ordinano a chi è preposto al servizio postale, telegrafico, telematico o di telecomunicazione di sospendere l'inoltro. Se entro quarantotto ore dall'ordine della polizia giudiziaria il pubblico ministero non dispone il sequestro, gli oggetti di corrispondenza sono inoltrati (357, 2, lett. e).".

Anche per tale norma il legislatore, probabilmente sulla base della consueta quanto semplicistica assonanza terminologica, ha operato una trasposizione dello schema classico alla nuova realtà della posta elettronica, ottenendo un lettera a tratti paradossale.

Nel regolare il potere di acquisizione di plichi e corrispondenza, il comma 3 è così scandito:

1) si prevede che oggetto dell'acquisizione possano essere lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza, anche se in forma elettronica o se inoltrati per via telematica, ove è veramente difficile ipotizzare oggetti di corrispondenza materiali ma in formato elettronico o inoltrati per via telematica, mentre il legislatore avrebbe potuto definire il tutto mediante la categoria elementare ma onnicomprensiva dei "dati della corrispondenza informatica e telematica"; l'effetto caducatorio della lettera può essere evitato solo dopo un'esegesi adattativa della norma alla fattispecie concreta;

2) l'inciso "per i quali è consentito il sequestro a norma dell'art. 254", riprende casi e condizione previsti in punto di mezzi di ricerca della prova;

3) gli ufficiali di polizia giudiziaria possono procedere in caso di urgenza, per cui nel caso in cui non ricorra il requisito dell'urgenza, il diritto

[184] Sul punto, v. HUEBNER E, ZANERO S., Open Source Software for Digital Forensics, Springer, New York, 2010.

costituzionalmente garantito al segreto della corrispondenza non può essere compresso;

4) se ordinano a chi è preposto al servizio postale, telegrafico, telematico o di telecomunicazione di sospendere l'inoltro, l'ordine deve essere formale e motivato;

5) se entro quarantotto ore dall'ordine della polizia giudiziaria il pubblico ministero non dispone il sequestro, gli oggetti di corrispondenza sono inoltrati, procedura che sembra presupporre l'offerta degli oggetti in esame al pubblico ministero, il che ripropone il tema della copia forense e delle modalità e tecniche con le quali attuarle, rispettando l'integrità e la conservazione dei dati.

Infine, va esaminata la norma in virtù della quale la polizia giudiziaria può operare accertamenti urgenti sui luoghi, sulle cose e sulle persone, prevista dall'art. 354 *"Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro - Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato [253 1] siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero (1).*

2. Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità. Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti [att. 113].

3. Se ricorrono i presupposti previsti dal comma 2, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sulle persone diversi dalla ispezione personale [245]."

Orbene, per questo articolo l'intervento del legislatore è consistito nell'innestare nel comma 2 l'inciso relativo agli elementi informatici in una previsione riguardante la realtà non digitale, e per i quali possono essere mossi rilievi di forma e contenuto:

1) in relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, restano gli oggetti dell'attività disciplinata, in merito ai quali valgono le considerazioni già effettuate.

2) quanto agli ufficiali della polizia giudiziaria, questi devono adottare, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso, per cui è

imposta un'attività proattiva in vista della tutela degli oggetti che o devono adottare essi stessi, o devono prescrivere di adottare, con tutte le problematiche di adeguatezza professionale dei prescritti e delle responsabilità conseguenti, proprie dei prescritti, ma anche in eligendo da parte degli ufficiali di polizia giudiziaria;

3) provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità, in ogni caso devono assicurare il fine della duplicazione degli oggetti con le procedure che a breve verranno analizzate.

Infine, è stato integrato l'articolo 132 del codice in materia di protezione dei dati personali, di cui al D. Lgs. 30 giugno 2003, n. 196[185], che nel testo risultante dalle successive modifiche, allo stato prescrive quanto segue:"*Art. 132. Conservazione di dati di traffico per altre finalità (1)(12)*

1. Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico, sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione. (2)

1-bis. I dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al

[185] Il testo in commento è quello risultante dalle modifiche intervenute successivamente a quello introdotto dalla L. 48/08, che invece era il seguente: "*(...) 4-ter. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonche´ gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalita` indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive di cui al citato articolo 226 del decreto legislativo n. 271 del 1989, ovvero per finalita` di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, puo` prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi.*
4-quater. Il fornitore o l'operatore di servizi informatici o telematici cui e` rivolto l'ordine previsto dal comma 4-ter deve ottemperarvi senza ritardo, fornendo immediatamente all'autorita` richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici e` tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attivita` conseguentemente svolte per il periodo indicato dall'autorita`. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca un piu` grave reato, le disposizioni dell'articolo 326 del codice penale.
4-quinquies. I provvedimenti adottati ai sensi del comma 4-ter sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia ».

pubblico oppure di una rete pubblica di comunicazione, sono conservati per trenta giorni. (3)

2. [abrogato] (4)

3. Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto motivato del pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391-quater del codice di procedura penale, ferme restando le condizioni di cui all'articolo 8, comma 2, lettera f), per il traffico entrante. (5)

4. [abrogato] (6)

4-bis. [abrogato] (7)

4-ter. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi. (8)

4-quater. Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-ter deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'articolo 326 del codice penale. (8)

4-quinquies. I provvedimenti adottati ai sensi del comma 4-ter sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale,

se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia. (8)

5. Il trattamento dei dati per le finalità di cui al comma 1 è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'articolo 17, volti a garantire che i dati conservati possiedano i medesimi requisiti di qualità, sicurezza e protezione dei dati in rete, nonché a: (9)

a) prevedere in ogni caso specifici sistemi di autenticazione informatica e di autorizzazione degli incaricati del trattamento di cui all'allegato B);

b) [soppressa] (10)

c) [soppressa] (10)

d) indicare le modalità tecniche per la periodica distruzione dei dati, decorsi i termini di cui al comma 1. (11)"[186].

---

[186] 1) Articolo così modificato, inizialmente, dal decreto-legge 24 dicembre 2003, n. 354, convertito con modificazioni dalla legge di conversione 26 febbraio 2004, n. 45, recante interventi per l'amministrazione della giustizia; poi dal decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge di conversione 31 luglio 2005, n. 155, recante misure urgenti per il contrasto del terrorismo internazionale; successivamente, dalla legge 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; e, da ultimo, dal decreto legislativo 30 maggio 2008, n. 109, di attuazione della direttiva 2006/24/Ce riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/Ce.
Al fine di delineare con completezza il quadro normativo vigente in materia, si riportano gli articoli 6, comma 1, e 7 del decreto-legge del 27 luglio 2005, n. 144 "Misure urgenti per il contrasto del terrorismo internazionale", come modificato dal decreto-legge del 31 dicembre 2007, n. 248, convertito, con modificazioni, dalla legge di conversione n. 31 del 27 febbraio 2008: "*6. Nuove norme sui dati del traffico telefonico e telematico*

1. A decorrere dalla data di entrata in vigore del presente decreto e fino alla data di entrata in vigore del provvedimento legislativo di attuazione della direttiva 2006/24/Ce del Parlamento europeo e del Consiglio, del 15 marzo 2006, e comunque non oltre il 31 dicembre 2008, è sospesa l'applicazione delle disposizioni di legge, di regolamento o dell'autorità amministrativa che prescrivono o consentono la cancellazione dei dati del traffico telefonico o telematico, anche se non soggetti a fatturazione, e gli stessi, esclusi comunque i contenuti delle comunicazioni e limitatamente alle informazioni che consentono la tracciabilità degli accessi, nonché, qualora disponibili, dei servizi, debbono essere conservati fino alla data di entrata in vigore del provvedimento legislativo di attuazione della direttiva 2006/24/Ce del Parlamento europeo e del Consiglio, del 15 marzo 2006, e comunque non oltre il 31 dicembre 2008, dai fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico, fatte salve le disposizioni vigenti che prevedono un periodo di conservazione ulteriore. I dati del traffico conservati oltre i limiti previsti dall'articolo 132 del decreto legislativo 30 giugno 2003, n. 196, possono essere utilizzati esclusivamente per le finalità del presente decreto, salvo l'esercizio dell'azione penale per i reati comunque perseguibili.".

"7. Integrazione della disciplina amministrativa degli esercizi pubblici di telefonia e Internet

1. A decorrere dal quindicesimo giorno successivo alla data di entrata in vigore della legge di conversione del presente decreto e fino al 31 dicembre 2008, chiunque intende aprire un pubblico esercizio o un circolo privato di qualsiasi specie, nel quale sono posti a disposizione del pubblico, dei clienti o dei soci apparecchi terminali utilizzabili per le comunicazioni anche telematiche, deve chiederne la licenza al questore. La licenza non è richiesta nel caso di sola installazione di telefoni pubblici a pagamento, abilitati esclusivamente alla telefonia vocale.

La norma prevede l'obbligo a carico del fornitore:

1) di conservare i dati relativi al traffico telefonico per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità,
2) di conservare i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, per dodici mesi dalla data della comunicazione, sempre per le medesime finalità di accertamento e repressione dei reati, mentre.
3) di conservare per trenta giorni i dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione.

2. Per coloro che già esercitano le attività di cui al comma 1, la licenza deve essere richiesta entro sessanta giorni dalla data di entrata in vigore del presente decreto.".

(2) Comma così modificato prima dall'art. 6, comma 3, del decreto legge 27 luglio 2005, n. 144 convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155 e poi dall'art. 2 del decreto legislativo 30 maggio 2008, n. 109.

(3) Comma inserito dall'art. 2, comma 1, lett. b), del decreto legislativo 30 maggio 2008, n. 109, con la decorrenza indicata nell'art. 6 dello stesso decreto.

(4) Comma modificato dall'art. 6, comma 3, lett. a) e b), decreto legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, e successivamente abrogato dall'art. 2, comma 1, lett. c), del decreto legislativo 30 maggio 2008, n. 109.

(5) Comma così modificato dall'art. 6, comma 3, del decreto legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.

(6) Comma abrogato dall'art. 2 , comma 1, lett. c), del decreto legislativo 30 maggio 2008, n. 109.

(7) Comma aggiunto dall'art. 6, comma 3, lett. f, del decreto legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, e successivamente abrogato dall'art. 2, comma 1, lett. c) del decretolegislativo 30 maggio 2008, n. 109.

(8) Comma inserito dall'art. 10, comma 1, della legge 18 marzo 2008, n. 48.

(9) Alinea così modificato dall'art. 2, comma 1, lett. d), del decreto legislativo 30 maggio 2008, n. 109.

(10) Lettera soppressa dall'art. 2, comma 1, lett. d), numero 2, del decreto legislativo 30 maggio 2008, n. 109.

(11) Lettera così modificata dall'art. 2, comma 1, lett. d), numero 3, del decreto legislativo 30 maggio 2008, n. 109.

(12) In tema di conservazione di dati di traffico telefonico e telematico, si veda anche l'articolo 4-bis del decreto legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, come modificato dal decreto legge 30 dicembre 2015, n. 210, convertito con modificazioni dalla legge 25 febbraio 2016, n. 21, di cui si riporta per completezza il testo:" *Art. 4-bis Disposizioni in materia di conservazione dei dati di traffico telefonico e telematico*

1. I dati relativi al traffico telefonico o telematico, esclusi comunque i contenuti di comunicazione, detenuti dagli operatori dei servizi di telecomunicazione alla data di entrata in vigore della legge di conversione del presente decreto, nonchè quelli relativi al traffico telefonico o telematico effettuato successivamente a tale data, sono conservati, in deroga a quanto stabilito dall'articolo 132, comma 1, del codice di cui al decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni, fino al 30 giugno 2017, per le finalità di accertamento e di repressione dei reati di cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera a), del codice di procedura penale.

2. I dati relativi alle chiamate senza risposta, effettuate a decorrere dalla data di entrata in vigore della legge di conversione del presente decreto, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibile al pubblico oppure di una rete pubblica di comunicazione, sono conservati fino al 30 giugno 2017.

3. Le disposizioni di cui ai commi 1 e 2 cessano di applicarsi a decorrere dal 1° luglio 2017.".

Si tratta dei c.d. dati esterni alle conversazioni telefoniche e telematiche rilevanti per le investigazioni, anche difensive e per le indagini e costituiti, per esempio, dal numero di telefono chiamante, dal numero di telefono chiamato, dalla durata della conversazione ecc., nonché dall'indirizzo IP del dispositivo connesso alla rete, del dispositivo al quale si è connesso ad es. per visitare un sito web. ecc..

Durante i periodi di tempo appena indicati, i dati possono essere acquisiti presso il fornitore con decreto motivato del pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391-quater del codice di procedura penale, ferme restando le condizioni di cui all'articolo 8, comma 2, lettera f), per il traffico entrante.

Va tuttavia rilevato che i tempi di conservazione sono assolutamente incompatibili con quelli a disposizione delle parti diverse da quelle procedenti in quanto, normalmente, vengono a conoscenza del procedimento e quindi vedono maturare l'interesse e la possibilità di esercitare le facoltà investigative difensive a termini ampiamente scaduti.

Il comma 4-ter dell'art. 132 D.Lgs. 132/03, poi prevede che anche altri soggetti – e quindi il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, - possano autonomamente ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi.

Le ampie incertezze in punto di documentazione della delega del Ministro, dei corpi legittimati in via esclusiva, la genericità della previsione "specifici reati", nonché la mancata previsione delle norme a tutela e conservazione dei dati originari, destano notevoli dubbi sulla coerenza della norma con il sistema,

anche costituzionale, delle garanzie poste a tutela dei dati personali e dei titolari.

Il corollario previsto poi dall'art. 132-bis D.Lgs. 196/03 "*Procedure istituite dai fornitori (1) 1. I fornitori istituiscono procedure interne per corrispondere alle richieste effettuate in conformità alle disposizioni che prevedono forme di accesso a dati personali degli utenti.*

2. A richiesta, i fornitori forniscono al Garante, per i profili di competenza, informazioni sulle procedure di cui al comma 1, sul numero di richieste ricevute, sui motivi legali addotti e sulle risposte date."[187], legittima a ritenere che possano essere previste procedure e percorsi di accesso diretto ai dati personali, sottratte all'iter previsto dall'art. 132 del Codice, eventualità che costituirebbe un ampio e grave *vulnus* al sistema delle garanzie anche costituzionali in tema sia di tutela dei dati personali, sia di procedimentalizzazione delle deroghe al regime ordinario per finalità di giustizia.

4.5.2 I mezzi di ricerca della prova ad oggetto informatico

Come si è detto, la Legge 48/08 è intervenuta anche ad aggiornare i poteri di indagine svolte dal pubblico ministero o sotto la sua direzione e controllo, integrando con "previsioni informatiche" anche le norme riguardanti i casi e le forme delle ispezioni (art. 244, c. 2), i casi e forme delle perquisizioni (art. 247, c. 1-bis), la richiesta di consegna (art. 248, c. 2), il sequestro di corrispondenza (art. 254) il sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni (art. 254-bis), il dovere di esibizione e segreti (art. 256), la custodia delle cose sequestrate (art. 259, c. 2) e l'apposizione dei sigilli alle cose sequestrate (art. 260, c. 1 e 2).

Quanto alle ispezioni, è stato interpolato anche l'art. 244: "*(Casi e forme delle ispezioni). 1. L'ispezione delle persone, dei luoghi e delle cose (103) è disposta con decreto motivato (1253) quando occorre accertare le tracce e gli altri effetti materiali del reato.*

2. Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica (359, 364), anche in relazione a

[187] Articolo inserito dall'art. 1, comma 8, del decreto legislativo 28 maggio 2012, n. 69.

sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione."[188]

La previsione, incentrata sull'attività di ispezione, studio ed esame visivo, non trova corrispondenza tra gli atti diretti di polizia giudiziaria, ma è rimessa all'autorità giudiziaria che, per quanto riguarda i dispositivi digitali, può disporla anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. In tal senso, ancora una volta la norma non sembra fare i conti con la realtà ontologica dei dati digitali: un conto è disporre l'ispezione del dispositivo che costituisce il sistema informatico o telematico inteso nella sua materiale esteriorità, cioè l'hardware, un altro conto è ispezionare i dati. Se nel primo caso l'ispezione può essere effettuata riuscendo ad evitare gli effetti modificativi dell'interazione con il dispositivo adottando precauzione tecniche che impediscano la modifica dei dati, molto più complesso è attuare l'ispezione dei dati stessi evitando l'alterazione e garantendo la conservazione dei dati originari, alla luce delle regole basilari per le quali l'accesso ispettivo ai dati comporta l'intrusione dalla quale possono derivare effetti modificativi dell'integrità dei dati. Per tanto, ispezionare e garantire l'integrità e la conservaizone dei dati originari, costituisce l'ennesima antinomia del sistema.

L'unica tecnica che sembrerebbe idonea a conciliare i poteri e le modalità di esercizio è quella che prevede la realizzazione delle copie di lavoro con le tecniche di copia bit per bit, sulle quali poi svolgere l'ispezione.

Quanto alla norma sulle Perquisizioni, l'art. 247 prevede quanto segue: "*(Casi e forme delle perquisizioni). 1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato (2532) o cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato (60, 61) o dell'evaso, è disposta perquisizione locale (352).*

1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorchè protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. (1)

2. La perquisizione è disposta con decreto motivato (1253).

3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria (57) delegati con lo stesso decreto (370) (2)[189] *".*

[188] Articolo così modificato dall'art. 8 della L. 48/08, 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.

Orbene, al di là delle differenze in punto di diritto attinenti i soggetti e le procedure, in relazione ai punti riguardanti l'attività ad oggetto informatico, la perquisizione disposta dal pubblico ministero presenta i medesimi limiti già esaminati in relazione all'analoga attività di polizia giudiziaria già esaminata e che, per economia espositiva, qui si richiama.

Per l'attività di perquisizione riguardanti dati, informazioni e programmi informatici presso banche, l'art. 248, c. 2, prevede quanto segue: "*(Richiesta di consegna). 1. Se attraverso la perquisizione si ricerca una cosa determinata, l'autorità giudiziaria può invitare a consegnarla. Se la cosa è presentata, non si procede alla perquisizione, salvo che si ritenga utile procedervi per la completezza delle indagini.*
2. Per rintracciare le cose da sottoporre a sequestro (253 ss.) o per accertare altre circostanze utili ai fini delle indagini, l'autorità giudiziaria o gli ufficiali di polizia giudiziaria (57) da questa delegati (370) possono esaminare presso banche atti, documenti e corrispondenza nonchè dati, informazioni e programmi informatici. In caso di rifiuto, l'autorità giudiziaria procede a perquisizione (255). (1)[190]"

Anche in tal caso la lettera è infelice in quanto:

1) non si comprende per quale motivo l'esame presso banche dati, informazioni e programmi informatici non sia sottoposto alle medesime – per quanto imperfette – previsioni di tutela procedimentale e tecnica costituente paradigma introdotto dalla L. 48/08 a tutela dell'integrità e conservazione dei dati, che vengono invece indirettamente richiamate solo nel caso in cui si debba procedere a perquisizione in caso di rifiuto all'invito di consegna. Trattandosi sempre di oggetti digitali, non v'è motivo di introdurre modalità che non garantiscono la tutela minima dell'integrità dei dati.

Quanto al sequestro avente ad oggetto la corrispondenza, l'art. 254 prevede che "*(Sequestro di corrispondenza). 1. Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato.*

[189] Articolo così modificato dall'art. 8, c.2, della L. 48/08, 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.
(2) Cfr. l'art. 68 comma 2 Cost. nonché, per i reati di cui all'art. 90 Cost., l'art. 7, L. 5 giugno 1989, n. 219.

[190] Articolo così modificato dall'art. 8, c.3, della L. 48/08, 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.

2. Quando al sequestro procede un ufficiale di polizia giudiziaria (57), questi deve consegnare all'autorità giudiziaria gli oggetti di corrispondenza sequestrati, senza aprirli o alterarli e senza prendere altrimenti conoscenza del loro contenuto (353).

3. Le carte e gli altri documenti sequestrati che non rientrano fra la corrispondenza sequestrabile sono immediatamente restituiti all'avente diritto e non possono comunque essere utilizzati (1036) (1)."[191]

L'articolo ora annovera la stessa previsione appena analizzata a proposito dell'art. 353, cui si rimanda per evitare di ripetersi.

Anche in relazione al sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni l'art. 254-bis. prevede quanto segue:"*(Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni). – 1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali. (1)"*[192].

L'articolo si ricollega ai poteri previsti dall'art. 132 D. Lgs. 30 giugno 2003, n. 196, di cui, a mio parere, costituisce l'appendice che regolamenta la procedura per la richiesta di dati ai fornitori di servizi e che impone l'acquisizione mediante copia su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità, con l'ordine al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali.

Si può altresì notare la discrasia per la quale, ove sia l'autorità giudiziaria a disporre il sequestro dei dati, questi dovranno essere trattati secondo la procedura tecnica scandita dalla norma in esame, quando invece la stessa richiesta di dati venga avanzata dal difensore-investigatore ai sensi dell'art. 132 D. Lgs. 196/03, questa norma richiama la procedura semplificata dell'art. 391-

[191] Articolo così modificato dall'art. 8, c. 4, della L. 48/2008, 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

[192] Articolo così modificato dall'art. 8, c. 5, della L. 48/08, 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.

quater[193] che prevede una mera richiesta alla quale non segue l'obbligo per il fornitore dei servizi di conservare e proteggere adeguatamente i dati originali.

È evidente come tale disparità di trattamento, per quanto apparentemente avvantaggi la parte privata, si pone come irragionevolmente in contrasto con il principio di parità delle parti ex art. 111 Cost., per un duplice aspetto: da un lato onera il pubblico ministero di procedure più gravose rispetto al difensore, ma dall'altro priva sia il pubblico ministero che il difensore della possibilità di giovarsi del raffronto tra i dati ottenuti ed i dati originari conservati dal fornitore di servizi.

Sempre in ambito di mezzi di ricerca della prova, la L. 48/08 ha modificato anche l'art. 256 che così recita:"*256. (Dovere di esibizione e segreti). 1. Le persone indicate negli artt. 200 e 201 devono consegnare immediatamente all'autorità giudiziaria, che ne faccia richiesta, gli atti e i documenti, anche in originale se così è ordinato, nonchè i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto, e ogni altra cosa esistente presso di esse per ragioni del loro ufficio, incarico, ministero, professione o arte, salvo che dichiarino per iscritto che si tratti di segreti di Stato (202) ovvero di segreto inerente al loro ufficio o professione (200).*

2. Quando la dichiarazione concerne un segreto di ufficio o professionale (200), l'autorità giudiziaria, se ha motivo di dubitare della fondatezza di essa e ritiene di non potere procedere senza acquisire gli atti, i documenti o le cose indicati nel comma 1, provvede agli accertamenti necessari. Se la dichiarazione risulta infondata, l'autorità giudiziaria dispone il sequestro (1).

3. Quando la dichiarazione concerne un segreto di Stato, l'autorità giudiziaria ne informa il presidente del Consiglio dei Ministri, chiedendo che ne sia data conferma. Qualora il segreto sia confermato e la prova sia essenziale per la definizione del processo, il giudice dichiara non doversi procedere per l'esistenza di un segreto di Stato.

4. Qualora, entro sessanta giorni dalla notificazione della richiesta, il Presidente del Consiglio dei Ministri non dia conferma del segreto, l'autorità giudiziaria dispone il sequestro.

5. Si applica la disposizione dell'art. 204."[194].

---

[193] Art. 391 *quater*: "*(Richiesta di documentazione alla pubblica amministrazione) 1. Ai fini delle indagini difensive, il difensore può chiedere i documenti in possesso della pubblica amministrazione e di estrarne copia a sue spese.*
2. L'istanza deve essere rivolta all'amministrazione che ha formato il documento o lo detiene stabilmente.
3. In caso di rifiuto da parte della pubblica amministrazione si applicano le disposizioni degli articoli 367 e 368.".

[194] (1) Gli artt. 12 e 16 della L. 24 ottobre 1977, n. 801, recante norme sull'ordinamento dei Servizi segreti e la disciplina del segreto di Stato così dispongono: "*12. Sono coperti dal segreto di Stato gli atti, i documenti, le notizie, le attività e ogni altra cosa la cui diffusione sia idonea a recar danno alla integrità dello Stato democratico, anche in relazione ad accordi internazionali, alla difesa delle istituzioni poste dalla Costituzione a suo fondamento, al libero*

In particolare, il comma 1, prevede l'estensione ai soggetti gravati da segreto professionale ex art. art. 200[195] o da segreto di ufficio ex art. 201[196], dell'obbligo di consegnare immediatamente all'autorità giudiziaria, che ne faccia richiesta, gli atti e i documenti, anche in originale se così è ordinato,

esercizio delle funzioni degli organi costituzionali, alla indipendenza dello Stato rispetto agli altri Stati e alle relazioni con essi, alla preparazione e alla difesa militare dello Stato.
«In nessun caso possono essere oggetto di segreto di Stato fatti eversivi dell'ordine costituzionale».
«16. Di ogni caso di conferma dell'opposizione del segreto di Stato a' sensi dell'art. 352 c.p.p.
(*) il Presidente del Consiglio dei Ministri è tenuto a dare comunicazione, indicandone con sintetica motivazione le ragioni essenziali, al Comitato parlamentare di cui all'art. 11 della presente legge. Il Comitato parlamentare, qualora ritenga a maggioranza assoluta dei suoi componenti infondata l'opposizione del segreto, ne riferisce a ciascuna delle Camere per le conseguenti valutazioni politiche».
(*) Ora, ai sensi dell'art. 208 coord., art. 202.
(2) Articolo così modificato dall'art. 8, c. 6, della L. 48/2008, recante Ratifica ed esecuzione della Convenzione del Consiglio.

[195] Art. 200 *(Segreto professionale) 1. Non possono essere obbligati a deporre su quanto hanno conosciuto per ragione del proprio ministero, ufficio o professione, salvi i casi in cui hanno l'obbligo di riferirne all'autorità giudiziaria [331, 334]:*
a) i ministri di confessioni religiose, i cui statuti non contrastino con l'ordinamento giuridico italiano;
b) gli avvocati, gli investigatori privati autorizzati, i consulenti tecnici e i notai (1);
c) i medici e i chirurghi, i farmacisti, le ostetriche e ogni altro esercente una professione sanitaria;
d) gli esercenti altri uffici o professioni ai quali la legge riconosce la facoltà di astenersi dal deporre determinata dal segreto professionale [256 2, 271] (2).
2. Il giudice, se ha motivo di dubitare che la dichiarazione resa da tali persone per esimersi dal deporre sia infondata, provvede agli accertamenti necessari. Se risulta infondata, ordina che il testimone deponga.
3. Le disposizioni previste dai commi 1 e 2 si applicano ai giornalisti professionisti iscritti nell'albo professionale, relativamente ai nomi delle persone dalle quali i medesimi hanno avuto notizie di carattere fiduciario nell'esercizio della loro professione. Tuttavia se le notizie sono indispensabili ai fini della prova del reato per cui si procede e la loro veridicità può essere accertata solo attraverso l'identificazione della fonte della notizia, il giudice ordina al giornalista di indicare la fonte delle sue informazioni [195 7] (3)."
(1) Tale lettera è stata così sostituita ex art. 4, della l. 7 dicembre 2000, n. 397, che ha modificato tale elenco, sopprimendo la scomparsa categoria dei procuratori legali e inserendovi invece gli investigatori privati autorizzati.
(2) Categoria di carattere residuale in cui rientrano ad esempio psicologi, dottori commercialisti e i dipendenti del servizio pubblico per le tossicodipendenze, i quali non possono essere obbligati a deporre su quanto hanno conosciuto per ragione della loro professione né davanti all'autorità giudiziaria, né davanti ad altra autorità.
(3) Il regime particolare del segreto giornalistico riguarda solo i giornalisti professionisti iscritti nell'apposito albo, risultando quindi esclusi i c.d. pubblicisti.

[196] Art. 201 "*(Segreto di ufficio) 1. Salvi i casi in cui hanno l'obbligo di riferirne all'autorità giudiziaria, i pubblici ufficiali [c.p. 357], i pubblici impiegati e gli incaricati di un pubblico servizio [c.p. 358] hanno l'obbligo di astenersi dal deporre su fatti conosciuti per ragioni del loro ufficio che devono rimanere segreti [c.p. 326; c.p.p. 204, 256 2] (1).*
2. Si applicano le disposizioni dell'articolo 200 commi 2 e 3 (2) (3)."
(1) Tali soggetti non hanno tanto la facoltà, come previsto ex art. 200 in caso di segreto professionale, quanto l' obbligo di astenersi dal deporre.
(2) Tuttavia sono salvi i casi in cui tali soggetti hanno l'obbligo di riferire all'autorità giudiziaria (ad es. artt. 331, 361 e 362).
(3) Il segreto d'ufficio è inopponibile nei procedimenti relativi ai reati di alto tradimento e attentato alla Costituzione previsti dall'art. 90 del testo costituzionale, ex art. 6, comma 2 della l. 5 giugno 1989, n. 219.

nonchè i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto. Va osservato che essendo tali soggetti i destinatari dell'obbligo del compimento dell'operazione di copia su adeguato supporto, e non ad esempio gli ufficiali di polizia giudiziaria, e non essendo previsto alcun altro obbligo di conservazione e custodia dei dati originari, la previsione apre scenari giuridici dagli esiti più articolati e imprevedibili circa le conseguenza dell'effettuazione di copia su supporto inadeguato e sull'impossibilità sopravvenuta di effettuare il confronto tra i dati originari e quelli copiati e consegnati.

All'esito del sequestro conseguono alcuni obblighi a carico del custode delle cose sequestrate previsti dall'art. 259, c. 2, ora estesi anche al custode di dati digitali, così previsti:"*259. (Custodia delle cose sequestrate) (1). 1. Le cose sequestrate sono affidate in custodia alla cancelleria o alla segreteria. Quando ciò non è possibile o non è opportuno, l'autorità giudiziaria dispone che la custodia avvenga in luogo diverso, determinandone il modo e nominando un altro custode, idoneo a norma dell'art. 120 (att. 813, 82; reg. 10, 11).*

2. All'atto della consegna, il custode è avvertito dell'obbligo di conservare e di presentare le cose a ogni richiesta dell'autorità giudiziaria nonché delle pene previste dalla legge penale per chi trasgredisce ai doveri della custodia. Al custode può essere imposta una cauzione. Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria. Dell'avvenuta consegna, dell'avvertimento dato e della cauzione imposta è fatta menzione nel verbale. La cauzione è ricevuta, con separato verbale (135), nella cancelleria o nella segreteria."[197].

Le implicazioni della norma balzano evidenti ove si consideri che i dati, non essendo cose, vengono comunque fatte oggetto di obbligo di custodia, mentre nulla si dice circa la sorte degli eventuali supporti, essendo l'unica prescrizione riservata al supporto sul quale consegnare la copia. Nulla si dice in relazione al concetto di adeguatezza del supporto, che pertanto non potrà che rimandare al concetto di adeguatezza tecnica e quindi rivolgere l'attenzione alle prescrizioni informatiche che indicano i requisiti in materia.

Di sicuro rilievo vi è che la custodia ex comma 1 può essere affidata alla cancelleria del tribunale o alla segreteria che diventano custodi *ex lege* o ad un terzo nominato custode *ad hoc*. Il comma 2, nel prevedere le avvertenze e gli obblighi del custode in relazione ai dati, informazioni o programmi informatici, non distingue tra le due tipologie di custodi, e fa dipendere l'"*obbligo di*

[197] Articolo così modificato dall'art. 8, c. 7, della L. 48/2008, 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.

impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria" dalla custodia e non dalla qualità del custode". Sembra quindi fondato ritenere che la cancelleria e la segreteria, investite di tali obblighi, dovrebbero conoscere le tecniche ed i contenuti dell'Informatica forense al fine di svolgere al meglio la custodia.

Inoltre, poiché la custodia si risolve in una forma di trattamento di dati (anche sensibili), tale aspetto suscita sia gli obblighi di adozione delle misure di sicurezza ex art. 34 del D. Lgs. 196/03, ove in caso di omissione, consegue la responsabilità penale ex art. 169 del Codice, sia la responsabilità per i danni cagionati per effetto del trattamento ex art. 15 del Codice, che richiama la responsabilità ex art. 2050 c.c..

Come si è già detto, non sono previsti altri obblighi atteso che l'All. C) al D. Lgs. 196/03 - Trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia - non è stato ancora adottato (ex artt. 46 e 53 Cod.) nonostante il termine ex art. 181, 3° c., sia scaduto dal 30 giugno 2004.

Quindi, gli obblighi di custodia dei dati risultano molto gravosi.

Infine, sempre per ciò che attiene al sequestro, è stato modificato l'art. 260: "*(Apposizione dei sigilli alle cose sequestrate. Cose deperibili). 1. Le cose sequestrate si assicurano con il sigillo dell'ufficio giudiziario e con le sottoscrizioni dell'autorità giudiziaria e dell'ausiliario che la assiste (126) ovvero, in relazione alla natura delle cose, con altro mezzo, anche di carattere elettronico o informatico, idoneo a indicare il vincolo imposto a fini di giustizia (349 c.p.).*

2. L'autorità giudiziaria fa estrarre copia dei documenti e fa eseguire fotografie o altre riproduzioni delle cose sequestrate che possono alterarsi o che sono di difficile custodia, le unisce agli atti e fa custodire in cancelleria o segreteria gli originali dei documenti, disponendo, quanto alle cose, in conformità dell'art. 259. Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria.

3. Se si tratta di cose che possono alterarsi, l'autorità giudiziaria ne ordina, secondo i casi, l'alienazione o la distruzione (att. 83)"[198].

Anche per questa norma il legislatore ha esteso il concetto analogico di sigillo alla dimensione digitale, introducendo il concetto di sigillo elettronico o informatico da apporsi, evidentemente alle riproduzioni delle cose sequestrate che possono alterarsi o che sono di difficile custodia.

[198] Articolo così modificato dall'art. 8, c. 8, della L. 48/08, 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

Peraltro, la norma specifica proprio che in caso di riproduzione dei dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria.

A quest'ultimo proposito, la previsione di una custodia degli originali in luoghi diversi, suscita tutte le considerazioni appena esposte a proposito dell'articolo precedente. Inoltre, la ricorrenza anche in questo caso delle modalità di effettuazione della copia, impongono di passare alla disamina delle tecniche con le quali devono essere attuate le forme di trattamento dei dati a fini processuali penali.

4.6 Le tecniche di attuazione delle procedure introdotte nel codice di procedura penale dalla L. 48/08

La novella ha introdotto alcuni principi ricorrenti in tutte le norme del codice di procedura penale al fine di garantire l'attendibilità dei dati oggetto id trattamento a fini processuali, ma non fissa le specifiche tecniche. Sul punto, un ampio settore di pratici ha semplicisticamente invocato la necessità di best practice investigative al pari di alcune esperienze d'oltreoceano[199], ritenendo che un protocollo uniforme possa costituire la soluzione dei problemi. In realtà, tale approccio trascura che le tecniche di Informatica forense non possono essere procedimentalizzate in quanto unicamente sottoposte alla verifica e validazione con metodo scientifico. In secondo luogo, mancano autorità investite del potere di fissare le procedure in best practice; inoltre, il progresso tecnologico è così rapido, che ogni best practice subirebbe un processo di rapida obsolescenza; vi è poi che, l'applicazione della legge non può essere subordinata all'esistenza o all'applicazione di regole extragiuridiche; infine, è difficile ipotizzare best practice così proattive da anticipare la stessa immissione sul mercato di nuovi dispositivi o software (si pensi ad es. alla necessità di acquisire dati relativi ad un reato commesso con un telefono cellulare appena immesso sul mercato).

Alcuni studiosi operanti presso la Cattedra di Informatica forense di Bologna hanno invece messo a punto delle procedure empiriche che hanno attuato i principi della Convenzione (uso di supporti ottici, firma digitale, calcolo dell'hash mediante appropriati algoritmi, ecc.) che danno forma tecnica ai precetti appena esaminati, che sono stati ritenuti scientificamente fondati, e che di recente hanno incontrato l'avvallo degli standard ISO 2012:27037.

[199] Cfr. BREZINSKI D., KILLALEA T., *Guidelines for evidence collection and archiving*, RFC 3227, Best Current Practice 55 della Internet Engineering Task Force, 2002, in https://tools.ietf.org/html/rfc3227 .

Le norme modificate dalla L. 48/08 prevedono ora che la procedura paradigmatica da realizzare allorquando i dati vengano trattati a fini giudiziari, consista nella realizzazione di copia dei dati che deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione; inoltre, la procedura può prevedere l'apposizione alla copia del sigillo elettronico o informatico.

Gli strumenti che realizzano tale obbligo sono l'immagine bit per bit, su memorie secondarie durevoli, verificate mediante l'hash, firmate digitalmente e marcate temporalmente.

4.6.1 La procedura per la copia forense dei dati

La procedura di acquisizione e copia dei dati costituisce un momento centrale dell'investigazione-indagine sui dati informatici[200]. Allo stato, il miglior metodo per l'acquisizione dei dati da una memoria è ritenuto essere il processo di produzione di una c.d. *bit-stream image* o immagine bit per bit che, per la valenza processuale è detta anche "copia forense", vale a dire una copia completa e integrale della memoria sulla quale sono archiviati i bit, inclusi gli spazi non allocati, quelli apparentemente non allocati e gli slack space, e con modalità che non comportano alterazione di dati (ad esempio, date di creazione, ultimo accesso, di ultima modifica).

Infatti, possono verificarsi casi nei quali sulla memoria siano stati archiviati non solo i dati che "appaiono", e cioè quelli che sono immediatamente fruibili, ma anche altri non visibili in quanto cancellati, o archiviati con particolari modalità, quali ad esempio le tecniche di cifratura o steganografia o entrambe simultaneamente.

La cancellazione dei dati da una memoria mediante le procedure standard fornite dai sistemi operativi, salvo che non sia effettuata con particolari tecniche di c.d. *wiping* che vadano a sovrascrivere i dati, riguarda solo l'indice che consente di ricostruire i documenti cosicché l'utente non riesce più ad accedervi. Tuttavia, i dati c.d. cancellati, fino a quando non vengono sovrascritti, sono ancora archiviati sulla memoria e quindi potenzialmente recuperabili e analizzabili.

Stesso discorso va fatto per i dati registrati nei c.d. *slack space*[201]. Per comprendere il fenomeno bisogna partire dall'organizzazione della memoria la

[200] Per le tecniche di acquisizione, cfr. FERRAZZANO M., Indagini forensi in tema di scambio di file pedopornografici mediante software di file sharing a mezzo peer-to-peer, Tesi di dottorato XXVI ciclo Università di Bologna. 2014, in *http://amsdottorato.unibo.it/6697/*.

[201] Ci sono varie tipologie di slack space: *volume slack*, cioè lo spazio che residua alla fine di un disco; *partition slack*, ossia lo spazio che residua alla fine della partizione di un disco; *sector slack*, cioè lo spazio che residua alla fine del settore non utilizzato dal nuovo file archiviato. Nel

quale è strutturata in blocchi (settori) di dimensione fissa. Su tali blocchi vengono archiviati i bit, a prescindere dalle dimensioni del file. Allorquando i file sono di dimensioni inferiori a quella dei blocchi, rimarrà un'area di memoria inutilizzata, più o meno vasta. Ma se in tale area erano stati già archiviati dati dei file successivamente cancellati, nell'area all'interno dei blocchi rimasta inutilizzata dall'archiviazione dei file successivi continueranno ad insistere dati dei file precedentemente archiviati e continueranno ad essere ivi archiviati finché lo spazio non verrà sovrascritto a seguito di allocazione di nuovi file o di operazioni di wiping.

Pertanto, il processo di acquisizione e copia dei dati deve essere svolto in modo tale da non alterare alcun bit della memoria originaria e deve essereintegrale, deve cioè (tendere a) realizzare una sequenza di bit da archiviare su una memoria di destinazione che rappresenti perfettamente la sequenza originaria di bit archiviata sulla memoria sorgente. A tal fine, tra la memoria sulla quale sono archiviati i dati originari e la memoria di destinazione dell'immagine bit per bit, vengono interposti dei dispositivi hardware o software o combinazione dei due, che impediscono l'accesso in scrittura alla memoria, e quindi la modifica, dei dati originari.

Il risultato finale di una tale procedura di acquisizione di dati deve essere un perfetto clone della memoria originaria, e quindi una memoria sulla quale è archiviata la stessa identica sequenza della memoria sorgente, oppure un file immagine (o una serie di file frammentati) che riproduca la stessa identica sequenza di bit archiviata sulla memoria originaria; in questo secondo caso, è possibile applicare algoritmi di compressione dei dati.

La verifica di conformità tra i dati originari e la copia bit per bit ottenuta viene effettuata mediante la funzione di hash, già descritta nei primi capitoli: se l'hash della stringa costituita dai bit della copia bit per bit coincide con l'hash della stringa costituita dai bit originari, allora esse sono conformi.

Per attuare tali operazioni, sono necessarie modalità operative e strumenti che dipendono dalla situazione, dai tempi necessari all'effettuazione dell'operazione, e dai costi di esecuzione.

Inoltre, affinché possano essere replicabili e verificabili da qualunque altra parte o dai loro consulenti tecnici, le operazioni devono essere dettagliatamente documentate.

Le norme esaminate impongono altresì che la copia venga effettuata su un "adeguato supporto", senza specificare che cosa si intenda con tale espressione, ma evidentemente rinviando alla scienza informatica per l'individuazione della tecnica che in concreto realizzi tale obiettivo. Inoltre, opportunamente la legge

caso appena indicato, i dati dello slack space sono sempre parzialmente sovrascritti e si collocano nella parte finale di un settore tra la fine del file e la fine del settore. Effettuata l'acquisizione, può procedersi alla ricerca di dati rilevanti mediante una ricerca per parola chiave. Per queste notazioni e altre sugli slack space, cfr. FERRAZZANO M., op.cit., p. 34.

non ha messo limiti alla scelta dello strumento da usare, atteso che la tecnologica in materia, come già esposto agli inizi della presente esposizione, è in costante evoluzione. Allo stato attuale, i supporti ritenuti adeguati sono costituiti dalle memorie magneto-ottiche (IDE, SCSI, RAIDs.) e dai dischi ottici (CD-ROM, DVD, Blu-Ray Disc)[202].

Alla copia bit per bit viene quindi apposta la marca temporale, una funzione ben descritta dall'art. 20, c. 3, del D. lgs 82/2005 (Codice dell'Amministrazione Digitale) come sistema offerto da un Certificatore Accreditato, che permette di associare data e ora certe e legalmente valide ad un documento informatico, consentendo quindi di associare una validazione temporale opponibile a terzi.

Tale funzione viene apposta per dare certezza temporale all'hash della stringa copiata, anche quale data certa ai fini della procedura di apposizione del sigillo elettronico.

Infine, alla copia bit per bit viene apposta la firma digitale dell'operatore (ufficiale di polizia giudiziale, consulente tecnico, perito o terzo).

4.7 Le carenze della L. 48/08

Sul versante esterno sembra ancora lontano l'obiettivo della Convenzione di Budapest di armonizzare le normative degli Stati aderenti al fine di dare, coordinamento, effettività ed efficacia alla normativa comune, in vista dell'unificazione della disciplina della prova informatica a livello europeo[203].

Sul versante interno, invece, la Legge 48/08 ha avuto il merito di introdurre principi senza dubbio innovativi, per quanto il panorama normativo sia ancora caratterizzato da una lunga e articolata serie di criticità.

Difatti, la frettolosa tecnica interpolativa attuata dal legislatore con la L. 48/08 ha comportato ampi interventi sul codice di procedura penale, per cui le nuove norme per le attività investigative e di indagine ad oggetto informatico non sono dedicate ai soli reati informatici, ma a tutti i tipi di reato, comuni o speciali che siano, purché vi siano elementi informatici rilevanti per le indagini.

Ne è derivato un effetto tanto paradossale rispetto agli intenti del legislatore quanto benefico per il principio di uguaglianza e per il sistema delle garanzie difensive: dovendo applicarsi le nuove norme e le tecniche di informatica forense a qualunque tipo di reato - e quindi ai reati informatici in senso stretto, ai reati a condotta libera commessi mediante l'informatica e la telematica e ad ogni altro tipo di reato i cui indizi o elementi di prova possano essere rinvenuti

---

[202] Per una breve rassegna dell'evoluzione tecnologica delle memorie secondarie, v. *http://www.tecnoteca.it/museo/16/document_view*.

[203] Su tale ambizioso progetto, si vedano i risultati della ricerca promossa dalla Commissione Europea – Direzione Generale Giustizia Libertà e Sicurezza - Progetto AGIS 2005/AGIS/119 su "The Admissibility of Electronic Evidence at Court: Fighting against High Tech Crime", atti in Cybex, (a cura di), conclusioni del Programma, in www.cybex.es (testo in inglese, francese e spagnolo).

nei sistemi informatici o telematici - anche le problematiche tecniche e giuridiche ancora irrisolte riguardano *ope legis* ogni tipo di fattispecie di reato.

Inoltre, l'applicabilità delle nuove tecniche a tutti i tipi di reati, da un lato neutralizza la paventata specializzazione che giustificherebbe l'ormai anacronistica riserva di competenza per i reati informatici prevista dall'art. 51[204] in favore delle procure distrettuali, dall'altro, impone a tutti gli attori del procedimento di conoscere e governare le nuove dinamiche procedimentali riguardanti i dati informatici.

Sul versante interno, sotto il profilo teorico, se la dottrina è alacremente impegnata in analisi puntuali[205] e la giurisprudenza di merito mostra aperture progressivamente sempre più ampie verso tali tematiche, la giurisprudenza di legittimità rimane assestata su posizioni che dimostrano una sostanziale inadeguatezza culturale e tecnica, informatica e giuridica, verso la comprensione dei nuovi fenomeni.

Infine, se da un lato va riconosciuto che la Legge 48/08 ha introdotto principi senza dubbio innovativi per l'ordinamento italiano, non può essere sottaciuto che essa è caratterizzata anche da una lunga e articolata serie di criticità cui si dovrebbe porre rimedio prima che si producano effetti dannosi, e di cui si rassegnano le più rilevanti:

1. è mancata una disciplina transitoria rispetto all'entrata in vigore della L. 48/08, per cui si sono verificati casi in cui gli indizi e gli elementi di prova sono stati raccolti prima dell'entrata in vigore o nel periodo di *vacatio legis,* e quindi senza il rispetto delle modalità di acquisizione previste dalla legge, e casi nei quali l'acquisizione è avvenuta successivamente all'entrata in vigore della legge, e quindi secondo modalità giuridiche diverse, sicuramente più affidabili rispetto a quelle precedenti alla novella. Tale fenomeno ha creato una profonda disparità di trattamento, con violazione del principio fondamentale di uguaglianza, per quanto, non si può non notare che dette modalità di acquisizione introdotte dalla L. 48/08 potevano e dovevano essere applicate anche prima dell'entrata in vigore in quanto finalizzate a mantenere integro e attendibile il patrimonio informativo dei dati informatici;

[204] V. l'art. 51, c. 3 bis, prevede che per i procedimenti per i delitti, consumati o tentati, di cui agli artt. 416, sesto comma, 600, 601, 602, (8) 416 bis e 630 del codice penale, per i delitti commessi avvalendosi delle condizioni previste dal predetto art. 416 bis ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo, nonché per i delitti previsti dall'art. 74 del testo unico approvato con D.P.R. 9 ottobre 1990, n. 309, e dall'articolo 291 quater del testo unico approvato con decreto del Presidente della Repubblica 23 gennaio 1973, n. 43, le funzioni di pubblico ministero nelle indagini preliminari e nei procedimenti di primo grado, sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente .

[205] Cfr. LUPARIA, L., (a cura di), (2009), *passim*.

2. è mancata l'espressa previsione di inutilizzabilità se non di nullità dei mezzi di prova acquisiti in violazione delle procedure previste dalle norme introdotte con la L. 48/08[206];
3. è mancata la previsione di una catena di custodia dei reperti informatici sequestrati, ovvero la formalizzazione di una procedura di registrazione di tutti i passaggi ai quali sono soggetti gli elementi di prova al fine di tutelare la loro capacità rappresentativa[207];
4. è mancato l'adeguamento delle norme a tutela dei dati personali e sensibili oggetto di trattamento per fini di Polizia e di Giustizia di cui all'Allegato C) previsto dagli artt. 46 e 53 del D. Lgs. 196/03, in punto di "Trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia", allegato mai varato sino ad oggi. Il

[206] In generale, sulle invalidità e nullità delle prove penali, v. ANGELETTI R., Le invalidità delle prove e dei mezzi di prova, op.cit.

[207] Sulla catena di custodia in materia di dispositivi informatici, il legislatore potrebbe trarre suggerimenti, ad esempio, dal Codice penale colombiano (LEY n. 906 del 31 agosto 2004, Còdigo de Procedimiento Penal della Repubblica di Colombia, in http://www.pensamiento penal.com.ar/system/files/2014/12/legislacion30901.pdf), il quale disciplina in modo puntuale la fase del sequestro di dispositivi informatici, la catena di custodia (art. 254 e ss.) e la responsabilità dei pubblici ufficiali che entrino in contatto con i mezzi di prova: "*Artículo 236. Recuperación de información dejada al navegar por internet y otros medios tecnológicos que produzcan efectos equivalentes.*
Cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para inferir que el indiciado o el imputado ha estado transmitiendo información útil para la investigación que se adelanta, durante su navegación por internet y otros medios tecnológicos que produzcan efectos equivalentes, ordenará la aprehensión del computador, computadores y servidores que pueda haber utilizado, disquetes y demás medios de almacenamiento físico, para que expertos en informática forense descubran, recojan, analicen y custodien la información que recuperen.
En estos casos serán aplicables analógicamente, según la naturaleza de este acto, los criterios establecidos para los registros y allanamientos.
La aprehensión de que trata este artículo se limitará exclusivamente al tiempo necesario para la captura de la información en él contenida. Inmediatamente se devolverán los equipos incautados."
Cadena de custodia Artículo 254. Aplicación. Con el fin de demostrar la autenticidad de los elementos materiales probatorios y evidencia física, la cadena de custodia se aplicará teniendo en cuenta los siguientes factores: identidad, estado original, condiciones de recolección, preservación, embalaje y envío; lugares y fechas de permanencia y los cambios que cada custodio haya realizado. Igualmente se registrará el nombre y la identificación de todas las personas que hayan estado en contacto con esos elementos.
La cadena de custodia se iniciará en el lugar donde se descubran, recauden o encuentren los elementos materiales probatorios y evidencia física, y finaliza por orden de autoridad competente.
Parágrafo. El Fiscal General de la Nación reglamentará lo relacionado con el diseño, aplicación y control del sistema de cadena de custodia, de acuerdo con los avances científicos, técnicos y artísticos.
Artículo 255. Responsabilidad. La aplicación de la cadena de custodia es responsabilidad de los servidores públicos que entren en contacto con los elementos materiales probatorios y evidencia física.
Los particulares que por razón de su trabajo o por el cumplimento de las funciones propias de su cargo, en especial el personal de los servicios de salud que entren en contacto con elementos materiales probatorios y evidencia física, son responsables por su recolección, preservación y entrega a la autoridad correspondiente.

termine per l'adozione del Regolamento, ex art. 181, 3° c., è scaduto dal 30 giugno 2004 e da quella data il nostro Ordinamento conosce una inammissibile *lacuna legis* in favore dello Stato. L'enorme quantità di dati soggetta all'attività investigativa, di indagine e giudiziaria in senso lato, viene trattata al di fuori delle previsioni comuni della legge a tutela dei dati personali ed è priva di qualunque forma di protezione, soprattutto a riguardo delle misure di sicurezza da adottarsi per prevenire ed evitare danni ai dati, soprattutto quando riguardano soggetti del tutto estranei ai fatti per i quali si procede. Di fatto, tale situazione costituisce una grave violazione del principio di legalità e priva di tutela tutti i cittadini i cui dati incorrano in trattamenti illeciti per motivi di giudiziari e di polizia;

5. manca l'espressa previsione di inutilizzabilità o, meglio, di nullità dei mezzi di prova acquisiti in violazione delle procedure previste dalla L. 48/08;
6. per quanto lo imponga la Convenzione di Budapest, l'ordinamento non è stato adeguato alle condizioni e alle tutele previste dal proprio diritto interno, agli obblighi di tutela dei diritti umani e delle libertà, nonché al principio di proporzionalità. Difatti, tra molte altre avverse ragioni (si pensi alla lesione del principio di proporzionalità, per cui le nuove previsioni, a seguito della loro collocazione nella disciplina comune, si applicano anche ai casi di reati bagatellari), non vi è stato alcun intervento che abbia aumentato le tutele difensive;
7. non è ancora stato attuato il fondamentale precetto previsto dalla Convenzione di Budapest secondo il quale, a fronte dell'adozione delle nuove tecniche che minacciano i diritti e le libertà individuali, si impone il rafforzamento delle tutele degli indagati al fine di bilanciare la pervasività dei nuovi strumenti investigativi, cosicché appare evidente come, al contrario, il nuovo assetto abbia ampliato ulteriormente le asimmetrie tra i poteri inquirenti e le facoltà difensive. A tal proposito, basti pensare al mancato coordinamento tra i principi previsti dall'art. 6 della Convenzione dei Diritti dell'Uomo in materia processuale e dall'art. 111 della Costituzione italiana in punto di Giusto processo (dal diritto alla celere informazione della persona accusata, alla formazione in contraddittorio della prova, alle eccezioni a tale principio) e l'esegesi delle norme dell'ordinamento processual penale in tema di investigazioni e indagini ad oggetto informatico.

Tale carenza non è certo rilevata dalla giurisprudenza di legittimità che, anzi, sta consolidando orientamenti giurisprudenziali del tutto discutibili sotto il

profilo del corretto inquadramento giuridico delle fattispecie ad oggetto informatico e soprattutto incoerenti con i principi fondamentali degli altri istituti dell'ordinamento giuridico italiano.

5 La questione delle best practice in Informatica forense

Soprattutto nel periodo ante L. 48/08, gli operatori impegnati in indagini aventi ad oggetto dati informatici, hanno avvertito l'esigenza di metodologie pratiche condivise, indicate come best practice, linee guida, criteri, ecc., per l'attuazione delle operazioni tecniche di trattamento dei dati informatici a fini forensi.

In senso più ampio, per best practice[208] si intende l'"*Insieme delle attività (procedure, comportamenti, abitudini ecc.) che, organizzate in modo sistematico, possono essere prese come riferimento e riprodotte per favorire il raggiungimento dei risultati migliori in ambito aziendale, ingegneristico, sanitario, educativo, governativo e così via". L'espressione fa riferimento anche al processo di sviluppo e applicazione di standard operativi usati dalle organizzazioni complesse, ma vi sono espressioni equipollenti*[209].

Nell'ambito dell'Informatica forense, con l'espressione best practice si è fatto spesso riferimento alle pratiche sviluppate oltreoceano da agenzie federali o da associazioni del settore operanti nel settore ritenute un punto di riferimento per l'approccio agli aspetti tecnico-informatici dell'Informatica forense[210].

---

[208] In prima approssimazione:"MIGLIORE PRATICA, TECNICA DELLA (BEST PRACTICE)" è l' "*Insieme delle attività (procedure, comportamenti, abitudini ecc.) che, organizzate in modo sistematico, possono essere prese come riferimento e riprodotte per favorire il raggiungimento dei risultati migliori in ambito aziendale, ingegneristico, sanitario, educativo, governativo e così via. L'espressione è stata inizialmente elaborata in ambito manageriale ai primi del Novecento in riferimento all'osservazione delle tecniche che si rivelavano in grado di ottenere i migliori risultati e che, quindi, opportunamente sistematizzate, potevano costituire un sistema di regole da rispettare per rendere più efficiente le modalità produttive. Nel campo della produzione aziendale (prima della certificazione ISO 9001), il sistema della best practice rappresentava, quindi, la tecnica di riferimento per ottimizzare i risultati (massimo risultato, minimo dispendio di risorse ed elevato standard qualitativo), superando passaggi inutili e inefficaci. Nel corso del tempo, tale sistema è stato progressivamente applicato a molti altri settori e inquadrato in specifici standard normativi che rappresentano il benchmarking e il modello di autovalutazione per i diversi contesti. (...) Le best practice possono differenziarsi in pratiche promettenti (promising practices) e pratiche basate su prove di efficacia (evidence-based practices)." in* TRECCANI.IT, 2012, da *http://www.treccani.it/enciclopedia/migliore-pratica-tecnica-della_%28Dizionario-di-Economia -e-Finanza%29/*).

[209] Sono usati in termini equivalenti, espressioni come "Golden standard", "pratiche migliori", "linee guida", "protocolli", "Criteri guida".

[210] Esempi di best practice per la Computer forensics sono quelle predisposte dall'International Organization on Computer Evidence (IOCE), in *http://www.oas.org/juridico/english/cyber_links.htm*, quelle dello Scientific Working Group on Digital Evidence (SWGDE), tra le quali si segnalano le Best Practices for Computer Forensics, (Ver. 1.0, 15/11/2004; ver. 3.0, Sept. 2013, in *https://www.swgde.org/documents/Archived%20Documents*, quelle dello Scientific Working Group on Imaging Technology (SWGIT) soprattutto per ciò che attiene alle Best Practices on Imaging, in *https://www.swgit.org/documents*, quelle del National Institute of Standards and Technology (NIST) relative al settore Forensic Science — Digital and

Il dibattito svoltosi nella prima metà degli anni 2000 ha preso le mosse da problemi reali quali l'inadeguatezza della normativa processuale che non prevedeva riferimenti o indicazioni tecniche da adottare; l'inadeguatezza delle procedure investigative, non sufficientemente sviluppate, l'inadeguata formazione tecnica degli addetti e la scarsità dei mezzi a disposizione degli operatori. Tuttavia, si può ritenere che fosse soprattutto la polizia giudiziaria a necessitare di linee guida per indirizzare al meglio la propria attività, a mio parere non tanto per zelo epistemologico quanto, più utilitaristicamente, per consentire ai risultati dell'indagine di "resistere" alla pugna processuale.

Il dibattito sulle best practice in Informatica forense si è quindi concentrato su vari elementi:

- circa l'oggetto da definire, veniva evidenziata la necessità di delineare procedure tecniche uniformi per il trattamento standard di dati digitali a fini processuali;

- circa la loro finalità, veniva individuata nella necessità di fornire supporto teorico e pratico alle attività tecniche di indagine e di investigazione della Polizia Giudiziaria, del pubblico ministero e dei relativi consulenti;

- in merito alle figure da coinvolgere, venivano individuati alcuni operatori forensi, e quindi sostanzialmente addetti di polizia giudiziaria, magistrati, avvocati, tecnici;

- sul riconoscimento alle best practice di una efficacia processuale privilegiata, e quindi la presunzione *iuris tantum* di validità delle procedure seguite e la vincolatività di tutte le parti del processo.

Tuttavia, alla miglior disamina, tale impostazione ha rivelato gravi limiti, così sintetizzabili:

- circa l'oggetto delle best practice della Computer Forensics, emergeva evidente la lacuna costituita dalla mancanza di principi giuridici circa il trattamento di dati digitali a fini di prova, peraltro sancita dalla prima giurisprudenza attestata su posizioni ancora arretrate;

Multimedia Evidence e sopratutto per quelle sviluppate nell'ambito dell'attività di controllo e testing degli strumenti per la Computer forensics, in *http://www.cftt.nist.gov/*; va segnalata anche l'attività dell'International Association of Computer Investigative Specialists (IACIS), una delle prime associazioni attive nel settore della computer forensics; per altre raccolte di best practice sviluppate in ambito europeo, v. quelle dell'Association of Chief Police Officers – Computer Crime Working Group (ACPO), Good Practice Guide for Digital Evidence, UK, 2012, quelle dell'European Network of Forensics Science Institutes, (ENFSI), Guidelines For Best Practice In The Forensic Examination Of Digital Technology (Ver. 6, 20/4/2009); uancerta rilevanza, è assunta dal lavoro ricognitivo svolto su incarico della Commissione Europea – Direzione Generale Giustizia Libertà e Sicurezza - Progetto AGIS 2005/AGIS/119 su "The Admissibility of Electronic Evidence at Court: Fighting against High Tech Crime" in *http://www.cybex.es*; da ultimo, vedi le best practice dei gruppi di studio operanti in seno all'UE "Cybercrime@IPA Regional Co-operation in Criminal Justice: Strengthening capacities in the fight against cybercrime", Guida alla prova digitale - Linee guida per polizia giudiziaria e autorità giudiziaria, Versione 1.0.

- le finalità perseguite, in assenza di principi e riferimento alla mutuabilità nell'ambito delle investigazioni difensive, concretizzavano il rischio di strumentalizzazione delle procedure da parte degli addetti alle attività di investigazione e di indagine;

- quanto ai redattori delle best practice non veniva evidenziato alcun criterio valido di selezione nell'ambito di un valido percorso accademico e scientifico, rimanendo così l'espressione di un'attività volontaristica ed estemporanea; inoltre, l'omessa indicazione degli ausiliari del procedimento quali soggetti da coinvolgere (cancellieri, ufficiali giudiziari, custodi), costituiva un indice dell'errore di fondo a riprova di un approccio parziale, e quindi non scientifico, alla questione;

- infine, in merito all'efficacia processuale delle best practice, si ignorava che una loro efficacia privilegiata avrebbe condizionato il giudicante (e il giudizio) violando simultaneamente i principi costituzionali e processuali di sottoposizione del giudice unicamente alla legge (art. 101, c. 2, Cost.), della formazione del libero convincimento del giudice (art. 192), del contraddittorio e della formazione della prova nella fase del dibattimento (art. 111 Cost.).

Rispetto al dibattito svoltosi nella prima metà degli anni 2000 per l'individuazione di prescrizioni tecniche spendibili in ambito forense, più che ai "migliori strumenti", ritengo che il risultato sia approdato tutt'al più a risultati condivisibili o, al più, praticabili.

Da ultimo, alcuni tentativi, per quanto risultato di lodevole volontarismo, non sono stati riconosciuti come vincolanti o rilevanti per gli attori del processo e si sono presto rivelati inidonei sia a soddisfare l'esigenza di continua revisione per tenere il passo con il progresso tecnologico.

5.1 Le best practice nelle sentenze del "caso Vierika"

Tra le prime decisioni che hanno affrontato il tema dell'autonoma rilevanza giudiziaria delle best practice di Informatica forense, figurano quelle pronunciate sul c.d. caso Vierika, rispettivamente dal Tribunale, 21 luglio – 22 dicembre 2005 n. 1823 [211] e dalla Corte d'Appello di Bologna, 30 gennaio-27

[211] V. *http://www.penale.it/page.asp?mode=1&IDPag=182*; alcuni commenti in CATULLO F. G., Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova penale digitale. Profili sostanziali, in Diritto dell'Internet, 2006, n. 2; LUPARIA L., "Vierika": un'interessante pronuncia in materia di virus informatici e prova penale digitale. I Profili processuali, in Diritto dell'Internet, 2006, n. 2, p. 153; IANULARDO M., Processo "Vierika", c'è la sentenza, Punto Informatico, Anno X, n. 2460 ; SCARDINO P., Nota a Sentenza Trib. Penale di Bologna, I Sez. Giudice Monocratico, Sent. 21.07.05 in *http://www.computerlaw.it/entry.asp?ENTRY_ID=176*; v. la sentenza d'appello Corte d'appello di Bologna, sentenza 28 marzo 2008 in *http://www.informaticaforense.it/materiali2011/SentenzaVierika30012008.pdf*; per notazioni adesive alla sentenza, v. PESCI S., op.cit., *passim*.

marzo 2008 n. 369[212], all'esito di un processo a carico di due imputati per la violazione degli artt. 615 ter e quinquies, 81 cpv., 110 c.p., sostanzialmente per accesso abusivo a sistema informatico e telematico e danneggiamento informatico[213].

Al di là della specifica vicenda, tali decisioni suscitarono un vivace dibattito dottrinale, anche critico, sui principi in esse esposti in merito ad alcune questioni centrali dell'Informatica forense, e in particolare sulla rilevanza e necessità dell'adozione o meno di tecniche per la corretta acquisizione dei dati nell'ambito del procedimento, nonché sulla successiva necessità di verifica peritale.

Si tratta di un procedimento svoltosi per tutta la sua durata, dall'esordio dell'indagine sino alla sentenza definitiva di appello, nel periodo intercorso tra la sottoscrizione della Convenzione di Budapest e l'entrata in vigore a seguito di ratifica da parte del *quorum* di Paesi aderenti previsto dalla stessa.

Tuttavia, l'intero procedimento non sembra essere stato in alcun modo influenzato dai principi tecnici già espressi dalla Convenzione di Budapest costituente il primo riconoscimento normativo della necessità del corretto trattamento dei dati digitali a fini di indagine[214].

Ai fini della presente disamina, si ripercorreranno solo i punti salienti delle due sentenze, cercando di evidenziarne i punti critici.

5.1.1 La sentenza del Tribunale di Bologna sul caso Vierika

Gli argomenti di interesse svolti dalla sentenza di primo grado sono quelli versati nel § 4., dove si affronta "Il problema del metodo e degli accertamenti tecnici di parte:" *(...) La difesa dell'imputato sia nel corso dell'istruttoria, che nell'arringa finale ha reiteratamente posto in discussione la correttezza sia del metodo utilizzato dalla p.g. per estrarre i programmi dal computer del ******, che di quello applicato dalla p.g. e dalle società ****** s.p.a e ***** s.p.a. per individuare l'amministratore degli spazi web (uno dei quali contenente il secondo script del programma Vierika).*

---

[212] V. *http://www.penale.it/page.asp?mode=1&IDPag=610*, oppure in *http://www.intertraders.eu/pronunce/giudiziarie/CAppBo_369_30012008.pdf* .

[213] Il capo di imputazione così recitava:"(...) *imputati agli artt. 110 c.p., 615 ter e quinquies c.p., 81 cpv., poiché, in concorso tra loro, creando un "virus" (programma atto a danneggiare sistemi informatici) denominato vierika trasmesso in via informatica al provider "***" e tramite questo a circa 900 utilizzatori del provider, si introducevano nei sistemi informatici di tali utenti e acquisivano dati anche riservati contenuti nei loro personal computers - tra i quali indirizzari e-mail - a loro insaputa, inoltre per mezzo del virus danneggiavano i programmi contenuti nei personal computers raggiunti e ne pregiudicavano il corretto funzionamento. In Bologna nel corso del 2001*.".

[214] Per una diversa risoluzione circa la rilevanza dei principi della Convenzione di Budapest in relazione agli atti investigativi e di indagine compiuti in pendenza della sua ratifica, v. ad es. Trib. Vigevano, sent. 17 dicembre 2009, op.cit. p. 37 e ss..

Il tema è, in termini generali, di non poco momento e certamente dovrà essere affrontato in maniera approfondita anche dalla giurisprudenza, ma appare nella fattispecie in esame di secondario rilievo.(...)".

Il Tribunale riconosce espressamente la rilevanza del tema "*del metodo utilizzato dalla p.g. per estrarre i programmi dal computer del ******"* – che, peraltro, diventa centrale in un processo in cui tutto il giudizio si basa sull'attendibilità dei dati risultanti dai mezzi di prova, ma purtroppo, subito dopo, sembra abdicare all'intento ritenendo che "*(...) Occorre innanzitutto precisare che non è compito di questo Tribunale determinare un protocollo relativo alla procedure informatiche forensi, ma semmai verificare se il metodo utilizzato dalla p.g. nel caso in esame abbia concretamente alterato alcuni dei dati ricercati.*

In altre parole, non è permesso al Tribunale escludere a priori i risultati di una tecnica informatica utilizzata a fini forensi solo perché alcune fonti ritengono ve ne siano di più scientificamente corrette, in assenza della allegazione di fatti che suggeriscano che si possa essere astrattamente verificata nel caso concreto una qualsiasi forma di alterazione dei dati e senza che venga indicata la fase delle procedure durante la quale si ritiene essere avvenuta la possibile alterazione. (...)".

Quindi, non si può non rilevare come il Tribunale abbia sostanzialmente declinato l'obbligo di verificare autonomamente, ad esempio mediante l'espletamento di una perizia, la fondatezza scientifica del metodo utilizzato dalla polizia giudiziaria per acquisire i dati portati a giudizio e, di conseguenza, la loro effettiva rappresentatività, prima ancora di entrare nel merito della disamina della fattispecie. Il Tribunale ha invece ritenuto che avrebbe dovuto pronunciarsi solo se il metodo utilizzato dalla polizia giudiziaria avesse, nel caso concreto, alterato i dati portati al Tribunale. In altre parole, in assenza dell'allegazione di fatti che nel caso concreto potessero essere stati alterati alcuni dati e della mancata indicazione della fase delle procedure nella quale la possibile alterazione fosse potuta avvenire, al Tribunale non sarebbe permesso – e quindi sarebbe stato precluso – escludere i risultati di una tecnica informatica utilizzata a fini forensi e solo perché alcune fonti ritenevano che ve fossero stati di più scientificamente corrette.

In tale passo della decisione, il giudicante sembra spogliarsi del suo potere - dovere di vaglio critico dei risultati dell'istruttoria dibattimentale e in piena autonomia rispetto alle opzioni processuali delle parti, quali ad esempio la non contestazione del metodo scientifico posto alla base dell'acquisizione dei dati.

Inoltre, il *non liquet* sul preliminare giudizio di affidabilità scientifica dei dati sottoposti a giudizio diventa incomprensibile rispetto all'esigenza di basare il giudizio sulle informazioni tratte proprio dai dati sulla cui affidabilità il senso critico è rimasto un passo indietro.

Pertanto, avanti al problema scientifico della correttezza dei dati proposti al giudice, sarebbe stato sempre consentito, anzi doveroso, anche in assenza di contrarie allegazioni, valutare l'esistenza di tecniche scientificamente (più?) corrette, anche per superare "ogni ragionevole dubbio" che l'allegazione di parte possa essere inesatta in astratto e – trattandosi di leggi scientifiche – in concreto.

Quindi, il Tribunale avrebbe potuto riconoscere l'esistenza del problema non tanto di determinare "*un protocollo relativo alla procedure informatiche forensi",* quanto di riconoscere che, ove esistente, l'adozione o meno del protocollo avrebbe condizionato la scientificità dei risultati propostigli, e che tale verifica si sarebbe posta in posizione strumentale e necessaria rispetto al conseguente tema di "*semmai verificare se il metodo utilizzato dalla p.g. nel caso in esame abbia concretamente alterato alcuni dei dati ricercati"*.

La sentenza prosegue affermando che:"*(...) In termini generali, quando anche il metodo utilizzato dalla p.g. non dovesse ritenersi conforme alla migliore pratica scientifica, in difetto di prova di una alterazione concreta, conduce a risultati che sono, per il principio di cui all'art. 192 c.p.p., liberamente valutabili dal giudice alla luce del contesto probatorio complessivo (fermo restando che maggiore è la scientificità del metodo scelto, minori saranno i riscontri che il giudice è chiamato a considerare per ritenere attendibili gli esiti delle operazioni tecniche).(...)"*.

Probabilmente nemmeno tale principio sarebbe stato espresso in situazioni di giudizio basate su questioni scientifiche più usuali, quali ad esempio in relazione a dubbi di medicina legale, o se solo le problematiche dell'Informatica forense fossero entrate a far parte delle nozioni scientifiche notorie.

Difatti, è naturale che ove non si rispettino le migliori regole metodologiche derivanti dalla scienza di riferimento, l'alterazione del risultato è altamente probabile.

Rovesciando i termini dell'assunto criticato, è proprio in difetto di prova di alterazione concreta del risultato che il giudizio non può arrestarsi avanti alla prospettazione dell'esistenza di una migliore pratica scientifica, in quanto è proprio la verifica scientifica secondo la migliore pratica che verifica l'alterazione concreta.

Un paradosso può spiegare la critica a tale impostazione: se in un giudizio si proponesse, ad esempio, la ricostruzione di un reato basato sulla circostanza che una determinata sostanza è ustionante ad una certa temperatura, ad esempio a 100°, e una parte allegasse che il reato è stato commesso con la sostanza a 50°, e l'altra parte, per ignoranza, o disattenzione, o incapacità economica nel sostenere i costi di consulenza, o anche solo per calcolo, non rilevasse l'erroneità dell'assunto, secondo il principio della decisione in commento, al giudice sarebbe precluso escludere il dato corretto solo perché l'altra parte non

ha allegato la diversa ipotesi scientificamente corretta ? Ciò è in evidente contrasto con le norme sui poteri riconosciuti al giudice sulla valutazione della prova ex art. 192, sui poteri dispositivi di perizia ex art. 220 e finanche sui poteri ammissivi di nuove prove (art. 507). E l'esistenza di una pratica scientifica capace di verificare l'assunto e i dati allegati da una parte da porre alla base del giudizio, deve suscitare il dubbio che tali dati vadano preliminarmente verificati.

E proseguendo nella motivazione:*"(...) Facendo applicazione di tali principi nel caso in esame, deve evidenziarsi come la difesa si sia limitata ad allegare che i metodi utilizzati, non essendo conformi a quelli previsti dalla (supposta) migliore pratica scientifica, conducono a risultati che non possono essere ritenuti ab origine attendibili, senza peraltro allegare che nel caso concreto si è prodotta una qualche forma di alterazione o che avrebbe potuto prodursene alcuna, indicandone la possibile fonte, forma e fase di azione.(...)"*

Quindi,alla parte si rimprovera di non aver provato l'alterazione dei dati a valle del procedimento, e quindi l'inattendibilità dei risultati come effetto derivato, pur avendo la parte allegato l'esistenza di migliore pratica scientifica, nonché "...*la possibile fonte, forma e fase di azione*..." e quindi, a monte, le cause dell'alterazione. Insomma, in mancanza di prova contraria su cause ed effetto di una possibile alterazione, il Giudice ha ritenuto buono il dato prodotto dall'altra parte, esimendosi dalla verifica del metodo alla luce di migliori metodologie pur riconosciute come esistenti e nel caso concreto non adottate[215].

Fin qui la motivazione non è condivisibile nella misura in cui il compendio di dati posto alla base della dinamica da provare, non è stata preliminarmente verificata da un perito, a prescindere da quanto allegato dalle parti.

In particolare, il passo successivo della sentenza si rimarca come l'eccezione difensiva abbia riguardato solo la metodologia e non gli effetti della stessa sui reperti: *"(...) Non può, inoltre, non evidenziasi che la difesa si è limitata a porre suggestivamente la questione in ordine alla metodologia di sequestro del programma: non ha, invece, allegato la sua avvenuta alterazione in concreto, nonostante la disponibilità della versione da cui fu copiato il programma successivamente analizzato dalla p.g., rimasta nel possesso dell'imputato, le avrebbe permesso l'accertamento e l'allegazione di eventuali*

[215] Sul metodo controfattuale, è condivisibile l'opinione di MAZZA O., I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione, in Diritto Penale Contemporaneo, in *http://www.penalecontemporaneo.it/upload/1355813018-Mazza%20Milano.pdf*, il quale ha rilevato che "*Il recupero della stretta legalità processuale si impone anche di fronte alla deriva delle invalidità e delle relative sanzioni. Basta rammentare l'opera di erosione condotta dalla giurisprudenza in ordine alla categoria della inutilizzabilità che doveva essere il baluardo invalicabile posto a tutela dell'ortodossia probatoria e che, invece, si è trasformato in un simulacro di sanzione, attraverso distinzioni e sotto distinzioni, sanatorie collegate alle scelte del rito, per finire con la prova di resistenza che salva anche motivazioni che utilizzano prove inutilizzabili, trasformando la Cassazione in giudice di merito chiamato ad assumere una nuova decisione con logica contraffattuale (...)."* .

*anomalie. Non solo il disco rigido dell'indagato non fu sottoposto a sequestro, ma non risulta che vennero nemmeno rimossi i files trovati nel computer del *****: venne, infatti, sottoposta a sequestro una loro copia masterizzata sul cd, lasciando gli originali nella disponibilità dell'imputato (teste *** (...);".*

Nella decisione si rileva quindi che l'imputato, essendo rimasto in possesso della copia dei file, avrebbe potuto accertare e allegare eventuali anomalie rispetto alla copia acquisita. Se da un lato ciò è vero, è anche vero che non si discute del file rimasto in possesso all'imputato, bensì della copia acquisita al procedimento con modalità non verificate secondo le metodologie scientifiche, cosicché l'esame successivo, di tipo peritale, avrebbe dovuto essere effettuato sul file oggetto di allegazione e giudizio. In virtù di ciò, sarebbe stato onere del procedente, secondo l'ordinaria ripartizione dell'onere probatorio in capo all'accusa, dimostrare, rectius: provare, che quanto portato in giudizio costituiva un compendio di dati copia bit per bit fedele al compendio originario e non invece invertire l'onere della prova. Ma così non è stato.

*"(...) Appare in questa sede opportuno precisare che non si è ritenuto necessario disporre una perizia volta ad esplicare il funzionamento del programma: da una parte, infatti, i testi di p.g. (in particolare, ****) avevano le competenze tecniche necessarie per la decifrazione del codice, dall'altra si è ritenuto che la difesa non abbia in sostanza contestato i meccanismi di funzionamento del programma, come esplicitati dai testi escussi e sopra descritti al punto 2, nonostante si sia servita anche della collaborazione di un esperto informatico (per criticare e contestare, come di è detto, aspetti della deposizione del teste **** che non sono stai valorizzati in questa sede).*

*Deve inoltre sottolinearsi che gli elementi di conoscenza probatoria di cui dispone il Tribunale poggiano anche su produzioni documentali assunte con il consenso delle parti, come la cd. analisi tecnica redatta da **** ed allegata alla nota di p.g. del 15/5/01 e la documentazione relativa ai files sequestrati nel computer dell'imputato (all. 1 alla nota di p.g. Del 28/3/01). (...)".*

In tale passaggio della sentenza, invece, vengono rassegnati i motivi a giustificazione della decisione di non disporre la perizia sul compendio, ovvero la serie di passaggi dibattimentali che avrebbero avallato le considerazioni sul funzionamento del programma, e quindi:

- quanto riferito dai testi di polizia giudiziaria (in particolare, ****) in possesso di competenze tecniche necessarie per la decifrazione del codice. A tal proposito va rilevato come tale operazione di elevazione di una testimonianza al rango di perizia non potesse essere compiuta per almeno due motivi: che i testi avessero competenze specifiche è affermazione che non trova fondamento nella motivazione della sentenza. In secondo luogo, la Cassazione aveva già avuto modo di ritenere non legittima l'operazione di elevazione dell'accertamento

tecnico disposto dalla polizia giudiziaria al rango di perizia attraverso l'assunzione come teste dello stesso[216]. A fortiori, non può essere ritenuta legittima l'operazione con la quale la stessa polizia giudiziaria, che durante le indagini ha compiuto atti e accertamenti tecnici ripetibili, sui quali abbia svolto anche considerazioni tecniche - invitabilmente di parte, valutative e opinabili – assurga nel dibattimento a testimone su tali questioni, né le sue dichiarazioni possono essere utilizzate dal giudice. Anche su tale principio la Cassazione, al momento della decisione in esame, aveva già dichiarato che "*gli accertamenti tecnici possono trovare ingresso nel processo solo attraverso perizia o consulenza tecnica. Il teste che non sia stato incaricato (e la PG non lo è stata) di eseguire tali accertamenti secondo le leges artis, non può essere autorizzato dunque a riferire sue impressioni o convincimenti in proposito, né il giudice può porre tali dichiarazioni a fondamento della sua decisione"*[217];

- anche il rilievo dell'atteggiamento acquiescente della difesa che non avrebbe contestato i meccanismi di funzionamento del programma esplicitati dai testi di polizia giudiziaria, pur essendosi servita anche della collaborazione di un esperto informatico per criticare e contestare, non trova sufficiente giustificazione atteso che, come si è già detto, l'acquiescenza di parte, non esime il giudice dal chiedersi e verificare autonomamente se i dati acquisiti siano attendibili o meno;

- né possono sopperire altri elementi di conoscenza probatoria derivanti da documenti assunti con il consenso delle parti in quanto soggette alle precedenti critiche per le quali il consenso delle parti sui documenti non vincola né preclude la successiva ed autonoma ponderazione rimessa al giudice il quale, in sede di valutazione, avanti alle rappresentazioni derivanti da dati digitali ha l'obbligo di chiedersi preliminarmente quali procedure tecniche siano state osservate nella loro assunzione e quale sia il conseguente grado di affidabilità scientifica di quei dati; nel caso in cui non siano state osservate le procedure

---

[216] Secondo la Suprema Corte, (Cfr. Cass., Sez. III pen., Sent. 9 febbraio 2005 n. 4686 in Guida al Diritto, n. 18, 7 maggio 2005, n. 4686, p. 81 e ss., con nota POMANTE G., Finalmente una certezza su come agire nei riscontri elettronici e informatici, ibibem, pp. 83 e ss.) "*Il tribunale ha invece ritenuto di poter elevare l'accertamento tecnico disposto dalla polizia giudiziaria al rango di perizia attraverso l'assunzione come teste del tecnico utilizzato dalla stessa polizia giudiziaria. L'operazione tuttavia non può considerarsi legittima in quanto si risolve nell'attribuire ad un mezzo di prova la funzione che è propria di altro mezzo di prova, con una operazione di torsione dell'uno - la testimonianza chiamata a svolgere il compito proprio della perizia - che è certamente estranea al sistema, tanto più che, escluso il ricorso alla perizia, l'imputato è stato privato nel caso in esame della possibilità di svolgere le proprie difese in sede tecnica.*".

[217] Cfr. Cass., Sez. V, Sent. 07/12/2004 n. 5672, secondo la quale: "*gli accertamenti tecnici possono trovare ingresso nel processo solo attraverso perizia o consulenza tecnica. Il teste che non sia stato incaricato (e la PG non lo è stata) di eseguire tali accertamenti secondo le leges artis, non può essere autorizzato dunque a riferire sue impressioni o convincimenti in proposito, né il giudice può porre tali dichiarazioni a fondamento della sua decisione".*

tecnicamente corrette, deve essere sciolto il dubbio su quanto quelle rappresentazioni siano fedeli e rappresentative dei fatti oggetto di prova.

Ma sulla motivazione alla base della negazione della perizia il Tribunale così prosegue: "*Non ignora il Tribunale l'emergere di un orientamento della Suprema Corte, non consolidato, che sembrerebbe adombrare una qualche forma di cogenza della perizia, ogni qual volta la ricognizione del reato presupponga accertamenti di tipo tecnico (Cass. Pen., sez. III, n. 4686/05, Corsi; Cass. Pen., sez. VI, n. 34089/03, Bombino).*

Nella fattispecie in esame la difesa, nonostante abbia presentato quattro memorie ex art. 121 c.p.p., non ha prodotto alcun documento o parere che disconosca il funzionamento del worm nei suoi aspetti delineati al punto 2, gli unici valorizzati in questa sede: a fronte della descrizione del codice operata dalla p.g., non ha invero allegato un diverso funzionamento del programma, chiedendone l'accertamento ad opera di un perito. (...)."

Il Tribunale, quindi pur riconoscendo a suo carico l'obbligo di disporre la perizia anche solo per fugare il dubbio sugli aspetti tecnici da accertare quale presupposto del reato, ha quasi rimesso la responsabilità della mancata disposizione della perizia alla difesa che non avrebbe evidenziato un diverso funzionamento del meccanismo oggetto di processo, ma così facendo, si ripete, ha abdicato, se non a un obbligo, quantomeno ad uno scrupolo di verifica, al fine di sgomberare "ogni ragionevole dubbio" sugli aspetti tecnici della fattispecie.

La massima sopra riportata pone il problema della collocazione del punto di equilibrio tra libero convincimento del giudice e quello del contraddittorio tra le parti, che viene risolto con il seguente passaggio:

"(...) Sotto altro aspetto, il menzionato orientamento giurisprudenziale non consente un agevole coordinamento tra il principio del libero convincimento del giudice e quello del contraddittorio tra le parti.

Tradizionalmente, infatti, in forza del primo principio, il giudice può valorizzare un accertamento di parte che sia ritenuto esaustivo, corretto ed appropriato, senza necessità di accertamenti ulteriori."

Ma così decidendo, il Tribunale sopravvaluta la funzione del libero convincimento in quanto, sganciato dal sostrato fattuale costituito da una lunga sequela di principi tecnico-scientifici non verificati, si basa sulla prospettazione tecnica di una parte che, pertanto, è "di parte". Così agendo, però, la necessità di autonoma verifica tecnica recede rispetto alla scelta di dare per buono un *"accertamento di parte"* che in assenza di autonoma verifica tecnica peritale, viene ritenuto*"esaustivo, corretto ed appropriato, senza necessità di accertamenti ulteriori."*.

Avviandosi verso la chiusura sul punto, la motivazione prosegue affermando che:*"In tal caso, la tutela delle parti, siano esse pubbliche o private, si esplica in primo luogo a livello motivazionale, dovendo l'organo*

giudicante dare compiuta contezza dei risultati raggiunti: qualora ritenga di aderire alla prospettazione tecnica di una delle parti, non è peraltro gravato dell'obbligo di fornire autonoma dimostrazione dell'esattezza scientifica delle conclusioni raggiunte e dell'erroneità di tutte quelle espresse, dovendosi considerare sufficiente che egli dimostri di avere comunque valutato le conclusioni e le argomentazioni delle parti (cfr. su tale tematica Cass. Pen., sez. IV, n. 34379/04, Spapperi). (...)."

Quindi, per il giudicante, avendo aderito ad una delle due prospettazioni, non deve autonomamente dimostrare la correttezza dell'una e l'erroneità, purché dia conto di aver valutato le conclusioni e le argomentazioni di entrambe.

Ma anche tale obiter, per quanto ripreso dall'orientamento della Cassazione, pone la base di ogni evidente e stridente opinabilità dell'argomento allorquando verta su aspetti tecnici che solo il paradosso di cui sopra può evidenziare: al giudice non sarebbe richiesto dimostrare autonomamente che una certa sostanza sia ustionante a 50° invece che a 100° e che l'altra parte nulla abbia obiettato, perché il suo libero convincimento, accompagnato alle altre considerazioni e al contraddittorio svoltosi sul punto, gli consente di obliterare la richiesta di perizia e di optare per una delle due alternative (e quindi anche per quella erronea) purché abbia dato conto di aver preso in considerazione entrambe le opzioni.

Tale opzione, a mio parere, non esime alcun giudicante dallo stabilire quale sia la prospettazione tecnica corretta tra quelle emerse e ove si decidesse per una delle due possibilità senza un minimo di autonoma verifica tecnica, sia che si opti per quella corretta, sia, a maggior ragione, ove si opti per quella erronea, la scelta non sarebbe in entrambi i casi sorretta da una valutazione scientifica, per cui il libero convincimento risulterebbe comunque degradato ad apodittico arbitrio.

Infine, chiudendo: "*(...) Quanto al principio del contraddittorio, la parità di armi fra accusa e difesa si garantisce non solo con il controesame del teste esperto addotto da una delle parti, ma con la facoltà di dedurre testimoni e produrre documenti e memorie, anche avvalendosi di consulenti tecnici (per la considerazione che il diritto alla controprova non può, invece, avere ad oggetto l'espletamento di una perizia, essendo questo mezzo di prova di per sé neutro, cfr. Cass. Pen., sez. VI, n. 275/96, Tornabene) (...)".*

La chiusa costituisce l'ultima riproposizione del tema dell'omessa controprova sugli assunti tecnici da parte della difesa che, sul piano del contraddittorio, avrebbe reso superfluo la perizia.

Ma la perizia è un mezzo di prova tipica – mentre non lo è in sé la consulenza tecnica che, invece, è solo il contenuto di attività di parte che viene esposta al decidente nelle forme dell'esame del consulente tecnico.

Pertanto, la perizia richiesta dalla parte costituiva esercizio del diritto di difendersi provando nel dibattimento, luogo deputato alla formazione in contraddittorio della prova su questioni e attività tecniche alle quali la parte non aveva partecipato.

5.1.2 La sentenza d'appello sul caso Vierika

La sentenza pronunciata dalla Corte di Appello di Bologna sullo stesso caso[218] segnò la fine all'iter procedimentale del caso Vierika, giungendo ad una revisione di alcuni profili sostanziali e del livello sanzionatorio stabiliti nella sentenza di primo grado, ma non segnò alcun cambio di rotta in merito agli argomenti appena rassegnati, in merito ai quali osservava quanto segue:"*(...) Il giudice ha ritenuto esaustive le risultanze probatorie così sommariamente ora riassunte, senza ravvisare la necessità di accertamenti peritali, richiesti dalla difesa sin dalla fase predibattimentale, ed esplicati con memoria tecnica prodotta all'udienza del 23.6.04, giacché sostanzialmente la stessa difesa non aveva messo in discussione il funzionamento del programma come sopra descritto, ma ne aveva offerto in definitiva una lettura non penalmente rilevante.", ed* in merito alla doglianza relativa al mancato espletamento della perizia, la Corte rilevava altresì che: *"(...) Per altro profilo la sentenza di primo grado motivatamente si discostava da certo orientamento di legittimità che proprio in materia pare indicare necessaria la perizia, in ragione dell'accertamento di natura tecnica imprescindibile per la ricognizione delle fattispecie dei "computer's crimes"."*

Pertanto, la Corte, basandosi sullo stesso argomento della non contestazione del funzionamento del programma, ha sostanzialmente avallato la decisione del Tribunale di non svolgere accertamenti peritali, rilievo per il quale valgono gli argomenti già riportati a proposito del passo della sentenza di primo grado.

Proseguendo, nella motivazione la Corte di Appello sosteneva la sentenza appellata così motivando sui punti di nostro interesse:" *(...)* ***Sull'accertamento istruttorio.***

Nel corso del dibattimento di primo grado (udienza 23.9.04) con l'accordo delle parti, sono state acquisite ex art. 493, c.3, c.p.p., e dichiarate utilizzabili per la decisione le annotazioni di polizia giudiziaria (Guardia di Finanza) del 13.3.01, 19.3.01, 28.3.01, 15.5.01.

Già il rilievo dell'acquisizione con dichiarazione di utilizzabilità, avvenuta con l'espresso consenso della difesa, è esaustivo della infondatezza dei motivi di impugnazione in proposito, relativi alla natura di accertamento tecnico non ripetibile delle annotazioni. (...)".

---

[218] Corte di Appello Bologna, Sez. II pen., 30 gennaio-27 marzo 2008 n. 369, in *http://www.penale.it/page.asp?mode=1&IDPag=610*, oppure in *http://www.intertraders.eu/pronunce/giudiziarie/CAppBo_369_30012008.pdf*.

Anche la Corte, quindi, muovendo dal consenso espresso dalle parti sull'acquisizione delle annotazioni di polizia giudiziaria, ha negato la necessità di svolgere attività peritale sul contenuto tecnico delle annotazioni, così dando per scontato che esse fossero tecnicamente fondate e corrette. Ancora una volta, aiuta il paradosso per cui ove in tali annotazioni fossero state annotate considerazioni scientificamente o tecnicamente errate, come ad es. che l'acqua bolle a 50 gradi, il fatto stesso del consenso delle parti all'acquisizione avrebbe tramutato tali affermazioni erronee in affermazioni utilizzabili ai fini della decisione. Ora, proprio il paradosso rivela come non si possa disinvoltamente utilizzare – per quanto legittimamente acquisite – le notazioni tecniche senza poi sottoporle al vaglio peritale.

Inoltre, la Corte ripropone l'argomento secondo la quale le parti del processo non hanno mosso alcuna critica tecnica, come se la scelta delle parti avesse valore dispositivo sugli aspetti di natura scientifica, e come se tale atteggiamento fosse idoneo a rendere scientificamente corretto ciò che palesemente non è (o potrebbe non esserlo).

"*Va aggiunto che, comunque, l'attività di accertamento compiuta è stata ripercorsa, con analogo risultato di acquisizione di fonti di conoscenza del fatto, nel corso delle deposizioni testimoniali degli ufficiali di polizia giudiziaria A, B, C, (udienza 27.11.03), D e F, responsabile di Tiscali SpA per i rapporti con l'autorità giudiziaria (udienza 27.5.04).*

Anche dalle suddette deposizioni risulta univocamente ricostruibile, nel termini descritti nella sentenza impugnata e sopra riportati, il funzionamento del programma informatico "Vierika"; è d'obbligo rilevare che si è trattato di testimoni (ufficiali di polizia giudiziaria appartenenti al Nucleo Crimini Informatici, forniti di specifica preparazione e formazione in materia informatica) che, in forza della ricordata particolare preparazione tecnica, hanno risposto su fatti e circostanze concernenti la loro attività professionale d'indagine.

In tema di prova testimoniale, va aggiunto, il divieto di esprimere apprezzamenti personali non vale qualora il testimone sia persona particolarmente qualificata, in conseguenza della preparazione professionale, quando i fatti in ordine ai quali viene esaminato siano inerenti alla sua attività, in quanto, in tal caso, l'apprezzamento diventa inscindibile dal fatto, dal momento che quest'ultimo è stato necessariamente percepito attraverso il "filtro" delle conoscenze tecniche e professionali del teste (vedi Casso n. 12942 de116/01/2007).

Pertanto sia le annotazioni di polizia giudiziaria, anche nelle parti relative ad accertamenti ripetibili, per effetto del ricordato consenso dibattimentale, e sia le deposizioni sono pienamente utilizzabili quali fonti di conoscenza per la decisione.".

Anche su tale passo, e quindi sull'argomento della testimonianza degli ufficiali di polizia giudiziaria, vale quanto già osservato sopra riportando il precedente della Cassazione.

In merito poi alla questione delle fonti di prova e della necessità di verifica peritale, anche la sentenza di appello ha ripercorso gli argomenti della sentenza impugnata:*"Altra questione è, all'evidenza, costituita dalla esaustività ed attendibilità di dette fonti di conoscenza, questione connessa alla dedotta necessità di accertamento peritale, negato dal giudice di prime cure.*

Anche in proposito i motivi d'appello non paiono fondati.

La prima questione è relativa alla "correttezza" della acquisizione delle cosiddette "tracce informatiche" o delle prove documentali di natura informatica.

In proposito è necessario previamente precisare, richiamando espressamente quanto esattamente osservato nella sentenza impugnata, che non è compito del giudicante determinare una sorta di protocollo delle procedure informatiche forensi, ma solo verificare se nella fattispecie l'acquisizione probatoria sia fidefaciente, o se abbia subito alterazioni.

E nella specie, quanto alla tracce informatiche, i dati consegnati alla polizia giudiziaria dal provider Tiscali, relativi agli interventi di manutenzione ed amministrazione del sito con indirizzo http://web.tiscalinetit/krivojrog/vierika/Vindex.html ed alla individuazione dell'utente con username "Krivoj" sono stati confermati dalle dichiarazioni dello stesso XXXXX.

Questi ha espressamente e correttamente riconosciuto (vedi verbale esame delegato del 7.9.01) di aver realizzato "Vierika", di averlo diffuso, di aver creato il sito web con il nome "Krivoj".

Non si vede come possa esser messa in dubbio la fidefacienza di una risultanza documentale (tale è la traccia telematica, seppur necessitante di appositi strumenti per la fruibilità), coincidente con le ammissioni dello stesso imputato.

Identica considerazione va svolta in relazione alla prova costituita dal sequestro informatico eseguito presso l'abitazione di XXXXX; come ricordato nella circostanza fu questi stesso – così evitando il sequestro dell'hardware- ad indicare alla polizia giudiziaria i files dì programma rilevanti per l'accertamento, masterizzandone la copia ora in atti.

I rilievi mossi alla metodologia del sequestro informatico peraltro mai sono stati attinenti all'effettivo funzionamento e scopo del programma "Vierika", come accertato nella sentenza impugnata e sopra ripercorso, in realtà mai messi in discussione, neppure nelle memorie "tecniche" depositate dalla difesa; in esse, e del pari nei motivi di appello, mai è allegato o prospettato un funzionamento del programma diverso da quello sopra descritto. Le stesse richieste di perizia attengono ad aspetti non rilevanti per l'accertamento del

funzionamento di Vierika, quali le modalità di generazione e conservazione dei log (registri di collegamento), acquisiti presso il gestore Tiscali ed Infostrada (rilevanti per individuare le generalità di "Krivoj", fatto non in discussione, od il numero di accessi al sito infettante), ovvero concernono l'originale del codice sorgente del programma e pertanto (atteso che esso era nel 2001 nella memoria del computer dell'imputato) non più espletabili, oltre che non necessarie.

Nel difetto di effettive necessità istruttorie - secondo il parametro dell'assoluta necessità richiesto dall'art. 507 c.p.p.- volte a colmare lacune o contraddizioni nell'accertamento dei fatti, va confermata l'ordinanza del Tribunale di rigetto della richiesta di integrazione probatoria; per i medesimi motivi, riportati anche al disposto dell'art. 603 c.p.p., va disattesa la richiesta di assunzione della prova nel giudizio di appello. (...)".

Quindi il giudice del gravame, muovendo dalle premesse sostanzialmente aderenti alla decisione di primo grado, all'ultimo capoverso del passo in commento introduce l'argomento della riconducibilità della perizia all'assoluta necessità di integrazione istruttoria prevista dall'art. 507.

E tuttavia, va ancora una volta rilevato come nella fattispecie la perizia non solo costituisse un'attività di "integrazione probatoria", ma anche una fisiologica e imprescindibile esigenza di autonoma verifica da parte del giudice della correttezza e della valenza rappresentativa dei compendi informatici oltre alla verifica *banco judicis* della loro rilevanza penale, alla luce della giurisprudenza sopra indicata, tanto più che nel momento in cui veniva pronunciata al sentenza di appello, la Legge del 18 marzo 2008 n. 48 era stata già approvata e in procinto di essere pubblicata[219].

5.1.3 Considerazioni finali sulle sentenze del caso Vierika

La disamina delle parti delle due sentenze sul caso Vierika consentono di rilevare che se da un lato esse sono meritevoli per aver affrontato argomenti nuovi e ardui con una certa ampiezza e diffusività di argomenti, dall'altro annoverano opzioni decisionali non condivisibili rispetto ad altre possibili.

Infatti, in nessun punto si prospetta la necessità di verificare le procedure con le quali sono stati trattati i dati digitali oggetto di procedimento, né viene affermato l'autonomo obbligo del giudice di procedere alla verifica dell'acquisizione, trattamento e analisi dei dati digitali ad uso processuale, né in

[219] "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001 Tribunale di Bologna n. 1823 del 21 luglio – 22 dicembre 2005, Corte di Appello Bologna, Sez. II pen., 30 gennaio-27 marzo 2008 n. 369, L. 18 marzo 2008 n. 48, (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) è stata pubblicata nella Gazzetta Ufficiale n. 80 del 4 aprile 2008 – S.O. n. 79 ed è entrata in vigore il giorno successivo alla pubblicazione.

via preliminare né quale momento indefettibile per il superamento di "ogni ragionevole dubbio".

Ritengo che tali decisioni possono avere dalla loro parte solo un rapporto temporale parzialmente sfavorevole con i provvedimenti normativi in tema di prova digitale: difatti, per quanto le attività di indagine si siano svolte a cavallo della sottoscrizione della Convenzione di Budapest avvenuta il 23 novembre 2001 (il sequestro presso l'imputato è del marzo del 2001), la sentenza del Tribunale di Bologna n. 1823 è del 21 luglio – 22 dicembre 2005, per cui almeno in fase dibattimentale si sarebbe potuta disporre una verifica peritale delle attività svolte alla luce dei principi della Convenzione; parimenti, anche la Corte di Appello Bologna, Sez. II pen., 30 gennaio-27 marzo 2008 n. 369, sulla base dei principi della Convenzione firmata circa sette anni prima, avrebbe potuto assumere una diversa decisione e ammettere la verifica peritale, per quanto certamente non compulsata dalla L. 18 marzo 2008 n. 48, (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) che è stata approvata nel periodo intercorrente tra la lettura del dispositivo ed in deposito della motivazione, pubblicata solo successivamente a quest'ultima in Gazzetta Ufficiale n. 80 del 4 aprile 2008 – S.O. n. 79 ed entrata in vigore il giorno successivo alla pubblicazione.

Per quanto debba riconoscersi che tali sentenze siano state pronunciate in fase anteriore alla vigenza della L. 48/08 e relativamente a procedure di indagine realizzate in assenza di specifiche giuridiche e tecniche vincolanti, i principi scientifici sottesi agli elementi di prova digitale non potevano essere obliterati dalla *vacatio legis*.

Inoltre, tali decisioni rappresentano l'inizio delle difficoltà della giurisprudenza a confrontarsi con la necessità di sottoporre al preliminare vaglio tecnico sia le modalità con le quali sono stati assunti e trattati i dati digitali, sia gli aspetti tecnico-scientifico degli elementi di prova digitale, operazione da compiersi con l'ampio armamentario tecnico-scientifico dell'Informatica forense prima ancora di passare alla valutazione del merito e quindi delle informazioni e rappresentazioni desumibili dai dati.

Pertanto, le considerazioni di merito, sistematiche e di rapporto con le norme rilevanti, espresse nelle sentenze appena esaminate, a mio parere, non possono costituire principi orientatori per la giurisprudenza successiva su casi analoghi.

5.2 La sentenza del Tribunale di Vigevano sul caso Garlasco

E qui affrontiamo uno dei capitoli più interessanti dell'intera disamina.

I passi salienti della sentenza del Tribunale di Vigevano[220] che di seguito si ripercorreranno, a prescindere dall'esito processuale che ha avuto la vicenda, costituiscono, a mio parere, il contributo giurisprudenziale di merito più rilevante sulle questioni centrali dell'Informatica forense.

La decisione inizia ad esaminare le vicende del reperto informatico costituito dal computer sequestrato all'imputato dal quale furono tratti i dati che avrebbero fornito le informazioni sul comportamento del suo proprietario in prossimità dell'evento omicidiario:"*(...) In data **14 agosto 2007** Stasi Alberto consegnava spontaneamente alla polizia giudiziaria il proprio computer portatile (marca "Compaq").*

*Da quel momento fino al **29 agosto 2007**, quando il reperto informatico veniva consegnato ai consulenti tecnici del pubblico ministero che procedevano all'effettuazione delle copie forensi dello stesso, i carabinieri accedevano ripetutamente e scorrettamente (senza l'utilizzo, cioè delle necessarie tecniche forensi di indagine) alla quasi totalità del contenuto del computer.*

Peraltro, già nel verbale di polizia giudiziaria datato 29 agosto 2007 i militari indicavano alcune delle operazioni condotte sul personal computer di Stasi.

In realtà le metodologicamente scorrette attività espletate su tale fonte di prova sono risultate, all'esito dei successivi accertamenti tecnici, ancora più consistenti: sette (e non cinque come riferito) accessi al personal computer di Alberto Stasi; non corretta indicazione dell'avvenuta installazione ed utilizzo di diverse periferiche USB (oltre a quella correttamente indicata); non corretta indicazione dell'avvenuto accesso al disco esterno in uso ad Alberto Stasi; non corretta indicazione di accessi multipli al file della tesi di laurea in vari percorsi di memorizzazione dello stesso: si vedano sul punto i rilievi del collegio peritale tecnico/informatico (ing. Porta e dott. Occhetti).

Il complesso di queste alterazioni veniva rilevato anche dai consulenti tecnici del pubblico ministero (i Ris di Parma) nella loro successiva analisi. Pur tenendo conto di quanto sopra, i Ris, nella loro relazione tecnica e successive integrazioni e chiarimenti, concludevano sostanzialmente nel senso che il giorno 13 agosto 2007 il computer portatile di Alberto Stasi veniva acceso alle ore 9.36; quindi venivano aperte delle fotografie digitali fino alle ore 9.57 e dopo le ore 10.17 non sarebbero presenti tracce informatiche che comportino la presenza attiva di un utente che interagisce con il PC. (...).".

Correttamente il Tribunale antepone l'esito delle valutazioni dei consulenti di parte e dei periti nominati per la verifica tecnica, allo stesso vaglio di merito dei dati rilevati dal repert. In altre parole, ritenuto che nei 15 giorni successivi al sequestro del dispositivo "(...*) i carabinieri accedevano ripetutamente e scorrettamente (senza l'utilizzo, cioè delle necessarie tecniche forensi di*

[220] V. Trib. Vigevano, sent. 17 dicembre 2009, op.cit., pp. 37-63.

indagine) alla quasi totalità del contenuto del computer(...)" il Tribunale correttamente si chiede – quale presupposto di ogni altra valutazione - se i dati presenti sul reperto sia affidabili o meno.

A tal proposito va altresì considerato che si tratta di valutare i dati dai quali trarre informazioni rilevanti per tutte le parti del procedimento e, in particolare, per la difesa dell'imputato, atteso che: "(...) *Il consulente tecnico della difesa, nel merito, evidenziava che in realtà il file della tesi era stato aperto alle ore 10.17 e che quella mattina erano state ivi scritte e memorizzate due pagine della tesi di laurea. In presenza tuttavia delle alterazioni al contenuto informativo della fonte di prova a causa degli accessi scorretti dei carabinieri e della ritenuta conseguente impossibilità di provare con certezza quanto sopra rilevato, la difesa dell'imputato eccepiva l'inutilizzabilità come fonte di prova del contenuto del computer portatile in parola. In presenza tuttavia delle alterazioni al contenuto informativo della fonte di prova a causa degli accessi scorretti dei carabinieri e della ritenuta conseguente impossibilità di provare con certezza quanto sopra rilevato, la difesa dell'imputato eccepiva l'inutilizzabilità come fonte di prova del contenuto del computer portatile in parola. Questo Tribunale respingeva tale eccezione mediante l'ordinanza datata 17 marzo 2009.*

Alcune delle questioni colà trattate devono essere qui riassuntivamente richiamate. (...)".

Questa circostanza, quindi, conferma uno degli assunti generali e basilari dell'Informatica forense, ovvero che i dati digitali maltrattati impediscono alle parti di trarre informazioni utili al processo, e ciò in grave violazione delle prerogative sia degli organi di accusa che della difesa, oltre al rischio di dover ritenere inutilizzabili gli stessi dati.

Difatti, la sentenza prosegue proprio con le motivazioni relative ad una questione spesso ricorrente in tali contesti: i dati digitali sequestrati, ove maltrattati, possono essere dichiarati inutilizzabili? Il Tribunale dà una risposta negativa, non condivisibile per i motivi che si diranno, ma motivandola con un iter logico argomentativo che, allo stato attuale, rappresenta la migliore sintesi delle problematiche dell'Informatica forense che, ritengo, sia dato leggere in un'argomentazione giurisprudenziale:

"(...) Il documento informatico è connotato da un'intrinseca caratteristica di fragilità: nel senso che le tracce elettroniche sono facilmente alterabili, danneggiabili e cancellabili.

Per questa ragione, può essere arduo (e ciò anche a prescindere da ipotetiche manipolazioni dolose ma perfino da eventuali comportamenti colposi posti in essere da chi interviene su di esso) conservare un documento informatico inalterato, in modo da assicurare che la prova sia autentica e genuina.

Di qui la necessità di adottare particolari cautele, quali l'adozione di copie di hard disk conformi all'originale, che vengono rese non modificabili mediante appositi procedimenti tecnici. (...)".

Il Tribunale apre sull'assunto della peculiarità fisico-scientifica dei dati (i.e. "tracce elettroniche", secondo l'espressione usata in gergo investigativo per indicare i dati digitali dei dispositivi individuati sulla scena del delitto) e del rischio per la loro "fragilità" in quanto alterabili, modificabili, cancellabili a seguito di manovre volontarie o semplicemente maldestre.

E proseguendo:" (…) *Al fine di ampliare la possibile valenza dimostrativa della prova informatica (c.d. digital evidence) superando alcune incertezze interpretative connesse ad istituti processuali disciplinati dal legislatore prima del consolidarsi sotto il profilo socio/culturale e scientifico dell'era informatica e nel contempo positivizzare questa imprescindibile esigenza (già ben conosciuta nella prassi) legata alla genuina acquisizione del documento informativo e alla successiva attendibile valutazione della prova informatica, la recente legge 18 marzo 2008 n. 48 (in esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica) ha, fra l'altro, modificato la disciplina di alcuni mezzi di ricerca della prova nel senso di estendere espressamente l'oggetto di questi anche ai sistemi informatici e telematici e ha prescritto, nel contempo, la necessità che il soggetto operante adotti idonee cautele tecniche che assicurino la conservazione del documento informatico e ne impediscano l'alterazione. Si veda l'art. 244 cpv c.p.p. in materia di ispezioni; gli artt. 247 e 248 c.p.p. in materia di perquisizioni; gli artt. 254, 254 bis, 256, 259, 260 c.p.p. in materia di sequestri; l'art. 352 c.p.p. in tema di perquisizione nei casi particolari ivi previsti; l'art. 354 c.p.p. in tema di accertamenti urgenti. L'art. 259 comma II c.p.p. prescrive, inoltre, che «quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria". (...)".*

Il Tribunale dà quindi atto che il fine dell'Informatica forense, quello di riconoscere e preservare tutta la potenzialità informativa dei dati, integra e affidabile[221] Affinché possa valere come mezzo di prova informatica *("c.d. digital evidence"),* fosse già conosciuto - e aggiungerei, perseguito – prima ancora che la legge 18 marzo 2008 n. 48 che ha ratificato la Convenzione del Consiglio d'Europa sulla criminalità informatica recepisse i principi riguardanti il corretto trattamento dei dati oggetto di accertamento urgente da parte della polizia giudiziaria[222].

[221] Cfr. MAIOLI C., Dar voce alle prove: elementi di Informatica forense, op.cit.
[222] Art. 354 "*Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro - Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato [253 1] siano*

E prosegue: *"(...) Ora, nel caso di specie l'attività di polizia giudiziaria presenta caratteristiche di sommarietà e di mera ricognizione di dati potenzialmente utili ai fini della immediata prosecuzione delle indagini tale da non poter essere correttamente inquadrata nell'ambito né della perquisizione, funzionale ad un sequestro che peraltro formalmente non c'è stato in quanto il computer è stato spontaneamente consegnato alla polizia giudiziaria, né dell'ispezione di cui all'art. 244 c.p.p. (in difetto sia dell'elemento formale del decreto autorizzativo sia dell'elemento sostanziale di un'"operazione tecnica" che richiama un concetto di controllo più penetrante e tecnicamente qualificato di quello effettivamente posto in essere).*

Correlato a quanto appena evidenziato, bisogna porsi, inoltre, la questione se le operazioni in parola possano, comunque, rientrare nella nozione processual/penalistica di accertamento tecnico ai sensi degli artt. 359/360 c.p.p.. La risposta è negativa.

Infatti, per configurare tale attività come accertamento tecnico ai sensi degli artt. 359 e 360 c.p.p., sarebbe stato necessario che la stessa fosse consistita in un'analisi completa ed approfondita del documento informatico in sequestro sulla base di un quesito posto dal pubblico ministero, che i soggetti procedenti possedessero le competenze tecniche al fine di svolgere gli accertamenti suddetti e che gli stessi alla fine avessero dato conto, mediante argomentata relazione scritta, dei risultati raggiunti.

In realtà, si è trattato di un'attività compiuta da ufficiali di polizia giudiziaria non esperti in materia, che hanno proceduto senza un previo quesito e che al termine hanno redatto solo un verbale in cui hanno riportato la data del compimento dei suddetti indicati atti. Dunque, siamo dinnanzi ad atti di polizia giudiziaria che rientrano, invero, nell'ambito del combinato disposto degli artt. 55 e 348 c.p.p. (attività finalizzata a raccogliere ogni elemento utile alla ricostruzione del fatto e all'individuazione del colpevole) e non integrano la fattispecie dei veri e propri accertamenti tecnici di cui agli artt. 359 e 360 c.p.p..(...)".

---

conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero (1).

2. Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità. Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti [att. 113].

3. Se ricorrono i presupposti previsti dal comma 2, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sulle persone diversi dalla ispezione personale [245].

Il Tribunale esclude che gli atti compiuti dalla polizia giudiziaria possano essere qualificabili come accertamenti tecnici in quanto non furono compiuti accertamenti approfonditi del documento informatico sulla base di un quesito posto dal pubblico ministero né gli operatori avevano le relative competenze, né questi relazionarono sui risultati dell'attività. Si sarebbe trattato invece di attività rientrati tra gli accertamenti urgenti. Nonostante tali assunti, si può invece osservare che la polizia giudiziaria ha di fatto realizzato tale attività e l'eventuale carenza di direttive delle operazioni tecniche, ad indagini inoltrate, delle due, accrescerebbe gli ampi dubbi e perplessità sulla corretta conduzione tecnico-giuridica del procedimento.

Prosegue la sentenza: *"(...) Ciò posto, non vi è alcun dubbio, tuttavia, che le condotte poste in essere sul computer da parte della polizia giudiziaria, sebbene superficiali, dovessero, proprio per la intrinseca fragilità del contenuto del documento informatico di cui sopra, essere eventualmente svolte (se proprio necessario) con l'assistenza di ausiliari tecnici che avrebbero messo in atto le necessarie preventive cautele tecniche atte ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso provvedendo, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicurasse la conformità della copia all'originale e la sua immodificabilità.*

Si deve, dunque, ritenere che questa preliminare e sommaria attività investigativa è stata posta in essere secondo una metodologia sicuramente scorretta, disattendendo i protocolli già invalsi in materia (anche prima dell'entrata in vigore della legge citata) venendo, quindi, a costituire una causa di potenziale alterazione e dispersione del contenuto del documento informatico. (...)".

Il Tribunale mette quindi in evidenza il principio della fragilità del contenuto dei documenti informatici e quindi dei bit, nonchè la conseguente necessità di prevenire ed evitare l'alterazione e la dispersione dei dati adottando le tecniche scientifiche messe a punto e già operanti prima della L. 48/08 come normale metodologia scientifica di trattamento dei dati a fini processuali.

La sentenza prosegue nell'analisi delle motivazioni soggettive che avrebbero portato agli errori di gestione dei reperti informatici escludendo la malafede degli operatori:"(...) *Non emergendo ragioni (e nemmeno la difesa dell'imputato, peraltro, prospettava tale evenienza) per affermare che in tali accessi ed operazioni sommarie da parte della polizia giudiziaria vi fosse stato un dolo di inquinamento probatorio di qualsiasi genere, siamo ragionevolmente di fronte ad errori di metodo compiuti, salva prova contraria, in totale buona fede.(...)".*

Attestata la portata degli errori, il Tribunale prosegue*:"(...) Ciò comporta due conseguenze di fondo.*

La prima: la questione se i risultati conseguiti correttamente (secondo il profilo metodologico) dai consulenti del pubblico ministero e della parte civile siano comunque ragionevolmente attendibili (ed in che misura) e/o se alcuni dati ed informazioni siano stati, invece, irrimediabilmente persi a causa, appunto, di tale iniziale errore metodologico da parte della polizia giudiziaria ha una valenza oggettiva. Nel senso che vi è il pericolo (e qui l'eccezione processuale della difesa dell'imputato assume una valenza di merito degna della massima attenzione) che Alberto Stasi non riesca più a provare il proprio alibi che invece, se fossero state salvaguardate al massimo l'integrità e genuinità del documento informatico, sarebbe riuscito per ipotesi a conseguire.

Ma vi è ugualmente il pericolo, all'opposto, che il contestato (dalla difesa dell'imputato) grado di attendibilità del risultato (emerso dalla consulenza tecnico/informatica dei Ris di Parma) sulla falsità dell'alibi offerto dall'imputato (come indizio a carico dello stesso che andrebbe valutato alla luce dell'art. 192 c.p.p.) possa essere (in tutto o in parte) inficiato, appunto, dagli accessi ed operazioni sommarie di cui sopra.

Dunque, una valenza oggettiva, appunto, in quanto emerge, in ultima istanza, il pericolo di un pregiudizio al fondamentale valore neutro dell'accertamento della verità. Sulla base di queste considerazioni, una volta che l'imputato chiedeva di essere giudicato con le forme del rito abbreviato, affidare ad autorevoli professionisti del settore un accertamento peritale in materia diventava assolutamente necessario ai fini della decisione.".

Nel passo appena riportato, il Tribunale evidenzia come gli effetti del maltrattamento dei dati informatici, ovvero il pregiudizio che ciascuna parte subisce riguardo alle proprie prerogative processuali, si verifichino sia per cui la difesa dell'imputato, che lamenta la distruzione di elementi di prova a sostegno del proprio alibi, sia per la difesa della parte civile che potrebbe essere pregiudicata dalla non verificabilità dell'alibi. È questo l'esempio paradigmatico per comprendere lo scopo ultimo intorno al quale ruotano i principi e il metodo dell'Informatica forense: proteggere l'integrità dei dati informatici per proteggerne il valore informativo Affinché ciascuna parte del procedimento possa svolgere le proprie prerogative all'interno del procedimento. Non è questa una concezione neutrale, ma è una concezione dichiaratamente di parte rivolta alla realizzazione degli ideali di Verità e di Giustizia che devono essere realizzati nell'ambito di un processo. E in tale frangente, il Tribunale, a difesa di una propria autonomia e terzietà anche sostanziale rispetto alle posizioni delle parti, riconosce l'essenzialità della preventiva indagine peritale sui dati quale risposta alla necessità di accertare l'affidabilità del valore rappresentativo degli stessi.

Prosegue il Tribunale: "(...) *Ebbene, il collegio peritale (ing. Porta e dott. Occhetti) evidenziava che le condotte scorrette di accesso da parte dei carabinieri hanno determinato la sottrazione di contenuto informativo con*

riferimento al personal computer di Alberto Stasi pari al 73,8% dei files visibili (oltre 56.000) con riscontrati accessi su oltre 39.000 files, interventi di accesso su oltre 1500 files e creazione di oltre 500 files.

Insomma interventi che hanno prodotto effetti devastanti in rapporto all'integrità complessiva dei supporti informatici (in questi termini si esprime il collegio peritale).(...)".

Sulla base delle verifiche peritali, il Tribunale definisce "devastanti" gli effetti dei ripetuti accessi ai dati sull'integrità degli stessi, tali da aver modificato quasi i ¾ dei dati archiviati nel dispositivo.

E il Tribunale così prosegue: *"(...) Queste alterazioni indotte da una situazione di radicale confusione nella gestione e conservazione di una così rilevante quanto fragile fonte di prova da parte degli inquirenti nella prima fase delle indagini ha comportato, in primo luogo, il più che grave rischio che ulteriori stati di alterazione rimuovessero definitivamente le risultanze conservate ancora nella memoria complessiva del computer. In secondo luogo, gli accessi in questione hanno comunque prodotto degli effetti metastatici rispetto all'esigenza di corretta e complessiva ricostruzione degli eventi temporali e delle attività concernenti l'utilizzo del personal computer portatile nelle giornate del 12 e 13 agosto 2007. Rispetto dunque ad altre questioni probatoriamente rilevanti (come, ad esempio, il movente/occasione dell'omicidio su cui torneremo nel prosieguo) non è più possibile esprimere delle valutazioni certe né in un senso né nell'altro: in questo ambito, il danno irreparabile prodotto dagli inquirenti attiene proprio all'accertamento della verità processuale. (...)".*

La conclusione più rilevante ai fine della disamina è l'attestazione del danno irreparabile arrecato ai dati contenuti nel dispositivo e alle informazioni da essi desumibili, in pregiudizio di entrambe le parti – e aggiungo, per la funzione svolta dalla pubblica accusa e dal giudicante in ogni stato e grado del procedimento - nonché per la Verità stessa.

La sentenza prosegue con la disamina dell'alibi dell'imputato effettuata dai periti muovendo dall'analisi di altre due versioni del documento al quale stava lavorando l'imputato: "(…) *Con riferimento all'alibi informatico, il collegio peritale (ing. Porta e dott. Occhetti) riusciva comunque a ricostruire le attività compiute da Stasi Alberto quella mattina sul proprio computer portatile.*

Ciò sulla base dei seguenti passaggi.

I periti avevano a disposizione in primo luogo la versione della tesi di laurea del 12 agosto 2007 alle ore 19.00 quando si verificava un crash del sistema che consentiva di rinvenire i files temporanei che attestano il lavoro pomeridiano alla tesi di laurea. Quindi una versione del 12 agosto alle ore 19.19 acquisita durante le operazioni peritali mediante la produzione di una chiavetta da parte dei consulenti tecnici dell'imputato. Questa versione della tesi riprodotta su tale supporto non presenta, come argomentato dal collegio

peritale in udienza, delle anomalie e quindi può essere considerata come una versione della tesi che si colloca attendibilmente fra quella del crash e quella del 14 agosto 2007. Del resto, è ragionevole la condotta di Stasi che, avvenuto il crash, decide di cautelarsi salvando il proprio lavoro su una chiavetta esterna temendo un eventuale successivo disguido (anomalia bloccante che poteva generare ulteriori crash) del sistema operativo.

Infine, la versione della tesi al momento del 14 agosto 2007 quando Stasi Alberto, avendo consegnato agli inquirenti il proprio computer, si presentava presso la caserma chiedendo loro di poter copiare la propria tesi di laurea su una pen drive.

Dunque, schematicamente possiamo ricostruire il lavoro alla tesi nelle seguenti fasi: alle ore 19.00 avviene il crash di sistema (sul sistema si cristallizzavano tutti i files temporanei attivi in quel momento non essendo avvenuta una chiusura normale dell'applicativo word), quindi vi è il salvataggio della tesi sulla chiavetta esterna. Da quel momento il sistema rimane praticamente inattivo fino alle ore 21.28 circa quando viene riaperto il file della tesi fino alle ore 21.59; alle ore 22.14 viene ripreso il lavoro alla tesi fino alle 00.10 quando viene chiuso il file di Word e messo in standby il computer.

La circostanza che l'attività sulla tesi di laurea sia stata eseguita anche successivamente al crash era, del resto, stata dimostrata dalla consulenza della parte civile (ing. Reale) che aveva evidenziato per la sera del giorno 12 l'inserimento nel dizionario personalizzato dell'utente informatico di due parole nuove "inerentemente" e "Garbarino".

Dunque, se Stasi aveva lavorato alla tesi anche la sera del giorno 12 era necessario aspettarsi che vi fossero dei files temporanei che attestassero il lavoro della tesi in quel lasso temporale: la circostanza che, invece, gli stessi mancassero era indice inequivocabile di come l'equazione sostenuta dai consulenti tecnici del pubblico ministero -mancanza di files temporanei uguale provata assenza di attività sul computer per la mattina del 13 agosto- fosse logicamente e tecnicamente scorretta.

Partendo da questo dubbio di fondo e tenuto conto della grave anomalia rappresentata dalle alterazioni del contenuto informativo dovute agli accessi dei carabinieri che ben potevano avere determinato la cancellazione delle normali evidenze presenti all'interno del sistema operativo, il collegio peritale (con la collaborazione dei consulenti tecnici delle parti) ricercava delle particolari informazioni che si trovano fuori del sistema operativo (i c.d. metadati).

Questa ricerca dava esito positivo: questi metadati ed il loro contenuto attestano con certezza (e questo è un'evidenza probatoria non contestata dalle parti) l'interazione diretta e sostanzialmente continuativa dell'utente con il computer dalle ore 10.17 fino alle ore 12.20 del giorno 13 agosto.

Dunque, possiamo dire con certezza che Stasi attivava il proprio personal computer alle ore 9.35 ed eseguiva le seguenti operazioni: accedeva al sistema con la digitazione della propria password;

quindi alle ore 9.38 (circa) visualizzava una prima immagine di natura erotico/pornografica; alle ore 9.39 (circa) una successiva immagine pornografica; alle ore 9.41 (circa) visualizzava due immagini dello stesso tenore di cui sopra; alle 9.47 (circa) visualizzava un'altra immagine di natura erotico/pornografica. Bisogna precisare che dalle evidenze riscontrate sul registro di windos alle ore 9.50 vengono aperte delle cartelle; quindi alle ore 9.50 visualizzava una nuova immagine di natura erotica/pornografica; alle ore 9.57 visualizzava una nuova immagine di natura erotica/pornografica;

alle 10.05 apriva la copertina di un filmato hard e poi utilizzava un programma di modifica delle immagini alle ore 10.07; poi alle 10.17 apriva la tesi.

Da quel momento sono state appunto recuperate le evidenze di un'attività sostanzialmente continua di videoscrittura sulla tesi di laurea dalle ore 10.17 fino alle ore 12.20 (quando il computer veniva messo in standby lasciando il file di word aperto).

Il collegio peritale ha quindi evidenziato che le informazioni rinvenute consentono di affermare che l'attività svolta sulla tesi è stata progressiva e quindi i salvataggi sono stati eseguiti in presenza di un testo che si è accresciuto progressivamente (la condizione di modifica del file è condizione essenziale per l'esecuzione del salvataggio che altrimenti non avviene): infatti, sia il numero di caratteri che risultano all'interno del documento sia l'andamento delle parole che tende ad aumentare progressivamente ad ogni revisione convergono verso questo risultato (si vedano sul punto i grafici a pag. 54 e 55 della relazione peritale).

Più specificamente possiamo dire che la sera del 12 e la mattina del 13 agosto Alberto Stasi procedeva ad un lavoro sulla sezione della tesi intitolata "credito d'imposta per i redditi prodotti all'estero": lo stesso è consistito in una complessiva scrittura di nuovo testo e in una revisione di parti di testo relative alle parti di testo già scritto, ad esempio con correzione di alcuni termini, introduzione di riferimenti normativi specifici, elaborazioni su dei calcoli effettuati, eliminazione di alcune parti ed aggiunta, appunto, di nuove parti di testo.

Il collegio peritale, facendo uso dei c.d. strumenti informatici di analisi del testo e considerando che il lavoro svolto la sera del giorno 12 e la mattina del giorno 13 è risultato complessivamente omogeneo non evidenziando anomalie di comportamento informatico, concludeva nel senso che "l'introduzione di revisioni specifiche relative in parte a riferimenti temporali e documentali e in parte a riflessioni in materia distribuite in tutto il corpo del testo sono compatibili con un'attività di concreta concentrazione mentale".

Con riferimento, quindi, al rapporto di tali evidenze informatiche con la questione della presenza effettiva di Alberto Stasi nella propria abitazione, bisogna risolvere due questioni.

La prima è relativa alla natura "portatile" del computer in parola e quindi all'ipotesi che tutta o parte dell'attività informatica rilevata il giorno 13 agosto possa essere stata svolta da Stasi in luoghi differenti dalla propria abitazione.

Questa ipotesi è da escludere con ragionevole certezza nel caso concreto.

In primo luogo, la riscontrata difettosità del cavo di alimentazione e le modeste prestazioni della batteria (che consentiva un'autonomia d'uso del personal computer per circa 2 ore) inducono convergentemente a considerare che il notebook non potesse essere collocato e utilizzato in luoghi non idonei per svolgere attività di significativa durata.

In secondo luogo, alle ore 9.55 Stasi riceveva sul telefono fisso dell'abitazione la chiamata della madre Ligabò Elisabetta della durata di 21 secondi: in concomitanza a tale evento il personal computer è risultato attivo ed in stato d'uso da parte di Stasi (attività di visualizzazione di immagini). Dal quel momento in poi non emergono circostanze che possano far ipotizzare spostamenti significativi del personal computer dalla posizione nella quale era stato collocato: spegnimenti, sospensioni, standby etc… (si veda sul punto la relazione peritale a pag. 100).

In terzo luogo, la sopra rilevata attività continuativa riscontrata sul personal computer fino alle ore 12.20 non permette ragionevolmente di configurare eventi di spostamento dell'elaboratore elettronico rispetto alla posizione nella quale era stato collocato all'atto della sua riattivazione e al momento della ricezione della chiamata telefonica di cui sopra. (...)".

Il brano appena ripercorso, nella sua articolata complessità, mostra un ulteriore motivo di correttezza nell'approccio alle metodologie di Informatica forense, i cui risultati non sono mai autoreferenziali ma vanno sempre incrociati e verificati con le altre informazioni derivanti da altre fonti di informazioni rinvenute nel contesto ambientale nel quale vengono svolte le investigazioni.

Quindi, le informazioni derivanti dai dati digitali sono state incrociate, ad esempio, con quelle derivanti dai dati di un diverso sistema telefonico per verificare se siano congruenti o meno.

Proseguendo, il Tribunale correttamente concentra l'attenzione sulla questione dell'attendibilità dei dati relativi agli orari dei file rispetto a quelli del dispositivo, per verificarne sia l'attendibilità relativa che quella assoluta:"(...) *La seconda questione attiene all'ipotesi che i tempi associati alle attività informatiche rilevate sul PC portatile in uso all'attuale imputato possano non essere corrispondenti all'ora reale a seguito di un'attività volontaria di alterazione dei riferimenti temporali di sistema (modifica di data ed ora).*

A seguito degli accertamenti peritali sul punto, l'unica astratta possibilità fa riferimento all'avvio di un sistema operativo esterno.

Tale ipotesi, tuttavia, è da escludere in concreto con ragionevole certezza.

Come convincentemente argomentato dal collegio peritale, bisogna infatti considerare che l'operazione descritta avrebbe innanzi tutto richiesto capacità e conoscenze informatiche superiori a quelle accertate in capo ad Alberto Stasi.

In secondo luogo, se un'operazione del genere fosse stata realmente condotta, ciò avrebbe implicato due scenari distinti: il primo relativo al fatto che l'operazione sia avvenuta in epoca precedente all'avvio del personal computer in data 13 agosto 2007 (ad esempio nel corso della notte del 13 agosto); il secondo relativo al fatto che l'operazione sia avvenuta la mattina del 13 agosto dopo le ore 9.36.

Questa operazione avrebbe presupposto una necessaria meticolosa sincronizzazione temporale delle diverse attività, viceversa si sarebbero riscontrati sfasamenti di orario all'atto del riavvio del PC.

Infatti, per entrambe le ipotesi tutta l'attività di lavoro sarebbe dovuta essere programmata in modo da rispettare le pause di attività informatica indotte dagli eventi esterni all'attività informatica stessa quali le telefonate effettuate e ricevute da Stasi nella mattina del 13 agosto 2007: telefonate che si inseriscano, appunto, perfettamente nella loro tempistica con l'attività di lavoro sulla tesi e con i relativi riscontri di data ed ora rinvenuti sul personal computer.

Infine, come rilevato ancora dal collegio peritale, una attività di questo tipo appare del tutto inverosimile nella sua attuazione anche in considerazione che non vi era modo per Alberto Stasi di verificare il risultato effettivo di una simile alterazione in termini di credibilità e di assenza di tracce informatiche in grado di palesare le alterazioni di orario in quanto nell'ipotesi dell'alterazione "notturna" il PC non poteva più essere avviato per non inficiare e compromettere l'esito dell'alterazione; nell'ipotesi dell'alterazione "mattutina" i tempi con i quali sarebbe stata condotta l'alterazione non consentivano alcuna verifica.

Dunque, non si può che concludere con elevato grado di credibilità razionale che le attività informatiche rinvenute sul PC portatile in uso a Stasi Alberto in data 13 agosto 2007 sono effettivamente corrispondenti all'ora reale e pertanto si sono verificate in corrispondenza degli orari rilevati.

Se combiniamo queste evidenze informatiche con i riscontri telefonici e quindi con la circostanza per cui le telefonate "anonime" si incastrano perfettamente nell'ambito temporale delle rilevate pause nell'attività di scrittura alla tesi di laurea, è ragionevolmente certo -e non più solo altamente probabile alla luce del ragionamento induttivo del collegio peritale sopra esposto- che l'utenza anonima dalla quale provengono le chiamate senza risposta ricevute dal cellulare di Poggi Chiara la mattina del 13 agosto è l'utenza fissa relativa all'abitazione della famiglia Stasi.(...)".

Sulla base di tali accertamenti, il Tribunale costituisce una griglia cronologica sulla quale verifica la compatibilità degli altri avvenimenti ricstruiti sulla base di altre informazioni desunte dall'analisi dei fatti e delle dichiarazioni: "(...) *Dunque, vi sono evidenze oggettive della permanenza di Alberto Stasi nella propria abitazione dalle ore 9.35 fino alle ore 12.20 con sostanziale continuità; quindi alle ore 12.46; alle ore 13.26 e alle ore 13.30. Dopo tale ora Alberto Stasi dichiarava di essere uscito dalla propria abitazione per verificare le ragioni per le quali la propria fidanzata non aveva risposto alle sue numerose telefonate per tutta il corso della mattina: sul punto, come visto, vi è il riscontro del vicino di casa Riboldi Antonio. (...)".*

Segue poi il brano dove emerge l'avvenuta analisi dei dati di un altro dispositivo, il cellulare dell'indagato, e in particolare dei dati della sveglia, accompagnata dalla notazione di un'altra grave lacuna investigativa costituita dall'omessa individuazione (e conseguente acquisizione e analisi) dei dati di tale dispositivo nell'immediatezza del fatto:"(...) *Con riferimento alle dichiarazioni di Alberto Stasi in merito alle attività compiute prima delle ore 9.35 (l'attuale imputato dichiarava di avere messo la prima sveglia alle ore 9.00 e la seconda sveglia alle ore 9.30; di essersi svegliato alle ore 9.00, di avere aperto leggermente la persiana ed acceso la televisione e di essere rimasto a letto sino alle ore 9.30) il collegio peritale, su indicazione di questo Tribunale, provvedeva ad accertare lo stato di impostazione delle funzioni di allarme o "sveglia" eventualmente presenti sul telefono cellulare che era in uso a Stasi Alberto al momento dei fatti e che è stato acquisito, con il consenso di tutte le parti, in data 18 giugno 2009 nell'ambito delle operazioni peritali. Dall'esame è risultato che nell'apposita sezione "sveglia" all'interno delle funzioni di "agenda" o "calendario" è presente l'impostazione di tre allarmi programmati per le ore 9.00, 9.30 e 14.30 per tutti i giorni della settimana; tutti gli allarmi risultavano disabilitati; inoltre era attiva l'opzione accensione automatica che consente l'attivazione degli allarmi a telefono spento qualora quest'ultimi si presentino abilitati. (...)".*

In considerazione del fatto che questo cellulare non è stato oggetto nell'immediatezza dei fatti di un'ispezione della polizia giudiziaria avente ad oggetto tale questione e che il presente telefono radiomobile è stato acquisito solo in data 18 giugno 2009, bisogna necessariamente porsi il problema dell'autenticità del contenuto dello stesso.

A questo riguardo è stato accertato che l'ultima traccia di utilizzo del cellulare è datata 22 agosto 2007; che al momento della consegna del cellulare al collegio peritale la batteria era completamente scarica; che mai durante le operazioni peritali e dopo la consegna del cellulare all'ing. Porta e al dott. Occhetti (nemmeno dopo la scoperta dei c.d. "metadati" e quindi dopo il sostanzialmente verificato alibi informatico) l'imputato (mediante i propri

consulenti tecnici) chiedeva di verificare le condizioni di programmazione delle funzioni di "sveglia" sul proprio telefono cellulare.

Del resto, le dichiarazioni verbalizzate di Stasi, laddove faceva riferimento alla propria abitudine di avere due sveglie mattutine alle ore 9.00 e alle ore 9.30, non specificavano che si trattasse della sveglia del cellulare e quindi fino al momento della presente verifica peritale non vi era un'indicazione esplicita da parte di Stasi nel senso che le sveglie in parola fossero relative proprio al cellulare.

Ora, già queste convergenti circostanze inducono a ritenere verosimile che l'impostazione dei tre allarmi programmati per le ore 9.00, 9.30 e 14.30 non sia stata oggetto di un'attività successiva al fatto di reato da parte di Alberto Stasi il quale in tal modo volesse adeguare il contenuto del proprio cellulare alle dichiarazioni rese agli inquirenti. È invece ben più ragionevole che, al momento in cui Stasi decideva di non utilizzare più il cellulare, abbia disabilitato gli allarmi onde evitare che, in presenza dell'opzione accensione automatica, il cellulare iniziasse a squillare come sveglia nelle ore programmate. (...)".

Ciò dimostra l'estrema importanza della prima delle quattro fasi del trattamento dei dati a fini processuali previste dall'Informatica forense - individuazione, acquisizione, analisi-presentazione e valutazione: individuare i dispositivi con memorie sulle quali possono essere archiviati i dati utili alle indagini, costituisce il caposaldo della filiera che consente lo sviluppo di tutte le fasi successive.

Nel passo seguente il Tribunale dimostra nuovamente di saper fare buon governo dei dati sottoponendoli a verifica mediante incrocio con altri dati di altri dispositivi, nella fattispecie tra i dati del cellulare e quelli telefonici e del computer: *"(...) Del resto, che le proprie abitudini mattutine fossero sostanzialmente corrispondenti a quanto dichiarato emerge anche da una verifica ulteriore: dall'esame dei tabulati telefonici e del personal computer nel periodo precedente al fatto di reato non emergono evidenze di attività facenti riferimento ad Alberto Stasi prima delle ore 9.00 del mattino, tendenzialmente le evidenze si collocano dopo le ore 10.00 e qualche volta tra le ore 9.00 e le ore 10.00; inoltre, le telefonate che la madre di Alberto Stasi effettuava al figlio nei giorni successivi alla partenza per il mare sono sempre successive alle ore 9.30: precisamente alle ore 9.49 del giorno 11 agosto 2007 (durata 25 secondi); alle ore 9.47 del giorno 12 agosto (durata 83 secondi); quindi, come già rilevato, alle ore 9.55 del giorno 13 agosto (durata 22 secondi).*

Ciò posto, questo complessivo accertamento se consente di affermare che le dichiarazioni di Alberto Stasi in merito alle proprie abitudini di svegliarsi tra le ore 9.00 e le ore 9.30 trovano sostanziale conferma, non possono certo costituire la base probatoria di un alibi per quel lasso temporale. Infatti, la probabile presenza delle sveglie programmate e attivate alle ore 9.00 e 9.30

conformemente con le proprie abitudini non esclude in astratto che la mattina del 13 agosto 2007 Stasi Alberto si sia comunque svegliato prima del solito e sia uscito dalla propria abitazione per poi farvi rientro prima delle ore 9.35. (...)".

Quindi, solo all'esito della verifica tecnica dei dati, il Tribunale muove all'estrapolazione di informazioni per la ricostruzione degli accadimenti, non scevra da ipotesi, anche alternative tra loro:"*Dunque, possiamo riassumere il complesso delle considerazioni sopra esposte in merito alla verifica delle dichiarazioni di Alberto Stasi sulle attività da lui dichiarate compiute la mattina nei seguenti termini: (...)"*[223].

Proseguendo, il Tribunale passa verificare altri aspetti della ricostruzione dei fatti, muovendo dai dati del dispositivo digitale[224]":(…) *Venendo alla disanima del secondo ordine di ragioni su cui si fondano altri significativi aspetti di criticità rispetto alla ipotesi accusatoria relativa alla finestra temporale 9.12/9.35, bisogna osservare quanto segue.*

L'attuale imputato attivava il proprio personal computer alle ore 9.35 ed eseguiva l'accesso al sistema con la digitazione della propria password: quindi a partire dalle ore 9.38 (circa) fino sicuramente alle ore 10.07 (come già sopra specificato) visualizzava immagini di natura erotico/pornografica; alle 10.17 apriva il file della tesi.

Bisogna precisare che le evidenze sopra specificate consentono di affermare con certezza che Stasi ha visualizzato quelle immagini, tuttavia non possiamo escludere che lo stesso ne abbia viste altre all'interno delle medesime cartelle. Questa impossibilità di verificare tale ulteriore dettaglio è dovuta al fatto che i carabinieri successivamente al sequestro hanno acceduto (come più volte sottolineato) ripetutamente e scorrettamente alla totalità del contenuto del computer, tra cui anche, appunto, alle immagini di natura pornografica.

Ebbene, è di grande importanza soffermarsi su questa prima attività informatica compiuta da Alberto Stasi la mattina dell'omicidio in quanto, seguendo l'ipotesi accusatoria, quei momenti si collocherebbero pochi minuti dopo l'uccisione da parte di questi della propria fidanzata.

In primo luogo, bisogna evidenziare che l'accertato inserimento di password errata al riavvio del PC in data 13 agosto alle ore 9:36:21 da parte di Alberto Stasi rappresenta un accadimento del tutto tipico e non può quindi costituire elemento sintomatico di un particolare stato d'animo dell'utente.

In molte sessioni di lavoro precedenti (in data 12 agosto alle ore 19:05:13, 21:27:16; in data 11 agosto alle ore 11:07:01, 15:24:25, 19:27:18) si riscontrano infatti errori di inserimento della password all'atto della riattivazione del PC: in totale dalla data del 25 luglio alla data del 13 agosto

[223] Per le ipotesi ricostruttive dei fatti, v. Trib. Vigevano, op.cit., da p. 47 a p. 50.
[224] *Ibidem,* p. 50 e ss..

occorrono 60 eventi di errato inserimento delle credenziali di autenticazione. Tecnicamente tale circostanza dipende più che verosimilmente, come spiegato dal collegio peritale, da motivi connessi alla riattivazione del PC: "accade, infatti, che la riattivazione determini spesso uno stato in cui trascorre un lasso di tempo prima della completa operatività del sistema operativo, nel quale, se l'utente preme un tasto, perché ad esempio inizia a digitare la password, questo non viene recepito in quanto il buffer della tastiera non appare ancora reattivo e l'esito di questa attività è la digitazione di una password mancante di uno o più caratteri iniziali, pertanto errata" (si veda relazione peritale a pag. 93).

In secondo luogo, la circostanza che Alberto Stasi, prima di iniziare il proprio lavoro alla tesi di laurea, visualizzasse immagini di carattere erotico/pornografico non rappresenta un accadimento anomalo, rientrando al contrario nelle sue non infrequenti abitudini.

Come rilevato dal collegio peritale in sede di relazione peritale e di audizione in udienza, sono stati infatti riscontrati nei giorni immediatamente precedenti al fatto (la ricerca non poteva che ricomprendere per ragioni tecniche solo un breve arco temporale prima del giorno dell'omicidio) le seguenti evidenze: il giorno 12 agosto 2007 l'attività informatica iniziava con una prima visualizzazione di contenuti multimediali espletata nel corso della mattina e quindi nel corso del pomeriggio di una videoscrittura della tesi di laurea; per il giorno 11 agosto 2007 vi è il riscontro di una preliminare visualizzazione, dopo l'accensione (intesa come uscita dallo standby) del computer, di immagini erotico/pornografiche e poi dell'inizio del lavoro alla tesi; analogamente nel corso della mattina del giorno 10 agosto Alberto Stasi prima guardava immagini di natura erotico/pornografica e quindi lavorava alla tesi; il giorno 9 agosto alle ore 9.36 l'attuale imputato guardava dapprima immagini pornografiche e quindi iniziava a lavorare alla tesi a partire dalle ore 10.12. (...)".

Anche da tali passaggi si desume come il Tribunale abbia tratto dai dati le informazioni per inferire, comportamenti, preferenze, abitudini dell'utilizzatore, ma abbia altresì verificato l'ipotesi che l'imputato abbia attivato tecniche di c.d. *antiforensics*, ovvero di contromisure per neutralizzare o sviare la successiva attività di analisi forense del dispositivo da lui utilizzato:"(...) *Bisogna a questo punto domandarsi quale fosse lo scopo di questa prima attività informatica del giorno 13 agosto 2007 cominciata da Alberto Stasi subito dopo l'attivazione del proprio personal computer e proseguita per alcune decine di minuti prima di iniziare a lavorare alla propria tesi di laurea.*

Possiamo con ragionevole certezza escludere che in tal modo l'attuale imputato volesse cancellare dal proprio personal computer alcuni contenuti di carattere appunto erotico/pornografico ivi contenuti: la circostanza che le immagini ed il video sicuramente visionati quella mattina fossero ancora

presenti al momento della consegna del computer agli inquirenti porta, infatti, a respingere questa ipotesi.

Assume allora centrale questione valutare se Alberto Stasi in quelle decine di minuti appena successive all'omicidio che lo stesso (seguendo questa ipotesi accusatoria) avrebbe commesso abbia voluto, mediante tale attività di visualizzazione di contenuti multimediali, crearsi un'iniziale alibi.

Sarebbe, infatti, del tutto ragionevole pensare che le attività che l'autore di un omicidio compia nell'immediatezza successiva al fatto siano logicamente e funzionalmente collegate a tale del tutto eccezionale accadimento e alle connesse istintive reazioni di autodifesa: insomma se Stasi accende il proprio computer e compie una certa attività pochi minuti dopo avere ucciso la propria fidanzata in modo così violento e rabbioso, è del tutto logico attendersi che tale immediatamente successiva attività informatica sia finalizzata a cancellare tracce pertinenti all'omicidio o a precostituirsi un alibi difensivo.

Ebbene, bisogna escludere anche quest'ultima ipotesi.(...)".

Nei brani della sentenza successivi a quelli riportati, il Tribunale si sofferma ad analizzare la compatibilità tra i dati rivenuti e un possibile movente dell'imputato[225], ad incrociare i dati degli apparecchi telefonici delle persone e dei luoghi coinvolti[226], a valutare i comportamenti di interazione con il computer partendo dall'analisi dei dati per ricostruire la compatibilità con gli accadimenti[227].

Come si è visto, gli argomenti della parte di motivazione esaminata si destreggiano tra lo sforzo di dare corretto rilievo alle procedure di Informatica forense disattese dalla polizia giudiziaria, quello di escludere eventuali profili di responsabilità di quest'ultima, e quello di recuperare informazioni utili alla ricostruzione degli eventi da reperti informatici irrimediabilmente compromessi dalla maldestria degli intervenuti nella prima fase delle investigazioni.

Al di là della vicenda di merito esitata come è notoriamente risaputo, la rassegna dei passi della sentenza del Tribunale di Vigevano relativi ai motivi di interesse per l'Informatica forense consente di apprezzare come un approccio non scientifico ai dispositivi oggetto di investigazione sia devastante per l'acquisizione dei dati rilevanti per il procedimento mentre, al contrario, il corretto approccio ai dispositivi e ai dati informatici, secondo metodologie ormai note e consolidate, nonchè giuridicamente obbligatorie, costituisca la chiave di volta per una corretta assunzione di informazioni rilevanti per il processo, nell'interesse di tutte le parti, in ogni fase e grado del procedimento.

Per questi motivi, il percorso logico-argomentativo della sentenza appena ripercorsa si pone come moderno paradigma per la corretta valutazione

[225] *Ibidem,* p. 52.
[226] *Ibidem,* pp. 52 – 59.
[227] *Ibidem*, pp. 60 e ss.

dell’attendibilità dei dati, nonché della corretta interrelazione delle informazioni derivanti dai dispositivi digitali.

6 La questione della ripetibilità o irripetibilità degli accertamenti tecnici ad oggetto informatico

Un'altra questione di fondamentale rilevanza nell'ambito dell'Informatica forense attiene alla definizione della natura giuridica delle operazioni di acquisizione, duplicazione e analisi di dati informatici nella fase delle indagini preliminari di un procedimento penale, e in particolare se queste siano qualificabili come accertamenti tecnici ripetibili o irripetibili ex art. 360 e/o art. 117 disp. att. e, in caso affermativo, quale si il regime giuridico conseguente.

Difatti, da tale qualificazione deriva la conseguenza di ritenere tali operazioni soggette o meno al regime di atti assistiti dalle garanzie di informazione e di intervento delle altre parti non procedenti, come imposto dall'art. 360.

Sul punto la giurisprudenza si sta assestando su posizioni giuridicamente non condivisibili che muovono da un'errata percezione ed impostazione del fenomeno fattuale.

Per meglio comprendere le implicazioni della questione nell'ambito dei procedimenti con accertamenti tecnici informatici, è essenziale ripercorrere la disciplina generale degli accertamenti tecnici nel procedimento penale.

6.1 Gli accertamenti tecnici del pubblico ministero

Come è noto, il pubblico ministero è tenuto, ai sensi dell'art. 358 (Attività di indagine del pubblico ministero), a compiere"...*ogni attività necessaria ai fini indicati nell'art. 326 e svolge altresì accertamenti su fatti e circostanze a favore della persona sottoposta alle indagini".*

Sempre nel corso delle indagini preliminari, può sorgere la necessità per il pubblico ministero o per il difensore delle parti private di svolgere accertamenti che comportano specifiche conoscenze scientifiche, tecniche o artistiche[228].

In tal caso, la parte che ne abbia necessità può ricorrere alla particolare procedura dell'incidente probatorio prevista dall'art. 392 (lett. b) e c))[229] e chiedere al giudice la nomina di un perito.

---

[228] V. TONINI P., Manuale di procedura penale, Giuffrè, Milano, 2003, pp. 405 e ss..

[229] *"TITOLO VII Incidente probatorio. 392 Casi - 1. Nel corso delle indagini preliminari [326-415 c.p.p.] il pubblico ministero e la persona sottoposta alle indagini possono chiedere al giudice che si proceda con incidente probatorio:*
a) all'assunzione della testimonianza [194 c.p.p.] di una persona, quando vi è fondato motivo di ritenere che la stessa non potrà essere esaminata nel dibattimento per infermità o altro grave impedimento;

Per ovviare ai tempi lunghi di attivazione e all'esame preventivo di ammissibilità da parte del giudice, il codice prevede lo strumento della consulenza tecnica di parte di cui all'art. art. 359 c. 1 che così recita: "*(Consulenti tecnici del pubblico ministero) Il pubblico ministero, quando procede ad accertamenti, rilievi segnaletici, descrittivi o fotografici ed ogni altra operazione tecnica per cui sono necessarie specifiche competenze, può nominare e avvalersi di consulenti, che non possono rifiutare la loro opera (348, 366 c.p. e 141 bis).*

Il consulente può essere autorizzato dal pubblico ministero ad assistere a singoli atti di indagine (att. 73).".

In tal caso, il pubblico ministero procede autonomamente alla nomina del consulente e all'espletamento degli accertamenti tecnici ripetibili.

Vi sono poi casi nei quali, il pubblico ministero, preliminarmente qualificati come irripetibili in relazione al dibattimento gli accertamenti tecnici, non può compierli autonomamente ma deve avviare la procedura prevista dall'art. 360 che prevede quanto segue:"*Art. 360 (Accertamenti tecnici non ripetibili). Quando gli accertamenti previsti dall'art. 359 riguardano persone, cose o luoghi il cui stato è soggetto a modificazione, il pubblico ministero avvisa, senza ritardo, la persona sottoposta alle indagini, la persona offesa dal reato (90) e i difensori (96, 101) del giorno, dell'ora e del luogo fissati per il conferimento dell'incarico e della facoltà di nominare consulenti tecnici (233; att. 117).*

Si applicano le disposizioni dell'art. 364 comma 2. (i.e. Nomina e assistenza del difensore).

---

b) all'assunzione di una testimonianza quando, per elementi concreti e specifici, vi è fondato motivo di ritenere che la persona sia esposta a violenza, minaccia, offerta o promessa di denaro o di altra utilità affinché non deponga o deponga il falso;
c) all'esame della persona sottoposta alle indagini su fatti concernenti la responsabilità di altri [quando ricorre una delle circostanze previste dalle lettere a) e b)];
d) all'esame delle persone indicate nell'articolo 210 [quando ricorre una delle circostanze previste dalle lettere a) e b)];
e) al confronto tra persone che in altro incidente probatorio o al pubblico ministero hanno reso dichiarazioni discordanti, quando ricorre una delle circostanze previste dalle lettere a) e b);
f) a una perizia [220, 508] o a un esperimento giudiziale [218], se la prova riguarda una persona, una cosa o un luogo il cui stato è soggetto a modificazione non evitabile;
g) a una ricognizione [213], quando particolari ragioni di urgenza non consentono di rinviare l'atto al dibattimento.
1 bis. Nei procedimenti per i delitti di cui agli articoli 572, 600, 600 bis, 600 ter e 600 quater, anche se relativi al materiale pornografico di cui all'articolo [[n600quater.1cp]], 600 quinquies, 601, 602, 609 bis, 609 quater, 609 quinquies, 609 octies, 609 undecies e 612 bis del codice penale il pubblico ministero, anche su richiesta della persona offesa, o la persona sottoposta alle indagini possono chiedere che si proceda con incidente probatorio all'assunzione della testimonianza di persona minorenne ovvero della persona offesa maggiorenne, anche al di fuori delle ipotesi previste dal comma 1.
2. Il pubblico ministero e la persona sottoposta alle indagini possono altresì chiedere una perizia che, se fosse disposta nel dibattimento, ne potrebbe determinare una sospensione superiore a sessanta giorni ovvero che comporti l'esecuzione di accertamenti o prelievi su persona vivente previsti dall'art. 224 bis. [467, 468 5].

I difensori nonché i consulenti tecnici eventualmente nominati hanno diritto di assistere al conferimento dell'incarico, di partecipare agli accertamenti e di formulare osservazioni e riserve.

Qualora, prima del conferimento dell'incarico, la persona sottoposta alle indagini formuli riserva di promuovere incidente probatorio (392, 393), il pubblico ministero dispone che non si proceda agli accertamenti salvo che questi, se differiti, non possano più essere utilmente compiuti.

Se il pubblico ministero, malgrado l'espressa riserva formulata dalla persona sottoposta alle indagini e pur non sussistendo le condizioni indicate nell'ultima parte del comma 4, ha ugualmente disposto di procedere agli accertamenti, i relativi risultati non possono essere utilizzati nel dibattimento (431, lett. c); att. 116, 117, 240 bis)".

Orbene, il momento della qualificazione della natura ripetibile o irripetibile degli accertamenti tecnici da parte del pubblico ministero (eventualmente con l'ausilio dello stesso consulente tecnico) è di fondamentale importanza in relazione alla formazione del *thema probandum* in quanto tale operazione esegetica condizionerà indefettibilmente tutto il prosieguo del procedimento.

Le conseguenze della distinzione sono rilevanti dal punto di vista della scelta delle procedure da seguire previste dagli artt. 359 e 360.

Difatti, se gli accertamenti risulteranno ripetibili, allora il pubblico ministero potrà procedere autonomamente con il proprio consulente tecnico allo svolgimento dell'attività tecnica ai sensi dell'art. 359 e il verbale delle attività compiute sarà inserito nel fascicolo del pubblico ministero allorquando, svoltasi l'udienza preliminare, sarà stato disposto il rinvio a giudizio.

Se invece gli accertamenti tecnici da svolgere saranno qualificati come irripetibili, allora si dovrà percorrere la diversa procedura prevista dall'art. 360, la cui articolazione è molto più ampia rispetto all'altra procedura, in quanto comporta l'intervento partecipativo delle parti, per quanto meno ampia della procedura peritale e dagli effetti assimilabili – ma non sovrapponibili – a quelli della perizia[230].

Il codice di rito non solo non tipizza gli accertamenti tecnici, ma la portata delle norme in proposito è ampia e atipica, a cominciare dal concetto di "irripetibilità" degli accertamenti tecnici che può assumere varie accezioni:

- l'irripetibilità in senso "giuridico" (art. 360) ricorre allorquando si tratti di accertamenti che "riguardano persone, cose o luoghi il cui stato è soggetto a modificazione" "tali da far perdere loro in tempi brevi, ogni

[230] Sugli accertamenti tecnici non ripetibili, v. FOCARDI F., La consulenza tecnica extraperitale delle parti private, Cedam, Padova, 2003; GIUNCHEDI F., Gli accertamenti tecnici irripetibili, Utet, Milano, 2009; sugli accertamenti in fase processuale, v. CONTE, M., LOFORTI R., Gli accertamenti tecnici nel processo penale, Giuffrè, Milano, 2006; GIUNCHEDI F., Gli accertamenti tecnici tra non ripetibilità e non rinviabilità, in Arch. pen., 1, 2014.

valenza probatoria in relazione ai fatti oggetto di indagini e di eventuale futuro giudizio[231], come ad es. nel caso delle operazioni di rilevazione delle tracce di polvere da sparo;

- l'irripetibilità nel senso di "indifferibilità" (art. 360, 4° c.) si verifica allorquando gli accertamenti sono di natura fisica tale che, ove differiti, non possono più essere utilmente compiuti[232];
- l'irripetibilità "tecnica" (art. 117 disp. att.) ricorre allorquando gli stessi accertamenti determinano "modificazione delle cose, dei luoghi, o delle persone tali da rendere l'atto non ripetibile"[233].

Alla qualificazione degli accertamenti tecnici come irripetibili, però, consegue l'obbligo del pubblico ministero di dare previo avviso e senza ritardo alla persona sottoposta alle indagini, alla persona offesa dal reato e ai loro difensori del giorno, dell'ora e del luogo fissati per il conferimento dell'incarico e della facoltà di nominare consulenti tecnici.

Gli avvisati e i loro difensori hanno facoltà di nominare un proprio consulente tecnico, mentre i difensori e i tecnici eventualmente nominati hanno facoltà di assistere al conferimento dell'incarico, di partecipare alle operazioni e di formulare osservazioni e riserve.

È in questa fase, prima del conferimento dell'incarico, che la persona sottoposta alle indagini formuli può avanzare riserva di promuovere incidente probatorio (artt. 392, 393) e, nel caso in cui ciò avvenga, il pubblico ministero dispone che non si proceda agli accertamenti salvo che questi, se differiti, non possano più essere utilmente compiuti.

Nel caso in cui venga avanzata la riserva, il pubblico ministero non può più procedere all'accertamento tecnico e deve attendere che venga instaurata la procedura dell'incidente probatorio; altrimenti, dovrà decidere se l'accertamento possa essere differito o meno; nel caso in cui l'accertamento tecnico sia differibile e il pubblico ministero disponga di procedere ugualmente nonostante l'espressa riserva formulata dalla persona sottoposta alle indagini pur non sussistendo le condizioni indicate nell'ultima parte del comma 4, i relativi risultati non potranno essere utilizzati nel dibattimento (artt. 431, lett. c, 116, 117, disp. att., 240 bis)". Se invece l'accertamento non è differibile perché ove differito non sarebbe più utilmente compiuto, il verbale delle operazioni viene inserito direttamente nel fascicolo per il dibattimento ex art. 431, c. 1, lett. c)[234].

---

[231] v. Cass., 26 marzo 1993, n. 2999, Cornacchia; v. GIORDANO F.P., Le indagini preliminari, Cedam, Padova, 2003, p. 418.
[232] Cfr. GIORDANO F.P., op.cit., p. 420.
[233] È il caso, ad es., dell'esame chimico di una limitata quantità di sostanza stupefacente o della matricola abrasa di un'arma da fuoco, il cui compimento altera o distrugge irreversibilmente l'oggetto dell'esame.
[234] Così in TONINI P., op.cit. 407.

Gli effetti della qualificazione degli accertamenti sono quindi molto rilevanti ai fini dell'esercizio della facoltà processuali inquisitorie e difensive previste dal rito per i rispettivi titolari, il pubblico ministero le parti e i relativi difensori in quanto ove le garanzie difensive non venissero osservate, conseguirebbe l'inutilizzabilità degli atti, costituente un caso di nullità a regime intermedio ex art. 178, 1° c., eccepibile prima della deliberazione della sentenza di I grado.

Quanto infine ai tecnici cui le parti possono affidare l'incarico, la legge non pone limiti o condizioni alla loro scelta in relazione al *minimum* di competenza tecnica di cui essi devono essere in possesso. Solo il pubblico ministero è tenuto a scegliere "di regola" i propri consulenti tra quelli iscritti nell'albo dei periti ex art. 73 disp. att..

6.2 Gli accertamenti tecnici del difensore

L'istituto è previsto anche per l'analoga attività svolta dal difensore delle parti svolta secondo le norme sulle investigazioni difensive previste dalla legge n. 397 del 2000.

La novella, introducendo nel codice i poteri attivi della difesa (anche tramite il proprio consulente tecnico) ha previsto e disciplinato il caso in cui sia il difensore a svolgere attività di investigazione difensiva in piena autonomia e in alternativa al pubblico ministero anche in punto di accertamenti tecnici irripetibili.

In particolare, per quanto attiene alle investigazioni difensive aventi ad oggetto questioni tecniche[235], la prima norma di riferimento è l'art. 233 il quale così recita: "*Consulenza tecnica fuori dei casi di perizia.*

1. Quando non è stata disposta perizia [359], ciascuna parte può nominare, in numero non superiore a due, propri consulenti tecnici. Questi possono esporre al giudice il proprio parere, anche presentando memorie a norma dell'articolo 121.

1 bis. Il giudice, a richiesta del difensore, può autorizzare il consulente tecnico di una parte privata ad esaminare le cose sequestrate nel luogo in cui esse si trovano, ad intervenire alle ispezioni, ovvero ad esaminare l'oggetto delle ispezioni alle quali il consulente non è intervenuto. *Prima dell'esercizio dell'azione penale l'autorizzazione è disposta dal pubblico ministero a richiesta del difensore. Contro il decreto che respinge la richiesta il difensore può proporre opposizione al giudice, che provvede nelle forme di cui all'articolo 127.*[236]

[235] Prima dell'entrata in vigore della legge sulle investigazioni difensive, ai difensori erano già riconosciute facoltà in materia tecnica, quali, ad es., quella di presentare memorie e richieste durante le IP (art. 367 c.p.p.).

[236] I commi 1 bis e 1 ter sono stati inseriti dall'art. 5, della L. 7 dicembre 2000, n. 397.

1 ter. L'autorità giudiziaria impartisce le prescrizioni necessarie per la conservazione dello stato originario delle cose e dei luoghi e per il rispetto delle persone.

2. Qualora, successivamente alla nomina del consulente tecnico, sia disposta perizia, ai consulenti tecnici già nominati sono riconosciuti i diritti e le facoltà previsti dall'articolo 230, salvo il limite previsto dall'articolo 225 comma 1.

3. Si applica la disposizione dell'articolo 225 comma 3."

Pertanto, al consulente della difesa è consentito esercitare i c.d. "poteri partecipativi"[237]:

- esaminare le cose sequestrate nel luogo in cui esse si trovano (e se si tratta di documenti, estrarne copia (art. 366, c. 1)[238], ove per "esaminare" si intende lo svolgimento delle attività che non arrecano modifiche o alterazioni dell'oggetto;
- intervenire nelle ispezioni compiute dagli organi dell'accusa, unitamente al consulente tecnico, previa autorizzazione del pubblico ministero prima dell'esercizio dell'azione, e del giudice in caso di opposizione avverso il decreto di respingimento;
- esaminare l'oggetto delle ispezioni alle quali il consulente non è intervenuto.

Nel caso in cui le attività di esame e ispezione vengano autorizzate, l'autorità giudiziaria è tenuta a verificare che l'esercizio di tali facoltà non costituisca pericolo per la genuinità dell'elemento di prova e stabilisce le precauzioni da seguire per la conservazione dello stato originario delle cose e dei luoghi e per il rispetto delle persone.

La legge sulle investigazioni ha poi introdotto una rilevante novità in relazione agli atti irripetibili compiuti dal difensore, la cui disciplina è prevista

---

[237] TONINI P., op.cit., p. 487.

[238] L'art. 366 così recita: "*Deposito degli atti cui hanno diritto di assistere i difensori.*

1. Salvo quanto previsto da specifiche disposizioni [268], i verbali degli atti compiuti dal pubblico ministero e dalla polizia giudiziaria ai quali il difensore ha diritto di assistere [350 1 , 2 , 3 , 4, 356, 364, 365], sono depositati nella segreteria del pubblico ministero entro il terzo giorno successivo al compimento dell'atto, con facoltà per il difensore di esaminarli ed estrarne copia nei cinque giorni successivi. Quando non è stato dato avviso del compimento dell'atto, al difensore è immediatamente notificato l'avviso di deposito e il termine decorre dal ricevimento della notificazione. Il difensore ha la facoltà di esaminare le cose sequestrate nel luogo in cui esse si trovano e, se si tratta di documenti, di estrarne copia.

2. Il pubblico ministero, con decreto motivato, può disporre, per gravi motivi, che il deposito degli atti indicati nel comma 1 e l'esercizio della facoltà indicata nel terzo periodo dello stesso comma siano ritardati, senza pregiudizio di ogni altra attività del difensore, per non oltre trenta giorni. Contro il decreto del pubblico ministero la persona sottoposta ad indagini ed il difensore possono proporre opposizione al giudice, che provvede ai sensi dell'articolo 127".

dall'art. 391 decies[239]:"*(Utilizzazione della documentazione delle investigazioni difensive) 1. Delle dichiarazioni inserite nel fascicolo del difensore le parti possono servirsi a norma degli articoli 500, 512 e 513.*

2. Fuori del caso in cui è applicabile l'articolo 234, la documentazione di atti non ripetibili compiuti in occasione dell'accesso ai luoghi, presentata nel corso delle indagini preliminari o nell'udienza preliminare, è inserita nel fascicolo previsto dall'articolo 431.

3. Quando si tratta di accertamenti tecnici non ripetibili, il difensore deve darne avviso, senza ritardo, al pubblico ministero per l'esercizio delle facoltà previste, in quanto compatibili, dall'articolo 360. Negli altri casi di atti non ripetibili di cui al comma 2, il pubblico ministero, personalmente o mediante delega alla polizia giudiziaria, ha facoltà di assistervi.

4. Il verbale degli accertamenti compiuti ai sensi del comma 3 e, quando il pubblico ministero ha esercitato la facoltà di assistervi, la documentazione degli atti compiuti ai sensi del comma 2 sono inseriti nel fascicolo del difensore e nel fascicolo del pubblico ministero. Si applica la disposizione di cui all'articolo 431, comma 1, lettera c).".

In questo caso, l'irripetibilità degli accertamenti è intesa nell'accezione di indifferibilità, che si verifica allorquando non potrebbero più essere utilmente compiuti in relazione al dibattimento.

Il terzo comma della norma prescrive a carico del difensore i medesimi oneri previsti a carico del pubblico ministero dall'art. 360, così ricalcando a parti invertite il meccanismo giuridico già esaminato.

Tuttavia, resta salva la prerogativa del pubblico ministero di intervenire con gli strumenti propri della sua funzione pubblica e bloccare il procedimento tecnico della difesa allorquando possa costituire pericolo di irrimediabile compromissione della fonte di prova[240].

Quanto infine ai tecnici cui il difensore può affidare l'incarico, come si è già detto la legge non pone limiti o condizioni alla loro scelta in relazione al *minimum* di competenza tecnica di cui essi devono essere in possesso.

6.3 Gli accertamenti tecnici informatici

Una delle questioni più rilevanti nell'ambito dell'Informatica forense attiene alla definizione della natura giuridica degli accertamenti tecnici ad oggetto informatico e, in particolare, delle operazioni di acquisizione, duplicazione e analisi di dati informatici nella fase delle indagini preliminari di un procedimento penale, per stabilire se queste siano qualificabili come

[239] Tale articolo, come l'intero Titolo di cui fa parte, è stato aggiunto dall'art. 11, della l. 7 dicembre 2000, n. 397.

[240] Sui poteri e limiti dell'attività difensiva in merito agli accertamenti tecnici non ripetibili compiuti nell'ambito delle investigazioni difensive, v. TONINI P., op.cit. pp. 489 e ss..

accertamenti tecnici ripetibili o irripetibili ex art. 360 e/o art. 117 disp. att. e, in caso affermativo, quale si il regime giuridico conseguente[241].

Difatti, da tale qualificazione deriva la conseguenza di ritenere tali operazioni soggette o meno al regime di atti assistiti dalle garanzie di informazione e di intervento delle altre parti non procedenti, come imposto dall'art. 360.

Alla luce delle norme ripercorse, la problematica riguarda indistintamente sia gli accertamenti tecnici effettuati dalla Polizia giudiziaria, di iniziativa o su delega del Pubblico ministero, sia gli accertamenti tecnici svolti dal difensore, con o senza l'ausilio di un Consulente tecnico nominato *ad hoc*, nell'esercizio della facoltà di svolgere investigazioni difensive ex art. 391-decies, c. 4.

L'importanza della questione deriva dalla circostanza per la quale, proprio dalla corretta impostazione e soluzione, dipende l'obbligo di conformare l'accertamento tecnico al modello processuale vigente, nonché la doverosità o meno dell'adozione della procedura garantita prevista dall'art. 360.

Infatti, se si considera che secondo il principio di separazione delle fasi che caratterizza un processo accusatorio, la fase delle indagini è distinta da quella del dibattimento e che è consentito utilizzare come prova nella fase dibattimentale solo quella formatasi (di regola) con il metodo del contraddittorio tra le parti[242], le operazioni tecniche svolte nella fase delle indagini costituiscono un'eccezione. Tuttavia, proprio perché parte del *thema probandum* si forma durante le indagini, l'oggetto del vaglio tecnico dei consulenti costituisce il presupposto di fatto da sottoporre al vaglio giuridico del pubblico ministero ai fini della decisione relativa all'esercizio dell'azione penale e del giudice ai fini della decisione sul merito della fattispecie.

Per poter qualificare giuridicamente la natura degli accertamenti tecnici aventi ad oggetto reperti informatici, bisogna innanzitutto determinare quale sia

---

[241] La questione fu proposta a livello dottrinale nell'ambito della presentazione tenuta dallo scrivente durante la seconda edizione del Master in Diritto delle nuove tecnologie organizzato dal CSIG-Centro Studi di Informatica Giuridica, 12 maggio 2003, Bari, sul quale v. GALEOTTI P., Master-Post eventum 12.05.03, in *http://www.avvocatiacquavivacassano.it*; v. INDOVINA B., Accertamenti tecnici informatici: atti ripetibili o irripetibili, 2012, in *http://www.medialaws.eu/accertamenti-tecnici-informatici-atti-ripetibili-o-irripetibili/*; GIUNCHEDI F., Le malpractices nella digital forensics. Quali conseguenze sull'inutilizzabilità del dato informatico? in Arch. Pen., 3, 2013, p. 821, *http://www.archiviopenale.it/apw/wp -content/uploads/2013/09/Confronto.Giunchedi.pdf*; RICCI A.E., Digital evidence e irripetibilità delle operazioni acquisitive, nota a Cass. Sez. I, sent. 5 marzo 2009-2 aprile 2009, n. 14511, in Dir. pen proc., 2009, p. 337; CERQUA F., Ancora dubbi e incertezze sull'acquisizione della corrispondenza elettronica, 2015, in *http://www.penalecontemporaneo.it/upload/1437560206 CERQUA_F._2015a.pdf*; CACCAVELLA D., E., Gli accertamenti tecnici in ambito informatico, in ATERNO S., MAZZOTTA P., La perizia e la consulenza tecnica. Cedam, Padova, 2006, p. 195.

[242] Cosi in NAPPI A., Guida al Codice di Procedura Penale, Giuffrè, Milano, 2000, pp. 109 e ss..

la natura fattuale delle operazioni e quale sia la loro rilevanza in relazione ai tipi di irripetibilità sopra esaminati.

La qualificazione giuridica deve essere preceduta da una rigorosa disamina della realtà tecnica costituita dall'oggetto.

In linea di prima approssimazione si può affermare che le molteplici situazioni che si vengono a crearsi durante l'interazione, sia operativa che investigativa, con i dispositivi digitali richiedono una profonda capacità di comprensione del fenomeno al fine di qualificarlo giuridicamente in modo corretto e quindi intraprendere gli schemi procedurali più appropriati.

Tale attività non può essere schematizzabile in modo rigido in quanto le situazioni che possono crearsi dipendono da molteplici fattori, tra i quali rilevano in particolar modo le caratteristiche tecnologiche dell'oggetto informatico sottoposto ad accertamento tecnico.

In linea di principio, non esente da ampie eccezioni, si può affermare che ogni interazione o accesso ai dispositivi informatici, hardware o software che siano, comporta cambiamenti irreversibili dello stato del sistema e soprattutto dei bit archiviati.

Come si è già detto, oggetto dell'attività di accertamento tecnico è l'acquisizione dei dati dai quali le parti, e solo in prima battuta gli organi dell'accusa, traggono informazioni utili, talvolta indispensabili, ai fini del procedimento.

Ma i dati sono codificati in bit, per cui ogni variazione di questi ultimi, anche minima, determina variazione dei dati e quindi variazione, e spesso perdita, di informazioni rilevanti per il procedimento.

Quando poi la minima variazione o la perdita riguarda bit relativi a dati particolarmente rilevanti, come ad esempio un orario, una data, un nome, un luogo[243], gli effetti sulle informazioni necessarie alla corretta ricostruzione dei fatti possono essere particolarmente gravi.

Se, infine, la variazione o perdita di bit riguarda dati dai quali una parte diversa da quella procedente all'accertamento tecnico avrebbe potuto trarre informazioni rilevanti per la propria posizione, gli effetti assumono caratteri di rilevante gravità[244]. È questo il caso in cui, ad esempio, la polizia giudiziaria, di iniziativa o su delega accedere ripetutamente ad un dispositivo informatico per trarre o anche solo leggerne il contenuto[245].

---

[243] È quanto dimostrato con i semplici esperimenti riportati in un precedente capitolo.

[244] È quanto accaduto nel caso Garlasco, oggetto della sentenza del Tribunale di Vigevano, op.cit., *passim.*

[245] È ad es. quanto verificatosi nel procedimento oggetto della sentenza del Tribunale di Vigevano, nel quale proprio i ripetuti accessi al pc dell'indagato effettuati dalla polizia giudiziaria senza la preventiva adozione delle misure idonee a proteggere i dati del sistema, ha determinato la modifica (e la perdita) irreversibile dei dati e quindi di informazioni rilevanti per il procedimento.

Orbene, ci si deve chiedere preliminarmente se e come sia possibile che interagendo con sistemi informatici e telematici e con i dati in esso archiviati, si possano determinare alterazioni e talvolta perdita di dati e quindi informazioni utili al procedimento.

A tal proposito, il giurista deve rivolgersi alla scienza informatica sia per cercare la corretta analisi del fenomeno empirico da qualificare, tenuto conto delle caratteristiche tecnologiche e delle situazioni oggetto di attività di accertamento tecnico, sia per implementare le soluzioni tecniche più opportune alla salvaguardia delle prerogative delle parti nel quadro degli schemi processuali in esame.

Innanzitutto va ricordato che i bit, oggetto di interesse delle parti del procedimento, sono archiviati sulle memorie.

Queste, come si è già detto, possono essere memorie primarie, caratterizzate da tecnologie e criteri di funzionamento che rendono i dati in esse archiviati estremamente volatili o da memorie secondarie, sulle quali i dati sono archiviati in modo più stabile e duraturo. Pertanto, i dati di un sistema sono sempre e solo temporaneamente archiviati in quanto:

1) o possono essere dispersi per fatto proprio della tecnologia delle memorie primarie;
2) o sono esposti al rischio di essere cancellati o modificati da sovrascrittura quale effetto di molteplici meccanismi, talvolta fisiologici, di sovrascrittura, a loro volta causati o da fattori esterni al sistema, quali l'azione volontaria o accidentale dell'operatore, malfunzionamenti, altre cause esterne in grado di modificare i dati, ovvero da operazioni svolte dal sistema operativo;
3) o sono destinati ad essere trasmessi per via telematica.

In secondo luogo, ogniqualvolta l'operatore interagisce con il dispositivo, o quest'ultimo interagisce con altri dispositivi, intervenendo sui file archiviati ed effettuando consapevolmente variazioni dei dati di cui sono composti i file, siano questi di testo, audio, video e comunque file digitali, si realizzano modifiche che alterano lo *status quo ante* dei dati, spesso in modo irreversibile e con modalità che spesso non consentono di individuare il diretto artefice della modifica se non ricorrendo, ove raramente possibile, ad altri dati e informazioni collaterali.

Ma qui termina la parte sulla rilevanza delle variazioni consapevoli dei dati digitali archiviati in un sistema.

Ciò che invece complica la questione delle variazioni dei dati è che vi sono una lunga e variegata serie di operazioni svolte dal sistema informatico e telematico di cui l'operatore è del tutto ignaro o inconsapevole, come comprovato dagli obiter che a breve si analizzeranno.

Difatti, va tenuto conto del fatto che ogni dispositivo è gestito da un sistema operativo[246] al quale è demandato il compito di sovrintendere alle funzioni fondamentali del sistema informatico e telematico. Tuttavia, vi sono molteplici funzioni, quali appunto la gestione dei dati di sistema, che sono per lo più automatiche e prescindono dal controllo dell'operatore. Una rilevante congerie di metadati riferiti ai file – come ad esempio la data e l'ora di creazione, di ultima modifica, di ultimo accesso ai file archiviati – vengono generati o modificati automaticamente dal sistema operativo ogniqualvolta vengono compiute le relative operazioni, anche se l'operatore ne è del tutto ignaro. Spesso, sono proprio questi dati che attirano l'attenzione delle parti del processo in quanto forieri, direttamente o indirettamente, delle informazioni riguardanti i (presunti) comportamenti dell'operatore in determinate circostanze di luogo e di tempo e quindi rilevanti ai fini della ricostruzione *ex post* di circostanze oggetto di indagine da parte degli organi dell'accusa o della difesa.

Vi sono altri file del sistema operativo che vengono modificati ogniqualvolta l'operatore interagisce con il dispositivo o questo interagisce con altri dispositivi; uno di questi è il file di log che, svolgendo la funzione di registro delle operazioni verificatesi in un sistema informatico, è soggetto a continui aggiornamenti e modifiche.

Vi sono poi altre operazioni sui dati che vengono svolte da programmi applicativi realizzati ad hoc per operare in c.d. modalità *background*, ovvero senza che l'operatore, ma non il sistema, percepisca alcunchè: è ad esempio il caso dei vari *demoni* che svolgono periodicamente e automaticamente delle funzioni routinarie, come ad esempio il *download* della posta elettronica sul programma cliente di posta, o l'aggiornamento dei programmi o, ancora, il controllo e l'eliminazione di virus.

Vi sono infine altre operazioni, come ad esempio l'attivazione della funzione di ricerca di una parola o di un file archiviato sull'hard disk o l'accensione e lo spegnimento del dispositivo, che sono apparentemente ancora più superficiali e meno invasive delle precedenti, tanto da far ritenere all'operatore medio che tali funzioni addirittura preservino intatti i dati, mentre sono tra quelle funzioni che determinano la maggior quantità di variazioni o perdite di dati.

Proprio a quest'ultimo proposito, sono impressionanti i risultati di una ricerca[247] che sulla base della tassonometria delle variazioni dei dati archiviati

---

[246] "*Si dice sistema operativo un programma (software che insieme alla macchina, in senso fisico, costituisce la base delle possibili modalità operative e in particolare ha il compito di governare o pilotare i componenti fisici e controllare l'esecuzione di altri programmi e fornire loro servizi specifici nonché di fungere da tramite tra utente e macchina*", cosi in BONI M., op.cit. p. 180.

[247] CINTI M., Quantificazione ed individuazione delle alterazioni dei dati nell'ambito di indagini di Informatica Forense, tesi di laurea, a.a. 2010-2011, Facoltà di Scienze matematiche,

sull'hard disk di un personal computer al compimento di operazioni molto semplici, comprova l'estrema vulnerabilità dei dati anche a seguito di un singolo accesso. Nell'esperimento, l'autrice ha creato alcune macchine virtuali[248] con diversi sistemi operativi e un numero ridotto ma identico di programmi e file (tra i quali un client di posta elettronica, un antivirus, un file di testo, un file grafico); quindi, ha misurato le variazioni intercorse al compimento di operazioni molto semplici quali accensione, spegnimento, apertura e chiusura di un file, lancio della funzione "cerca". Al compimento di ciascuna operazione, sono state misurate e comparate le rilevanti variazioni di dati intervenute, così come esaminando le operazioni apparentemente più banali, quali l'accensione e lo spegnimento del computer, sono risultate variazioni più o meno diverse a seconda dei diversi sistemi operativi; la mera attivazione della funzione "ricerca" (find) di una parola attivata con il sistema operativo ha causato sino al 75% dei dati archiviati nel computer.

Orbene, i dispositivi informatici, ancor più se connessi in rete o alla Rete, sono soggetti a tali tipi di fenomeni, il cui studio è ancora di là dall'essere intrapreso con metodo sistematico.

In ogni caso, tale approccio empirico consente sin d'ora di concludere che ogni interazione, anche minima, con un dispositivo informatico determina variazioni dei dati archiviati tali da imporre l'adozione di appropriate tecniche informatiche e, per ciò che rileva in questa sede, nel quadro di schemi giuridici che tengano conto di tale caratteristica di irreversibile modificabilità.

Orbene, se la realtà empirica della dimensione informatica è quella appena descritta, allora le interazioni con i sistemi informatici e telematici, anche le più semplici ed apparentemente innocue, costituiscono operazioni che alterano – se non, addirittura, disperdono – irreversibilmente quantità considerevoli di dati e quindi di informazioni.

Pertanto, all'esito della disamina fenomenologica, risulta doveroso qualificare come irripetibili le attività di interazione con i dati di un sistema informatico e in tutte le accezioni note sotto tale espressione:

1) in senso "giuridico" (art. 360), ricorrente allorquando si tratti di accertamenti che "riguardano persone, cose o luoghi il cui stato è soggetto a modificazione" "tali da far perdere loro in tempi brevi, ogni valenza probatoria in relazione ai fatti oggetto di indagini e di eventuale futuro giudizio", come per il caso in cui, ad esempio, si debbano acquisire dati archiviati in un dispositivo per proteggerli da rischi di cancellazione o sovrascrittura attuata automaticamente dal sistema operativo;

fisiche e naturali, Alma Mater Studiorum · Università di Bologna, in *http://amslaurea.unibo.it/2736/1/cinti_mariagrazia_tesi.pdf*.

[248] L'uso delle macchine virtuali per tale esperimento, costituisce un semplice modello paradigmatico delle potenzialità di tali tecnologie nella riproduzione artificiale di procedure informatiche utilizzabili negli esperimenti giudiziali informatici.

2) irripetibilità nel senso di "indifferibilità" (art. 360, 4° c.), che si verifica allorquando gli accertamenti sono di natura fisica tale che, ove differiti, non possono più essere utilmente compiuti, circostanza ricorrente nel caso in cui, ad esempio, sia necessario acquisire da una memoria primaria i dati archiviati esposti non solo al rischio di repentina e definitiva modificazione, ma al ben più grave rischio di dispersione e perdita;

3) irripetibilità in senso "tecnico" (art. 117 disp. att.), che ricorre allorquando gli stessi accertamenti determinano "modificazione delle cose, dei luoghi, o delle persone tali da rendere l'atto non ripetibile", come nel caso in cui si debba accedere al dispositivo per acquisire i dati in esso archiviati[249].

A mio parere, quest'ultima costituisce l'evenienza più ricorrente atteso che, come dimostrato dall'esperimento citato, la mera interazione con il dispositivo mette a rischio i dati archiviati sul sistema e, in ogni caso, il rischio cui vengono sottoposti i dati in relazione all'importanza rivestita dalla loro integrità ai fini del procedimento, impone non solo che il consulente tecnico eviti ogni rischio per l'integrità dei dati, ma che, nel dubbio, ricorra preventivamente alle migliori procedure tecniche previste per il trattamento dei dati ad uso processuale[250].

Non ci si nasconde che la qualificazione delle operazioni di acquisizione e analisi dei dati archiviati in dispositivi digitali potrebbe essere oggetto di una ulteriore e diversa qualificazione che, per quanto datata, potrebbe trovare ancora seguito.

Ci si riferisce al diverso approccio basato sulla tradizione esegetica del codice di procedura penale a marcata impronta inquisitoria e sostituito da quello attualmente in vigore, per il quale la Cassazione distingueva tra "semplici

---

[249] Notevoli analogie al trattamento dei dati digitali presenta il caso deciso da Cass., sez. V pen. 30 settembre 2013 n. 50589, per la quale: "*La consulenza disposta dal p.m. sul nastro carbografico di una macchina da scrivere costituisce accertamento tecnico irripetibile, sicché, qualora non si utilizzi la procedura garantita di cui all'art. 360 c.p.p. nell'ambito di un procedimento a carico di persone note, e sia anche solo ipotizzabile che detto accertamento possa riguardare taluno degli indagati, il contenuto dei "pizzini", ricostruito attraverso l'esame predetto, deve ritenersi inutilizzabile.*".

[250] Vanno ancora una volta ricordate le Linee Guida previste dai seguenti Standard Internazionali "ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence" pubblicato in versione definitiva il 15 ottobre 2012 (Linee guida per l'identificazione, raccolta, acquisizione e conservazioni delle prove digitali); "ISO/IEC 27038:2014 Information technology - Security techniques - Specification for digital redaction" pubblicato in versione definitiva il 13 marzo 2014 (Lienee guida per le specifiche di redazione digitale); "ISO/IEC 27041:2015 Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative method" pubblicato in versione definitiva il 15 giugno 2015 (Linee guida sulla garanzia di idoneità e adeguatezza dei metodi di investigazione); "ISO/IEC 27042:2015, su "Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence" pubblicato in versione definitiva il 19 giugno 2015 (Linee guida per l'analisi e l'interpretazione di prove digitali); "ISO/IEC 27043:2015 "Information technology - Security techniques - Incident investigation principles and processes" pubblicato in versione definitiva il 1 marzo 2015 (Principi e processi per l'investigazione di incidenti informatici).

rilievi" e "accertamenti tecnici", ove: "*La nozione di accertamento riguarda non la constatazione o la raccolta di dati materiali pertinenti al reato e alla sua prova, che si esauriscono nei semplici rilievi, ma il loro studio e la relativa elaborazione critica, necessariamente soggettivi e per lo più su base tecnico-scientifica. La distinzione trova testuale conferma normativa in ripetute disposizioni del nuovo codice che menzionano separatamente i termini "rilievi" ed "accertamenti", con l'implicita assunzione, per ciascuno, del significato specifico precedentemente delineato*"[251].

Seguendo tale impostazione, le operazioni di acquisizione di dati digitali avrebbero potuto addirittura essere qualificati come mera "raccolta di dati materiali pertinenti al reato e alla sua prova" nell'ambito del più ampio concetto di "rilievi", ma in tal caso l'intera attività sarebbe stata relegata al diverso ambito degli atti di polizia giudiziaria, secondo una sistematizzazione incompatibile con una lettura costituzionalmente orientata dell'art. 117 disp. att. del codice dell'89 rispetto all'art. 111 Cost. nel testo novellato.

Per quanto tale tipo di classificazione sia del tutto impraticabile in quanto incompatibile con l'attuale assetto normativo, tale distinzione, come si vedrà, è stata invece recuperata dalla giurisprudenza più recente per approdare agli esiti che si affronteranno in seguito.

Più di recente, invece, una delle sentenza maggiormente significative sugli aspetti generali del concetto di irripetibilità, è quella pronunciata dalla Cassazione a Sezioni Unite nel 2006[252].

Con tale decisione la Cassazione, muovendo dal concetto di irripetibilità in relazione agli atti di polizia giudiziaria, *incidenter tantum*, esamina anche la questione della definizione degli accertamenti tecnici ripetibili e non, così definendo gli ambiti: "(...) *In parte diversa è la nozione di non ripetibilità riguardante la descrizione di luoghi, cose o persone di interesse per lo sviluppo delle indagini, o per la celebrazione del processo, che assume carattere di irripetibilità quando si tratti di situazioni modificabili per il decorso del tempo (carattere peraltro presente anche negli atti tipici non ripetibili). In questi casi la non ripetibilità deriva non da un'assoluta impossibilità di descrizione delle situazioni modificabili ma dalla perdita di informazioni che deriva dalla possibilità di mutamento dello stato di luoghi, cose o persone che non renderebbe possibile, in caso di necessità, la ripetizione dell'atto.*

In questi casi la non ripetibilità trova un'indiretta conferma normativa nelle disposizioni degli artt. 354 commi 2° e 3° (che abilita la polizia giudiziaria a compiere rilievi sullo stato delle cose, dei luoghi e delle persone nel caso di pericolo di alterazione, dispersione o modificazione), 360 (che

[251] Cass., I, 14 marzo 1990 n. 301.
[252] Cass. S.U. 17 ottobre 2006 – 18 dicembre 2006 n. 41281, Prisco, in *http://www.altalex.com/documents/news/2007/04/23/cassazione-penale-ss-uu-sentenza-18-12-2006-n-41281*.

abilita il pubblico ministero, in situazioni analoghe, a disporre accertamenti tecnici non ripetibili utilizzabili nel dibattimento) e 391 decies commi 2° e 3° c.p.p. (ove si fa espresso riferimento alla documentazione di atti non ripetibili compiuti dal difensore in occasione dell'"accesso ai luoghi" e agli accertamenti tecnici non ripetibili). Queste norme consentono infatti, in deroga alla disciplina ordinaria, di svolgere attività investigativa - la cui documentazione è utilizzabile in dibattimento - a soggetti che di regola non dispongono dei relativi poteri proprio perché in dibattimento non sarebbe più possibile dare luogo al corrispondente mezzo di prova se non con la perdita della genuinità e quindi dell'affidabilità dell'atto. (...)"

Quindi la Cassazione riconosce lo spazio alla qualificabilità di non ripetibilità – e quindi ex art. 360 e 391 *decies* 2° e 3° c., a quei casi di "descrizione di...cose" di interesse per lo sviluppo delle indagini, o per la celebrazione del processo, e che assumono carattere di irripetibilità quando si tratti di situazioni modificabili per il decorso del tempo.

Come già evidenziato, in questi casi sono da annoverarsi anche le descrizioni di dispositivi digitali.

Proseguendo nella differenziazione, la Cassazione osserva: "(...) *E la conferma che* ***il concetto di non ripetibilità è strettamente ricollegato (anche) alla modificazione di cose, luoghi e persone si rinviene nel disposto dell'art. 117 delle disp. att. c.p.p., che estende la disciplina dell'art. 360 c.p.p. agli accertamenti che modifichino le situazioni indicate, e dell'art. 223 delle medesime disposizioni che prevede una particolare disciplina per le analisi di campioni con l'espressa previsione di acquisizione al fascicolo per il dibattimento dei verbali di analisi non ripetibili e dei verbali di revisione di analisi.*** *(...)***"**

La Corte, quindi, ritiene che: *"In conclusione ciò che giustifica l'attribuzione della qualità di non ripetibilità ad un atto della polizia giudiziaria, del pubblico ministero o del difensore è la caratteristica di non essere riproducibile in dibattimento. Ma ciò non è sufficiente: nel bilanciamento di interessi tra la ricerca della verità nel processo e sacrificio del principio costituzionale relativo alla formazione della prova è necessario che l'atto abbia quelle caratteristiche di genuinità e affidabilità che possono derivare soltanto da quell'attività di immediata percezione cristallizzata in un verbale che inevitabilmente andrebbe dispersa ove si attendesse il dibattimento.".*

Pertanto, viene consolidato il concetto per il quale l'irripetibilità è strettamente ricollegata non solo all'impossibilità di ripetere l'operazione in dibattimento, ma (anche) alle modificazioni che nel frattempo subiscono le cose.

Tornando invece al regime giuridico degli "*Accertamenti tecnici che modificano lo stato dei luoghi, delle cose o delle persone",* l'art. 117 disp. att.,

impone che:"*1. Le disposizioni previste dall'articolo 360 del codice si applicano anche nei casi in cui l'accertamento tecnico determina modificazioni delle cose, dei luoghi o delle persone tali da rendere l'atto non ripetibile."*

Alla luce dei principi appena ripercorsi, si può affermare che in linea generale, salve alcune eccezioni concretamente verificabili, vi sono molteplici considerazioni che fanno propendere per la prevalenza di tale opzione classificatoria rispetto a quella che ritiene ripetibili gli accertamenti che comportano interazione con i dispositivi e i dati digitali, quali:

- le caratteristiche fisiche dei bit, le cui modifiche, sono irreversibili;
- la modificabilità dei dati esterni dei file conseguente a cause fisiologiche o accidentali, o a modifiche, volontarie o accidentali;
- la fragilità intrinseca dei materiali che compongono la struttura delle memorie hardware;
- l'estrema facilità con la quale i dati archiviati possono essere alterati, modificati, cancellati senza che l'operatore lasci traccia dell'avvenuta modifica.

In tali circostanze, ove il rischio di alterazione irreversibile dei dati dovesse realizzarsi, verrebbe meno la loro capacità rappresentativa e con essa tutto il patrimonio informativo che dagli stessi può essere tratto ai fini dell'indagine o della difesa.

Chiariti i termini del problema, le implicazioni giuridiche possono essere comprese solo se calate nella più ampia problematica relativa al rapporto tra prova scientifica e diritto[253] e in particolare, della misurazione quantitativa delle modificazioni che affliggono un dispositivo, e soprattutto i dati in esso registrati, a seguito di azioni e interazioni con il medesimo.

Va rilevato che la dimensione tassonometrica delle variazioni è ancora oggetto di intuizione che si tramanda tralaticiamente, e ancora non trova ancora adeguati approfondimenti su base sperimentale.

Pertanto, le incertezze registrabili si giustificano considerando che mentre in ambito informatico sono molto chiari i fenomeni che affliggono la stabilità dei dati, tanto da assurgere a postulati tecnico-scientifici, in ambito giuridico tale consapevolezza non è ancora diffusa.

Pertanto, in mancanza di una solida base sperimentale che possa imporre il corretto inquadramento della questione empirica dell'alterabilità dei dati, in ambito giuridico è ancora dato assistere ad ampie oscillazioni tra i due possibili schemi in tema di accertamenti tecnici.

A tale dimensione riconduco anche la diversità di orientamenti che sul punto possono ancora registrarsi in dottrina e che si riflettono anche nella giurisprudenza.

[253] Cfr. DOMINIONI O., op.cit., *passim.*

Infatti, se la dottrina non è uniformemente orientata, la giurisprudenza è attestata su posizioni variegate: in particolare, mentre la giurisprudenza di merito conosce varie posizioni che oscillano tra la concezione ripetibile e quella irripetibile, l'attuale orientamento maggioritario della Cassazione tende ad escludere che gli accertamenti tecnici ad oggetto informatico rientrino nella categoria degli accertamenti tecnici non ripetibili.

Per concludere sul punto, ritengo che la qualificazione secondo l'orientamento maggioritario si ponga in contrasto con l'art. 111 della Costituzione, con lo spirito e la lettera della Convenzione di Budapest e con il sistema processuale come modificato dalla legge di ratifica della stessa.

6.4 La giurisprudenza di merito sugli accertamenti tecnici

In merito alla qualificabilità degli accertamenti tecnici informatici, mentre la giurisprudenza di merito conosce varie posizioni, l'attuale orientamento maggioritario della Cassazione, come si dirà meglio in seguito illustrando le decisioni rilevanti sul punto, tende ad escludere che essi rientrino nella categoria degli accertamenti tecnici non ripetibili.

Tale qualificazione giuridica è in evidente contrasto con lo spirito e la lettera della Convenzione di Budapest e con lo stesso sistema introdotto dalla della legge di ratifica della stessa.

Eppure, in passato, la prima giurisprudenza di merito, ancor prima dell'avallo della Convenzione di Budapest e della L. 48/08, aveva posto fausti auspici verso la corretta impostazione della questione, preconizzando che le attività di duplicazione dei dati potessero porre problemi di irripetibilità, con il conseguente problema di scegliere la procedura più opportuna.

In particolare, sin dal 2000, il Tribunale di Torino[254], tra le altre affermazioni relative alla fattispecie dedotta in giudizio, aveva correttamente posto alcuni punti fermi sulle questioni oggetto della presente disamina:"(...) *Pare invece accoglibile il motivo di riesame concernente la non necessità del sequestro dell'hard disk. Infatti nulla impediva agli agenti di p.g., per di più appartenenti a Sezione specializzata nell'ambito dai reati informatici di* ***procedere ad una copia integrale dell'hard disk, con specificazione verbale di ogni singola operazione. Inoltre qualora vi fossero stati problemi di irripetibilità, nulla impediva al P.m. di procedere ex art. 360 c.p,p.*** *anche a seguito del sequestro* ***ovvero in assenza dei problemi suddetti ex art 359 c.p.p.****..(...)".*

È evidente come detta decisione, prescrivendo la necessità di procedere all'effettuazione della "copia integrale" dell'hard disk, dando prova di considerare le problematiche tecniche presupposte, non abbia indicato quale tra

[254] Trib. riesame Torino, Ord. 7 febbraio 2000; il testo riportato è quello disponibile in *http:// www.ictlex.net/index.php/2000/02/07/trib-torino-sez-riesame-ord-7-febbraio- 2000/.*

i due possibili schemi procedurali optare per dare forma giuridica a tali operazioni, rimettendo al pubblico ministero la valutazione dell'elemento costituente il presupposto di fatto dell'una o dell'altra opzione, vale a dire l'esistenza di problemi di "irripetibilità".

Va quindi riconosciuto a tale sentenza il merito di aver posto la questione della qualificazione delle operazioni di duplicazione dell'hard disk avanti alle due alternative.

Negli anni successivi, ancor prima dell'entrata in vigore della L. 48/08, la prassi di diversi uffici inquirenti si è ispirata allo schema dell'irripetibilità delle operazioni di acquisizione dei dati[255].

All'estremo opposto dell'arco temporale, successivamente alla Legge 48/08, il Tribunale di Vigevano sul caso Garlasco, pur muovendosi con maggior dimestichezza tra i temi dell'Informatica forense, ha dato risposta negativa alla questione se le operazioni tecniche possano rientrare nella nozione processual penalistica di accertamento tecnico ai sensi degli artt. 359/360 c.p.p..

Il Tribunale ha infatti ritenuto che "*(...) per configurare tale attività come accertamento tecnico ai sensi degli artt. 359 e 360 c.p.p., sarebbe stato necessario che la stessa fosse consistita in un'analisi completa ed approfondita del documento informatico in sequestro sulla base di un quesito posto dal pubblico ministero, che i soggetti procedenti possedessero le competenze tecniche al fine di svolgere gli accertamenti suddetti e che gli stessi alla fine avessero dato conto, mediante argomentata relazione scritta, dei risultati raggiunti.*

In realtà, si è trattato di un'attività compiuta da ufficiali di polizia giudiziaria non esperti in materia, che hanno proceduto senza un previo quesito e che al termine hanno redatto solo un verbale in cui hanno riportato la data del compimento dei suddetti indicati atti. Dunque, siamo dinnanzi ad atti di polizia giudiziaria che rientrano, invero, nell'ambito del combinato disposto degli artt. 55 e 348 c.p.p. (attività finalizzata a raccogliere ogni elemento utile alla ricostruzione del fatto e all'individuazione del colpevole) e non integrano la fattispecie dei veri e propri accertamenti tecnici di cui agli artt. 359 e 360 c.p.p.. (...)".

Come si è già detto il Tribunale ha escluso che gli atti compiuti dalla polizia giudiziaria potessero essere qualificabili come accertamenti tecnici in quanto non furono compiuti accertamenti approfonditi del documento informatico sulla base di un quesito posto dal pubblico ministero, né gli operatori avevano le relative competenze, né questi relazionarono sui risultati dell'attività. Si sarebbe trattato invece di attività rientrati tra gli accertamenti

[255] Tra le altre che hanno adottato quasi sistematicamente lo schema degli accertamenti irripetibili, vanno ricordate le Procure della Repubblica presso i Tribunali di Torino, Milano, Latina.

urgenti. Ma, come si è detto, la polizia giudiziaria ha realizzato di fatto tale attività interagendo con un dispositivo digitale il cui stato si altera alla mera accensione o al mero accesso, il che fa scattare la previsione dell'art. 117 disp. att.. A nulla vale l'eventuale carenza di direttive delle operazioni tecniche, ad indagini inoltrate ove, delle due, accrescerebbe gli ampi dubbi e perplessità sulla corretta conduzione tecnico-giuridica del procedimento. Inoltre, in questi casi, il rischio dell'inutilizzabilità dei risultati è uno spettro troppo severo a carico di chi avrebbe potuto e dovuto provvedere diversamente e instaurare l'accertamento garantito, perché possa essere assunta in casi di rilevante gravità.

Prosegue la sentenza: "*(...) Ciò posto, non vi è alcun dubbio, tuttavia, che le condotte poste in essere sul computer da parte della polizia giudiziaria, sebbene superficiali, dovessero, proprio per la intrinseca fragilità del contenuto del documento informatico di cui sopra, essere eventualmente svolte (se proprio necessario) con l'assistenza di ausiliari tecnici che avrebbero messo in atto le necessarie preventive cautele tecniche atte ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso provvedendo, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicurasse la conformità della copia all'originale e la sua immodificabilità.*

Si deve, dunque, ritenere che questa preliminare e sommaria attività investigativa è stata posta in essere secondo una metodologia sicuramente scorretta, disattendendo i protocolli già invalsi in materia (anche prima dell'entrata in vigore della legge citata) venendo, quindi, a costituire una causa di potenziale alterazione e dispersione del contenuto del documento informatico. (...)"

Il Tribunale, quindi, in antitesi all'assunto della ripetibilità delle operazioni elenca i presupposti che caratterizzano l'irripetibilità mettendo in evidenza il principio della fragilità del contenuto dei documenti informatici e quindi dei bit, nonchè la conseguente necessità di prevenire ed evitare l'alterazione e la dispersione dei dati adottando le tecniche scientifiche messe a punto e già operanti prima della L. 48/08 come normale metodologia scientifica di trattamento dei dati a fini processuali. Ciò rileva sia ai sensi dell'art. 360 che, come si è detto, dell'art. 117 disp. att..

In conclusione sul punto, anche la giurisprudenza di merito, partita con il piede giusto, sembra aver concluso la sua parabola esegetica assestandosi sulle posizioni che sembrano essere ormai consolidate nella giurisprudenza di merito.

6.5 La giurisprudenza di legittimità sugli accertamenti tecnici

Solo di recente le questioni giuridiche appena ripercorse sono approdate all'esame della Cassazione la quale sembra che stia chiudendo il cerchio ricorrendo a diversi approcci che, con varie sfumature, si stanno affermando come principi tralatici in direzione divergente da quella appena prospettata.

A parere dello scrivente, le soluzioni che stanno emergendo si pongono in aperto contrasto sia con la realtà fattuale ben chiara a qualunque esperto di informatica, sia con le norme tecniche, sia con una corretta lettura delle norme di settore.

Come si avrà modo di specificare all'esito della seguente disamina delle pronunce più rappresentative sulla questione, gli approdi sono tutt'altro che pacifici sia sul piano giuridico, sia sul piano prettamente empirico, ambito dal quale proverranno i maggiori pericoli di involuzione operativa.

6.5.1 Cass., sez. I, sent. 26 febbraio 2009 – 18 marzo 2009, n. 11863

Affrontando il tema della qualificabilità delle operazioni di "estrazione di copia di "file" da un computer oggetto di sequestro", una prima decisione ha stabilito che:"*L'estrazione dei dati contenuti in un supporto informatico, se eseguita da personale esperto in grado di evitare la perdita dei medesimi dati, costituisce un accertamento tecnico ripetibile."*[256]

Con tale decisione la Suprema Corte ha spostato il baricentro del problema dalla natura fisica dei dati e relativi supporti, alle personali abilità del tecnico, come se le qualità fisiche oggettive dei bit potessero essere preservate dalle qualità soggettive dell'operatore. Anche tale operazione esegetica oblitera tutte le considerazioni empiriche già svolte in favore dei percorsi applicativi delle norme che tengono conto della peculiarità fisica dei dati, ma non è l'ultima. In ogni caso, se l'operazione è ripetibile essa potrà e dovrà essere ripetuta in sede dibattimentale, ove le tecniche a disposizione consentono altresì di verificare eventuali alterazioni dei dati.

6.5.2 Cass., sez. I, sent. 5 marzo 2009-2 aprile 2009, n. 14511

In un altro caso, la Cassazione si è spinta oltre qualificando in modo diverso le operazioni di estrazione di copia di file, giungendo ad un esito ancor più incerto, ove ha stabilito che: "*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 recare pregiudizio alla genuinità del contributo conoscitivo nella*

[256] Cass., sez., I, sent. 26 febbraio 2009 – 18 marzo 2009, n. 11863, in CED Cass. n. 243922.

prospettiva dibattimentale, essendo sempre comunque assicurata la riproducibilità d'informazioni identiche a quelle contenute nell'originale."[257].

Orbene, in tale decisione viene obliterata ogni considerazione tecnico-scientifica che dimostra il contrario degli assunti, con il paradosso di giungere a conclusioni ribaltate rispetto ai fenomeni empiricamente verificabili.

Infatti, la Suprema Corte consegna agli operatori alcune direttive che costituiscono una vera e propria griglia per la qualificazione giuridica dei fatti aventi ad oggetto dati digitali:

1) *l'attività di estrazione di copia di "file" da un computer oggetto di sequestro non è attività irripetibile in quanto*
2) *essa non comporta alcuna attività di carattere valutativo su base tecnico-scientifica,*
3) *né determina alcuna alterazione dello stato delle cose, tale da recare pregiudizio alla genuinità del contributo conoscitivo nella prospettiva dibattimentale,*

Per converso, secondo tale schema, ove l'attività di estrazione di copia di file da un computer, *comporti attività di carattere valutativo su base tecnico-scientifica,* allora tale operazione sarà qualificabile come irripetibile.

Tale impostazione approda ad un esito paradossalmente rovesciato rispetto alla dimensione ontologica delle operazioni, atteso che la corretta impostazione è quella esattamente contraria a quella ritenuta dalla Corte:

1) è l'attività di estrazione di copia di "file" da un computer oggetto di sequestro che costituisce attività irripetibile in quanto:

2) essa non comporta alcuna attività di carattere valutativo su base tecnico-scientifica,

3) ma può determinare alterazione dello stato delle cose, tale da recare pregiudizio alla genuinità del contributo conoscitivo nella prospettiva dibattimentale.

Inoltre, a ciò potrebbe aggiungersi il corollario per il quale, così operando, l'attività di carattere valutativo su base tecnico-scientifica svolta sulla copia è sempre ripetibile, e in quanto tale può essere sempre ripetuta al dibattimento, peraltro sotto la supervisione del giudice.

Pertanto, l'attività di estrazione del file dovrebbe essere effettuata sempre ai sensi dell'art. 360, anche al solo fine di calcolare l'impronta del compendio originario in base al quale poter poi svolgere l'attività di confronto per accertare l'integrità dei dati, la loro eventuale modificazione ed eventuali responsabili della catena di custodia. Invero, su tale facoltà - fondamentale per la parte che

[257] Cass. Sez. I, sent. 5 marzo 2009-2 aprile 2009, n. 14511, in Cass. pen. 2010, p. 1522 con nota LORENZETTO E., Utilizzabilità dei dati informatici incorporati su computer in sequestro; dal contenitore al contenuto passando per la copia e in Dir. pen proc., 2009, p. 337 con nota RICCI A.E, Digital evidenze e irripetibilità delle operazioni acquisitive, op.cit.

non ha proceduto all'acquisizione – la Cassazione recupera l'obiter già incontrato nella sentenza "Vierika", per il quale: "(...) *Lo stesso ricorrente, del resto, non ha in concreto allegato alcuna forma di distruzione o alterazione dei dati acquisiti, tale da confortare il suo assunto, ma si è limitato a prospettare ipoteticamente alcune situazioni potenziali che esulano dalla fattispecie sottoposta all'esame della Corte* (...)".

Che tale opzione sia spesso impraticabile, è confermata dal fatto che non sempre è possibile evidenziare le modificazioni o alterazioni dei dati acquisiti durante la fase delle investigazioni e delle indagini perché spesso non sono stati acquisiti, o vengono a mancare, i reperti originari costituenti l'unico valido metro di paragone rispetto ai dati acquisiti.

Tuttavia, tale decisione pone un punto fermo, il cui unico motivo di pregio è costituito dal fatto che i principi esposti, in quanto nuovi e pronunciati in merito ad attività svolte dagli organi dell'accusa, potranno valere anche per la difesa che voglia acquisire materiale informatico mediante attività tecniche simmetriche, sia empiricamente che giuridicamente.

6.5.3 **Cass., sez. II, sent. 4-16 giugno 2015, n. 24998**

A quanto sopra, è seguita un'ulteriore decisione della Cassazione[258] la quale, ha notevolmente ampliato l'ambito dei temi sino ad ora percorsi.

Infatti, pur dando atto dei cambiamenti introdotti dalla L. 48/08 di Ratifica della Convenzione di Budapest, la seguente decisione ripropone i principi che si muovono nella direzione già più volte criticata: "(...) *In punto di diritto, è ben noto che la L. n° 48 del 2008 - nel ratificare e dare esecuzione alla Convenzione del Consiglio d'Europa sulla criminalità informatica firmata a Budapest il 23.11.2001 - ha novellato diverse norme del c.p.p. consentendo accertamenti urgenti della Polizia Giudiziaria in materia di perquisizioni, ispezioni, e sequestri di programmi o sistemi informatici: cfr art. 244 c.p.p., co. 2, art. 247 c.p.p., co. 1-bis, art. 248 c.p.p., co. 2, artt. 254, 254-bis, 256, 259 e 260 c.p.p., art. 352 c.p.p., co. 1-bis, art. 353 c.p.p., art. 354 c.p.p., co. 2.*

Il dato comune che si può rinvenire dalla lettura delle suddette norme è che, nell'effettuare le operazioni ivi previste, la Polizia Giudiziaria deve adottare "misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione", nonché provvedere, "ove possibile alla loro immediata duplicazione su adeguati supporti mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità". (….).

[258] Cass., sez. II, sent. 4-16 giugno 2015 n. 24998, con nota di FRATTALLONE S., La mera estrazione dei dati da un computer non è atto irripetibile, in *http://www.frattallone.it/penale/561-penale-la-mera-estrazione-dei-dati-da-un-computer-non-e-atto-irripetibile*.

Quindi la Suprema Corte inizia a fare i conti con le previsioni della L. 48/08 muovendo proprio dai principi relativi agli obblighi di adozione delle misure tecniche finalizzate alla conservazione dei dati e alle modalità minime di trattamento finalizzate a garantire il livello minimo di conformità ai dati originari e la loro immodificabilità ("*...la Polizia Giudiziaria deve adottare misure tecniche dirette ad assicurare la conservazione del dati originali e ad impedirne l'alterazione", nonché provvedere, "ove possibile alla loro immediata duplicazione su adeguati supporti mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità...").*

Tuttavia, prosegue la Corte, non vi sono norme che prescrivono come tutto ciò debba essere attuato, né le sanzioni in caso di inosservanza: "*(...) Nessuna norma del codice, però, descrive quale debba essere la procedura da seguire, nè alcuna norma prevede sanzioni di alcun genere per l'eventuale violazione delle suddette prescrizioni: in altri termini, per l'acquisizione ed utilizzazione dei dati informatici il legislatore non ha ritenuto di riproporre tutta la minuziosa normativa che, ad es., presidia l'istituto delle intercettazioni.(...)";*

Orbene, è evidente che tale lettura di fatto sterilizzi il portato della L. 48/08 in direzione sostanzialmente abrogatrice.

Infatti, se per "procedura da seguire" si intende uno schema procedurale di dettaglio, va rilevato come le indicazioni introdotte dalla L. 48/08 – con tutti i limiti già rassegnati – costituiscono già il *minimum* sufficiente a indirizzare l'azione degli operatori verso il perseguimento delle finalità di corretta acquisizione e conservazione dell'integrità dei dati come indicate dalla Convenzione di Budapest. In altre parole, l'attuale assetto – per quanto, si ripete, perfettibile - fornisce già le coordinate delle finalità da perseguire e delle modalità di massima per realizzarle, senza necessità di ulteriore specificazione giuridica.

Se invece per "procedura da seguire" si intende la modalità tecnica per realizzare il nuovo dettato, allora la considerazione appare ovvia: se il legislatore avesse dovuto specificare le modalità tecnico-scientifiche per realizzare il principio evidenziato ("*...la Polizia Giudiziaria deve adottare misure tecniche dirette ad assicurare la conservazione del dati originali e ad impedirne l'alterazione", nonché provvedere, "ove possibile alla loro immediata duplicazione su adeguati supporti mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità...")* avrebbe dovuto inserire nel codice di procedura penale, normandolo, l'intero apparato tecnico studiato dall'Informatica forense costituente il presupposto scientifico alla base dei principi della Convenzione di Budapest. Ciò avrebbe causato il paradosso per il quale, a seguito dell'innovazione tecnologica

notoriamente soggetta a radicali e frequenti salti evolutivi[259], il codice avrebbe dovuto essere aggiornato a stagioni alterne per adeguarlo alle nuove tecniche che si susseguono nel tempo. Al contrario, la Convenzione di Budapest, presupponendo le finalità da perseguire, ovvero la conservazione dell'integrità dei dati originari e la loro duplicazione a fini forensi, ha formalizzato i principi minimi, le modalità di massima per realizzarle, ma lasciandolo opportunamente fuori dall'ambito dell'intervento normativo tutto l'ambito tecnico-scientifico del corretto trattamento dei dati ritenuto un mero presupposto idoneo a garantire l'automatica applicazione delle tecniche che realizzano le finalità codificate.

Tutto ciò, fermo restando che sin dal 2012 l'ISO/IEC ha pubblicato le amplissime e specifiche Linee guida 27037:2012 regolamentazioni tecniche su base scientifica per il trattamento della *digital evidence* cui si può e deve fare riferimento per attuare le norme di metodo previste dal codice. Pertanto, se può essere vero che i fatti oggetto del procedimento erano probabilmente concomitanti con il varo delle Linee guida ISO/IEC, diversamente, al momento della decisione in esame, tali Linee guida erano state pubblicate da almeno tre anni e la Corte non poteva ignorarle.

La decisione così prosegue: "*(...) Il compito dell'interprete consiste, quindi nello stabilire: a) innanzitutto, se i dati informatici siano o meno stati alterati: il che costituisce oggetto di un evidente accertamento di fatto; b) in caso affermativo, stabilire in cosa consista l'alterazione e, quindi, se il dato informatico possa o meno continuare ad essere utilizzabile nonostante l'alterazione: anche questo aspetto costituisce oggetto di un accertamento di fatto in quanto, alla fin fine, si tratta di accertare se il dato informatico, nonostante l'alterazione, continui ad essere attendibile. (...)*".

In tale passo, la decisione circoscrive correttamente il campo di azione dell'interprete, per quanto non sia del tutto condivisibile che esso sia del tutto relegabile alle questioni di fatto.

"(...) La conclusione alla quale si è pervenuti, trova un puntuale riscontro nella giurisprudenza di questa Corte la quale, in fattispecie similari, ha ritenuto che:

a) non esiste, ad oggi, uno standard prestabilito per la metodologia di trattamento ed analisi delle prove informatiche: Cass. Sez. F., Sentenza n° 44851 del 2012;

b) non da luogo ad accertamento tecnico irripetibile l'estrazione dei dati archiviati in un computer, trattandosi di operazione meramente meccanica, riproducibile per un numero indefinito di volte: Cass. 23035/2009 rv. 244454;

[259] Si pensi solo al periodo di diciotto mesi previsto dalla Legge di Moore per il raddoppio delle capacità delle memorie e l'effetto che esse hanno su tutto il settore dell'ICT; cfr. *https://it.wikipedia.org/wiki/Legge_di_Moore*.

Cass. 11863/2009 rv. 243922; Cass. 14511/2009 rv. 243150; Cass. Sez. II, n° 42969 del 2011."

La conclusione poggia quindi su due principi che vengono tralaticiamente richiamati e che sono stati già oggetto di ampia critica nel corso della presente disamina che, per economia espositiva, si richiama.

Va semplicemente ricordato che il principio sub a) è smentito dall'esistenza degli standard ISO/IEC 27037:2012 per il trattamento della digital evidence varati nello stesso periodo dei fatti oggetto di processo e da almeno tre anni al momento della decisione in commento, mentre il principio sub b) è smentito dalla qualificabilità delle operazioni di estrazione di dati come accertamento tecnico irripetibile.

La sentenza prosegue con la disamina delle peculiarità del fatto:*"(...) In questa sede, il C., ha convenuto sul fatto che gli accertamenti in questione non sono, in sè, affetti da nullità o inutilizzabilità dei risultati e dei dati acquisiti (cfr pag. 3 ricorso C.), ma ha sostenuto che si trattava di accertamenti tecnici irripetibili sicché avrebbero dovuto essere eseguiti nel contraddittorio fra le parti ex art. 360 c.p.p.: non essendo ciò avvenuto, si era verificata un'ipotesi di nullità ex art. 178 c.p.p., co. 1, lett. c) "con la conseguenza ...dell'inutilizzabilità della prova informatica costituita dal file "(omissis)" e dalle riprese del sistema di videosorveglianza quest'ultime insistenti propro nell'archivio informatico dell'hard disk Hi., oggetto di attività additiva" (pag. 14 ricorso).*

Sul punto, va subito osservato che la censura non supera il dato fattuale emergente da entrambe le sentenze di merito e cioè che non vi è alcuna evidenza che possa far ritenere che le eventuali irregolarità effettuate dai Carabinieri nella prima fase dell'acquisizione dei dati informatici, determinò un'irreversibile alterazione dei suddetti dati tanto da rendere i medesimi assolutamente inaffidabili e, quindi, inutilizzabili.

Va, infatti, osservato che la suddetta questione fu oggetto di un ampio dibattito nel processo di primo grado: ma la Corte di Assise, con una motivazione amplissima, accurata e minuziosa (che si legge da pag. 123 a pag. 128 della Sentenza di primo grado) ha preso in esame ogni eccezione della difesa e l'ha confutata alla stregua di puntuali elementi fattuali concludendo che: "dalla deposizione del D. B. risulta dunque che venne dal tecnico effettuata una estrapolazione di dati mediante copia senza alcuna alterazione di dati. Ciò consente di ritenere dunque che gli investigatori avevano lavorato sulla copia, avevano esaminato i file che erano presenti nel computer del C. e, a differenza di quanto prospettato dalla difesa, non avevano agli stessi apportato alcuna modifica. E non è di scarso rilievo il fatto che, come riferito dagli investigatori, venne anche rinvenuto nel computer, tra la molteplicità di documenti, anche quello intestato all'assistente ma. sul quale era apposta la foto del C.. Ciò consente di escludere del tutto l'ipotesi prospettata dalla difesa

circa l'alterazione ad opera di estranei del materiale contenuto nel computer. Del pari va escluso che il materiale fosse già presente nella memoria dell'hard disk che il C. aveva comprato senza formattare ... ovviamente neanche appare credibile quanto sostenuto dalla difesa circa la possibilità che vi sia stato un virus che, inseritosi nel computer del C., abbia alterato i dati in esso inseriti ...".

Riproposta la questione in sede di appello, la Corte l'ha nuovamente disattesa (pag. 19 ss) osservando che l'acquisizione dei dati sugli hard disk effettuata dai CC: "... non sono stati "estratti", bensì soltanto, con consapevolezza del P.M. procedente, copiati su di una pendrive, stante l'urgenza di proseguire nelle indagini, senza, perciò, alterare il contenuto del materiale posto sotto sequestro: in proposito dobbiamo qui ricordare che gli stessi esperti del GAT esaminati, Cap. Ce. e m.llo M. del Nucleo Speciale Frodi Telematiche, hanno confermato che gli accessi, successivi al 18.9, data del sequestro, e precedenti al loro intervento, sono stati di mera lettura e non altro; questa contestazione, tuttavia, prelude ad altra, per cui, detta informalità di operazione, posta in essere dal m.llo D.B. privo di specifica competenza, avrebbe introdotto un virus, che ben potrebbe, secondo alcuni degli appellanti, aver alterato il contenuto del materiale in esame: ciò dovrebbe rendere inutilizzabile il materiale probatorio scaturito dai dati informatici, a partire da quello iniziale, ovvero i "4 file (omissis)", ma in proposito si deve rilevare che, seppure non concordiamo in questa sede con l'assunto della Sentenza, per cui un virus non possa "distruggere", è vero senz'altro che nella fattispecie i files utilizzati a fini probatori distrutti non erano di certo e, se pure un virus possa in astratto alterare i dati, questo comporterebbe un'eventuale alterazione di quelli esterni, come i tempi degli accessi o similia, ma certamente non potrebbe mai modificare il contenuto di un documento (v. anche esami dei citati esperti); rispetto a ciò, diventa ultroneo sottolineare come questo supposto "virus creativo" avrebbe generato delle informazioni, che sarebbero poi, sorprendentemente, andate a convergere il 3.11 - lungi dal venire - con quelle acquisite a mezzo dei dati probatori seguiti al monitoraggio, pedinamento e fermo degli imputati di provenienza sarda"; conclusioni queste ribadite a pag. 27 della Sentenza.

A fronte di due sentenze che, in modo conforme, hanno, in punto di fatto, sostenuto che non vi fu alcuna alterazione significativa dei dati informatici tanto da comprometterne l'attendibilità e, quindi, l'utilizzabilità, si possono trarre le seguenti conclusioni giuridiche: a) qualora ci si trovi innanzi ad una cd. doppia conforme (doppia pronuncia di uguale segno) il vizio di travisamento della prova può essere rilevato in sede di legittimità solo nel caso in cui il ricorrente rappresenti (con specifica deduzione) che l'argomento probatorio asseritamente travisato è stato per la prima volta introdotto come oggetto di valutazione nella motivazione del provvedimento di secondo grado.

Infatti, in considerazione del limite del devolutum (che impedisce che si recuperino, in sede di legittimità, elementi fattuali che comportino la rivisitazione dell'iter costruttivo del fatto, salvo il caso in cui il giudice d'appello, per rispondere alla critiche dei motivi di gravame, abbia richiamato atti a contenuto probatorio non esaminati dal primo giudice) il sindacato di legittimità, deve limitarsi alla mera constatazione dell'eventuale travisamento della prova, che consiste nell'utilizzazione di una prova inesistente o nell'utilizzazione di un risultato di prova incontrovertibilmente diverso, nella sua oggettività, da quello effettivo. Non è possibile, invece, dedurre come motivo il "travisamento del fatto", giacchè è preclusa la possibilità per il giudice di legittimità di sovrapporre la propria valutazione delle risultanze processuali a quella compiuta nei precedenti gradi di merito. Nel caso di specie, entrambi i ricorrenti fondano le loro conclusioni sulla base di una diversa valutazione ora della prova ora del fatto, così come effettuata in modo concorde da entrambi i giudici di merito, sicché le doglianze non possono che essere disattese alla stregua del suddetto pacifico principio di diritto; b) le operazioni effettuate dai Carabinieri sul computer di marca H., prima che il medesimo fosse consegnato al GAT, trattandosi di mera estrazione dei dati informatici, vanno ritenute operazioni ripetibili per tali dovendosi intendere "l'atto contraddistinto da un risultato estrinseco ed ulteriore rispetto alla mera attività investigativa, non più riproducibile in dibattimento se non con la perdita dell'informazione probatoria o della sua genuinità. Sotto tale profilo gli accertamenti ex art. 360 c.p.p. consistono in attività di carattere valutativo su base tecnico-scientifica e non in attività di constatazione, raccolta, prelievo dei dati materiali pertinenti al reato .... Ciò posto, è da escludere che l'attività di estrazione di copia di file da un computer costituisca un atto irripetibile (nel senso in precedenza indicato), atteso che non comporta alcuna attività di carattere valutativo su base tecnico- scientifica nè determina alcuna alterazione dello stato delle cose, tale da recare pregiudizio alla genuinità del contributo conoscitivo nella prospettiva dibattimentale, essendo sempre comunque assicurata la riproducibilità di informazioni identiche a quelle contenute nell'originale": Cass. 14511/2009 op.cit. (...)".

In tale passo va dato rilievo, tra le altre, a due circostanze:

1) la prima, riguarda l'affermazione per cui, avendo entrambe le sentenze di merito concordemente concluso che non vi fu alterazione dei dati all'esito delle operazioni di acquisizione effettuata, si badi bene, con tecniche (trasferimento di file su pendrive) che in Informatica forense sono ritenute inidonee rispetto alle altre tecniche previste dagli standard ISO/IEC 27037:2012[260];

[260] Tra le trattazioni più aggiornate sulle tecniche di acquisizione, cfr. FERRAZZANO M., op. cit.

2) la seconda attiene al rilievo dato alla deposizione del tecnico il quale riferì di aver effettuato "*una estrapolazione di dati mediante copia senza alcuna alterazione di dati*", e che gli investigatori avevano lavorato sulla copia, avevano esaminato i file che erano presenti nel computer del C. e, a differenza di quanto prospettato dalla difesa, non avevano apportato agli stessi alcuna modifica; anche a tal proposito, come già notato sopra, il giudizio di conformità dei dati è basato su formule di stile ad alto contenuto di autoreferenzialità più che derivare dalla verifica empirica, strumentale e matematiche mediante il procedimento tecnico basato su regole scientifiche e svolte nel quadro delle norme procedimentali.

E ancora:"(...) *In altri termini, poiché secondo entrambi i giudici di merito, l'attività compiuta dai Carabinieri sul computer prima della consegna del medesimo al GAT, si concretizzò in null'altro che in una estrazione dei dati informatici per proseguire nell'immediatezza le indagini, la suddetta attività, come ha chiarito questa Corte nelle plurime decisioni op.cit., va ritenuta di mera riproduzione e, quindi, non un atto irripetibile ex art. 360 c.p.p. Che, poi, questa attività possa, in astratto, provocare danni ai dati informatici tanto da renderli inaffidabili e, quindi, inutilizzabili, si può anche ammettere: ma, si tratta di una mera quaestio facti che, nel caso di specie, è stata esclusa da entrambi i giudici di merito. E, sul punto, si può anche notare che, non a caso, le ipotesi di alterazione o distruzione dei dati informatici prospettate dai ricorrenti si sono rivelate, alla fin fine, delle mere ipotesi prive di ogni concreto riscontro, nonostante l'ampia istruttoria dibattimentale svolta sul punto. (...)".*

Come è dato leggere, il principio della "non contestazione" dell'esito dell'attività acquisitiva sembra essersi affermato come standard argomentativo di un meccanismo che, nella sostanza, inverte l'onere della prova. Pertanto, sembra che si sia instaurato un regime diverso da quello stabilito dalle norme costituzionali e procedurali in punto di onere della prova per cui, chi è gravato dell'onere di dimostrare la conformità dei dati a quelli originari per provare il proprio assunto non è più colui il quale allega il compendio informatico – accusa o difesa che sia – bensì colui il quale intende difendersi da un documento la cui conformità al documento originario è meramente affermata con clausola di stile non verificata o non verificabile empiricamente.

E tale inversione è uno degli effetti collaterali della concezione che poggia sull'apparente e immediata rappresentatività dei documenti informatici, ove questi vengano valutati in assenza di una preventiva verifica di conformità all'originario e di integrità.

Così conclude la Corte: "(...) *Pertanto, le censure riproposte con il presente ricorso, vanno ritenute null'altro che un modo surrettizio di introdurre, in questa sede di legittimità, una nuova valutazione di quegli elementi fattuali già ampiamente presi in esame dalla Corte di merito la quale, con motivazione*

logica, priva di aporie e del tutto coerente con gli indicati elementi probatori, ha puntualmente disatteso la tesi difensiva.(...)".

Anche in tale passo si rinviene il principio, già formulato nei precedenti esaminati, per cui l'accertamento tecnico è stato eseguito conformemente al relativo schema procedurale, mentre la chiusa della decisione verte sulla compattazione degli *obiter* già esaminati, compendiati in un'unica massima che sembra ormai costituire il caposaldo argomentativo per tali fattispecie: "(...) *Non essendo, quindi, evidenziabile alcun vizio motivazionale, la censura, essendo incentrata tutta su una nuova rivalutazione di elementi fattuali e, quindi, di mero merito, va disattesa alla stregua del seguente principio di diritto:* ***"non da luogo ad accertamento tecnico irripetibile la mera estrazione dei dati archiviati in un computer, trattandosi di operazione meramente meccanica, riproducibile per un numero indefinito di volte; poiché non esiste, ad oggi, uno standard prestabilito per la metodologia di trattamento ed analisi delle prove informatiche, l'eventuale alterazione dei dati informatici - e, quindi, la loro inutilizzabilità - a seguito di operazioni effettuate sugli hard disk o su altri supporti informatici, costituisce oggetto di un accertamento di fatto da parte del giudice di merito che, se congruamente motivato, non è suscettibile di censura in sede di legittimità****".*

Secondo tale approccio, la Cassazione non può intervenire a riqualificare giuridicamente la natura degli accertamenti tecnici impressa nella fase delle indagini, per cui sembra che venga definitivamente denaturata la dimensione giuridica della norma.

6.5.4 **Cass., sez. II, sent. 8 luglio 2015, n. 29061**

Infine, a riprova di quanto si è appena detto in merito al consolidamento di tale principio, depone una decisione[261] di pochi giorni successiva a quella precedentemente ripercorsa, che ripropone alcuni degli *obiter* appena esaminati, ma con la particolarità che, nel merito, accoglie il ricorso avverso la sentenza di assoluzione dei due imputati pronunciata dalla Corte di Appello. Dai motivi riportati non è agevole ricostruire la vicenda. Tuttavia, emerge che il giudice del gravame avrebbe disposto una perizia sul seguente quesito:" *se l'accertamento tecnico effettuato dal consulente del PM sia stato eseguito con garanzie di integrità del dato originario tale da garantire la sua ripetibilità",* che il perito si sarebbe espresso per la irripetibilità degli accertamenti tecnici atti e che la

[261] Cass., sez. II, sent. 8 luglio 2015, n. 29061, in *http://www.italgiure.giustizia.it/xway/application/nif/clean/hc.dll?verbo=attach&db=snpen&id=./20150709/snpen@s20@a2015@n29061@S.clean.pdf*; sulla natura di prova documentale dei dati rinvenuti nel computer, v. Cass. sez. III, Sentenza n. 37419 del 05/07/2012 dep. 27/09/2012, Rv. 253573, in *http://www.italgiure.giustizia.it/xway/application/nif/clean/hc.dll?verbo=attach&db=snpen&id=./20120928/snpen@s30@a2012@n37419@tS.clean.pdf*.

Corte avrebbe ritenuto gli accertamenti tecnici inutilizzabili ed assolto i due imputati a seguito dell'inosservanza delle disposizioni di cui alla legge 48/08.

La Cassazione, nell'annullare la decisione, per quanto ai soli effetti civili, ha ripreso gli argomenti sopra già analizzati, ritenendo che:

"*(...) I dati di carattere informatico contenuti nel computer, in quanto rappresentativi, alla stregua della previsione normativa, di cose, rientrano tra le prove documentali (Cass. Sez. 3, Sentenza n. 37419 del 05/07/2012 dep. 27/09/2012 Rv. 253573).*"

Tale affermazione è condivisibile nella misura in cui, come si analizza in questo stesso lavoro, i dati ben possono (e, aggiungo, dovrebbero essere) qualificati come documenti stante la clausola di atipicità dell'art. 234, alle condizioni poste dalle distinzioni formulate a tal proposito[262].

Ma la sentenza prosegue riproponendo l'obiter già esaminato sopra ma ormai assunto tralaticiamente: "*non dà luogo ad accertamento tecnico irripetibile l'estrazione dei dati archiviati in un computer, trattandosi di operazione meramente meccanica, riproducibile per un numero indefinito di volte (Sez. 1, Sentenza n. 23035 del 30/04/2009 dep. 04/06/2009 Rv. 244454).*".

Sulla base di tale assunto che sulla base delle considerazioni tecniche già esposte noon può ritenersi condivisibile, la Cassazione ha cassato la sentenza ritenendo invece erroneo il principio sposato dalla Corte d'Appello in quanto: "*Erroneamente pertanto la Corte territoriale ha ritenuto che l'ipotizzata inosservanza delle disposizioni di cui alla Legge n. 48 del 2008, dia luogo ad inutilizzabilità. Infatti la Legge 18 marzo 2008, n. 48, nel modificare le disposizioni del codice di procedura penale, ha previsto la possibilità di estrarre copia degli stessi con le modalità idonee a garantire la conformità dei dati acquisiti a quelli originali (Cass. Sez. 6, Sentenza n. 10618 del 12/02/2014 dep. 05/03/2014 Rv. 259782).*

Si versa quindi in ipotesi non di inutilizzabilità, ma di valutazione in concreto della prova e quindi, nella specie, dell'eventuale avvenuta o meno alterazione dei dati originali e della corrispondenza o meno di quelli estratti a quelli originali.

Sul punto la motivazione della Corte territoriale è del tutto carente dal momento che non prende in considerazione l'avvenuta alterazione in concreto dei dati estratti dai computer in sequestro e neppure si dà carico di confutare la contraria deduzione svolta nelle consulenze tecniche delle difese delle parti civili allegate ai ricorsi.".

Su tale affermazione va quindi notato che la Corte di Cassazione:

1) esamina la sentenza con la quale la Corte d'Appello, sulla base del giudizio di ritenuta irripetibilità degli accertamenti, ha sanzionato con la decisione di "inutilizzabilità" l'attività di estrazione dei dati;

[262] Cfr. TONINI P., (2009), op.cit., p. 401.

2) ritiene che l'inosservanza delle modalità previste dalla L. 48/08 non dia luogo ad inutilizzabilità (pertanto, il caso sembra diverso da quello precedente nel quale veniva affrontato il tema della dell'irripetibilità degli accertamenti);
3) esprime un giudizio di legittimità sulla qualificazione giuridica delle operazioni di estrazione come irripetibili espressa dalla Corte d'Appello;
4) ritiene la decisione poi cassata, carente sia sotto il profilo della valutazione in concreto dell'alterazione dei dati estratti dal computer, sia della mancata confutazione della contraria deduzione svolta nelle consulenze tecniche delle parti civili.

In definitiva, entrando nel merito della valutazione del fatto, la Corte esprime un giudizio che investe direttamente la qualificazione che la Corte di Appello aveva operato in relazione alla natura degli accertamenti tecnici ma che la Cassazione non condivide.

Per questo non sembra univoco l'atteggiamento della Corte che in merito alla qualificazione giuridica della natura degli accertamenti tecnici in materia informatica, di volta in volta entra nel merito della valutazione del fatto o se ne astiene.

6.6 Gli effetti dell'attuale orientamento della Cassazione

L'orientamento che predilige la concezione della ripetibilità delle operazioni di estrazione e copia dei file da un dispositivo digitale sembra, allo stato, in via di affermazione.

Se tale orientamento dovesse consolidarsi, le sue conseguenze avranno notevole impatto, in termini di efficacia, economia processuale e rispetto delle garanzie delle parti coinvolte, sia sui procedimenti in corso, sia su quelli che verranno impostati secondo tali principi.

Infatti, da tale concezione derivano gravosi oneri a carico degli attori processuali impegnati in accertamenti tecnici ritenuti ripetibili:

- gli organi dell'accusa – e principalmente la polizia giudiziaria – e ogni altra parte del procedimento, potranno autonomamente procedere all'acquisizione dei dati digitali dai dispositivi ai sensi dell'art. 359, escludendo le altre parti dalle operazioni, secondo una visione tipicamente inquisitoria;
- non sarebbe applicabile nemmeno quell'iter minimamente garantito previsto dell'art. 360-117 disp. att.;
- chi procede all'accertamento tecnico ripetibile dovrà comunque "adottare le misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione", nonché provvedere, "ove possibile alla loro immediata duplicazione su adeguati supporti

mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità";

- in caso di omessa adozione di tali procedure, non vi è alcuna sanzione processuale, nemmeno quella dell'inutilizzabilità;
- in ogni caso, il procedente in autonomia resterebbe comunque onerato di osservare, garantire e provare che dal momento in cui sono stati acquisiti sino al termine del procedimento:

1) adempia l'onere di custodire correttamente i dispositivi con i dati originari archiviati[263], sia l'eventuale copia dei dati estratti in quanto destinati al vaglio del giudice, in ogni fase e stato del processo e sino alla definizione ultima che, non di rado, conosce i tempi supplementari dei giudizi di rinvio o addirittura, anche a distanza di molto tempo, la rivincita costituita dal giudizio di revisione;

2) provi la conformità dei dati originari alla copia;

3) documenti correttamente la catena di custodia dei reperti informatici e dei dati; infatti, costituendo i dati, originari e in copia, il presupposto per l'esercizio delle facoltà della parte non coinvolta nelle operazioni ripetibili, alla loro dispersione conseguono le responsabilità a carico del custode di mezzi di prova, incluse quelle derivanti dal rispetto del Codice sul trattamento del dati personali previste dal D. Lgs. 196/2003;

- a tutte le altre parti escluse dalle procedure di acquisizione dovrà essere garantita la facoltà di chiedere e ottenere, nei tempi e quali condizioni necessari per preparare la sua difesa ex art. 111 Cost.[264], sia copia dei dati effettuata con modalità ripetibile, sia dei dati originari per consentire la verifica di conformità di entrambi i dati e per l'esercizio di tutte le facoltà processuali riconosciute alla parte richiedente;
- essendo operazioni ripetibili, i verbali degli accertamenti non andranno, ex art. 431, direttamente nel fascicolo del dibattimento, ma resteranno nel fascicolo del pubblico ministero per poter essere oggetto di contraddittorio dibattimentale prima della loro assunzione al fascicolo del giudice;
- essendo le attività di copia ripetibili, potranno e dovranno essere ripetute durante la fase dibattimentale;

[263] Cfr. art. 259, 2 c., che prescrive quanto segue: "*quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria*"

[264] v. art. 111, c. 3, Cost. "(...) *Nel processo penale, la legge assicura che la persona accusata di un reato sia, nel più breve tempo possibile, informata riservatamente della natura e dei motivi dell'accusa elevata a suo carico; disponga del tempo e delle condizioni necessari per preparare la sua difesa;* (...)"

- in caso di difformità tra gli hash dei dati originari e di quelli della copia, sarà onere di chi intende utilizzarli dimostrare:
  - che i dati rilevanti non sono stati modificati;
  - quali siano i dati modificati;
- tali corollari valgono ovviamente anche per il difensore-investigatore il quale non sarà più soggetto all'art. 391 *decies* e quindi non dovrà più avvisare il pubblico ministero dell'intenzione di procedere ad acquisizione e duplicazione di supporti informatici con elementi di prova a suo discarico.

Tali conseguenze dell'opzione esegetica criticata non esauriscono il carico gravante sul procedimento e sulle facoltà delle parti.

All'esito della disamina non si può evitare di notare come tali decisioni, pur non prestando sufficiente attenzione al dato scientifico-tecnico presupposto, finiscano per orientare l'azione degli operatori delle indagini.

Pertanto, la qualificazione dell'acquisizione del trattamento di dati informatici come operazione ripetibili, a mio parere costituisce un'indicazione fuorviante per le forze che si trovano ad interagire sul campo a diretto contatto con i reperti informatici e fino a quando tale orientamento non cambierà, non è escluso che possano riverificarsi situazioni come quelle già osservate nel corso delle indagini del caso Garlasco.

A ciò deve aggiungersi che la Suprema Corte mostra di essere pericolosamente orientata a declinare il vaglio di regolarità - *rectius*: conformità del trattamento dei dati digitali alle scarne regole processuali in ambito tecnico-scientifico – degradando la questione al rango di mero problema "di fatto" relegato alla cognizione delle fasi di merito.

Ma in tali fasi, come sempre più spesso è dato leggere negli atti processuali e nelle sentenze, il problema di fatto viene sbrigativamente liquidato con espressioni di stile quali "*...con clonazione forense dei supporti in modo tale da non alterare il dato originale e mantenerlo utilizzabile per eventuali ulteriori verifiche*", dando ragione a chi ha detto: "*Accade, talvolta, che le ragioni di diritto vengano piegate alle logiche di giustizia*"[265].

In ogni caso, avanti a tali fenomeni un ruolo preponderante verrà assunto da quel settore di ricerca dell'Informatica forense attento alla verifica e alla tassonometria dei fenomeni oggetto di decisioni tecnicamente e scientificamente opinabili.

[265] FRATTALLONE S., La mera estrazione dei dati da un computer non è atto irripetibile, in http://www.frattallone.it/penale/561-penale-la-mera-estrazione-dei-dati-da-un-computer-non-e-atto-irripetibile .

6.7 Le esegesi alternative

In alternativa a quella delineata nelle sentenze esaminate, ritengo che siano possibili altre esegesi.

Secondo un primo modello atipico, non essendo gli accertamenti tecnici riconducibili ad un unico schema precostituito ed essendovi invece varie situazioni che consentirebbero modalità di approccio diversificate[266], la scelta del modello procedurale da seguire andrebbe effettuata tenuto conto delle specifiche caratteristiche tecnologiche e di stato del dispositivo (acceso/spento, in funzionamento, ecc.) ed in relazione alle diverse situazioni nelle quali possono empiricamente rinvenirsi i dati, statici o dinamici, secondo apprezzamenti tecnici basati sull'analisi empirica della fattispecie, alla luce degli standard tecnici internazionali.

La correttezza dell'opzione procedurale sarebbe poi verificabile sulla base sia delle considerazioni tecniche, sia del risultato delle operazioni teso a verificare la conformità della copia ottenuta ai dati originari

Vi è un secondo modello, nei suoi passaggi fondamentali paradigmatico rispetto alla maggior parte delle situazioni che si verificano allo stato attuale della tecnologia.

Tale modello sposerebbe l'impostazione sistematica introdotta dalla L. 48/08 con i "poteri partecipativi"[267] delle parti coinvolte nel procedimento, così snellendo la procedura di acquisizione dei dati, realizzandola in una fase anticipata delle indagini, consentendo a ciascuna parte l'esercizio delle rispettive prerogative e sollevando il carico di oneri appena rassegnato:

- gli atti di estrazione e duplicazione dei dati dai dispositivi originari costituiscono accertamenti tecnici non ripetibili ex art. 117 disp. att. da effettuarsi nell'immediatezza della loro individuazione con la procedura prevista dall'art. 360, salva la riserva di incidente probatorio;

- in un unico contesto crono-procedurale verrebbero effettuate più operazioni quali l'estrazione dei dati, l'effettuazione di una copia master dei dati originari, la verifica della conformità con i dati originari, l'effettuazione da questa di una copia master, previa verifica della conformità dei dati con i dati originari, seguita dall'effettuazione delle successive copie di lavoro per le parti (secondo lo schema 1 copia master, da cui estrarre -N copie di lavoro, una per ciascuna parte), previa verifica della conformità con i dati originari della copia *master*;

[266] A tal proposito viene paradigmaticamente evocata la differenza intercorrente tra le necessità tecniche e procedurali nel caso di estrazione di dati da un dispositivo accesso e in funzionamento, da quelle relative ad un dispositivo spento, da quelle di acquisizione di dati trasmesse in un sistema telematico.

[267] L'espressione è di TONINI P., op.cit., p. 487.

- ove mediante *hash matching*[268] i dati della copia master risultino conformi ai dati originari, la copia, in quanto nuovo originale, terrebbe luogo del compendio originario e consentirebbe ad esempio, il dissequestro e la restituzione del dispositivo alla parte o al terzo;

- fissato definitivamente il compendio digitale originale, le successive operazioni di analisi dei dati, sarebbero effettuabili autonomamente da ciascuna parte sulle rispettive copie ottenute come sopra, costituenti altrettanti originali; tali operazioni di analisi costituirebbero accertamenti tecnici ripetibili effettuabili con le procedure e con gli strumenti tecnici ritenuti da ciascuna parte più idonei e utili, garantendo a quelli del pubblico ministero la doverosa osservanza delle esigenze di segreto e riservatezza.

Infine, secondo un ultimo modello che concilia l'impostazione introdotta dalla L. 48/08 con i poteri del giudice:

- i dati verrebbero qualificati, secondo quanto correttamente già ritenuto dalla Cassazione, come documenti rientranti nello schema tipico dell'art. 234;
- tuttavia, le caratteristiche ontologiche dei documenti digitali fanno si che, se vogliono mantenere integra la loro capacità rappresentativa, devono essere acquisite rispettando le modalità tecniche proprie dell'Informatica forense;
- ma le modalità tecniche di assunzione non sono previste dalla L. 48/08 e dalle norme interpolate, né è prevista alcuna sanzione di nullità o inutilizzabilità nel caso di inosservanza;
- pertanto, non essendo previste modalità tecniche di assunzione disciplinate dalla legge, i file sarebbero prove tipiche da assumersi con modalità atipiche ex art. 189 (Prove non disciplinate dalla legge). a tenore del quale "*Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti [187] e non pregiudica la libertà morale della persona [642, 188]. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova.*".
- quindi, il giudice potrebbe ammettere la prova documentale ma, sentite le parti sulle modalità di assunzione, dovrebbe poi provvedere probabilmente nella forma della perizia da effettuarsi secondo le regole tecnico-scientifiche dell'Informatica forense;
- pertanto, potrebbe disporre l'acquisizione dei dati con le modalità illustrate per il secondo modello.

Tale schema, se da un lato ricollocherebbe i dati nell'ambito della prova documentale e rivitalizzerebbe il ruolo partecipativo delle parti coinvolte nel

[268] Procedura di confronto di due hash di due stringhe di dati per verificare se sono identici gli hash e quindi le due stringhe di dati.

contraddittorio sulle forme di ammissione e della successiva fase acquisitiva, dall'altro risulterebbe più complesso da attuare e sposterebbe le operazioni dell'acquisizione in una fase troppo avanzata rispetto alle esigenze delle indagini o della difesa.

7 La questione della prova documentale penale informatica

7.1 Le precisazioni terminologiche in tema di documento informatico

Anche il tema del documento informatico, inteso come mezzo di prova penale occupa un posto centrale nell'ambito delle questioni affrontate dall'Informatica forense.

Va precisato che ai soli fini della presente disamina, da un punto di vista ontologico attento alle implicazioni giuridiche, per documento informatico intendo un documento creato mediante un sistema informatico e codificato digitalmente, mentre per documento digitale intendo una sequenza di bit anche ove non abbia l'apparenza di documento.

Orbene, l'attività di indagine e investigativa, anche difensiva, si concentra sull'individuazione, acquisizione, analisi-presentazione e valutazione di documenti digitali la cui natura giuridica nell'ambito del procedimento è quella di mezzo di prova documentale[269].

Da un punto di vista giuridico, invece, va preliminarmente rilevato come sia alquanto complesso sintetizzare in un'unica espressione tutti gli elementi e le caratteristiche che contribuiscono a delineare il concetto di "mezzo di prova documentale penale informatica o digitale".

A tal proposito, in linea di prima approssimazione, appare utile precisare la portata dell'espressione documento informatico rilevante a fini probatori in sede processual penale, per poi differenziarlo dalle (apparentemente) omonime figure di documento informatico riscontrabili in altri rami dell'ordinamento e che nel gergo giuridico vengono confusi sulla base di un'ingannevole assonanza:

1) innanzitutto il documento informatico, quale insieme di dati acquisito al procedimento penale, non può essere indicato semplicisticamente come "prova informatica penale" in quanto costituisce un mezzo di prova[270], appunto

[269] La considerazione vale per lo specifico processuale penale e, *mutatis mutandum,* per ogni altro ambito processuale (civile, erariale, amministrativo, tributario, ecc.).

[270] Va ricordato che nell'ambito del codice di procedura penale, il mezzo di prova costituito dai Documenti, trova la seguente articolazione: art. 234 (Prova documentale), art. 234 bis (Acquisizione di documenti e dati informatici), art. 235 (Documenti costituenti corpo del reato), Art. 236 (Documenti relativi al giudizio sulla personalità), art. 237 (Acquisizione di documenti provenienti dall'imputato), art. 238 (Verbali di prove di altri procedimenti), art. 238 bis (Sentenze irrevocabili), art. 239 (Accertamento della provenienza dei documenti), art. 240

documentale, che acquista il valore di prova solo dopo il compimento dell'iter di ammissione e valutazione da parte del giudice;

2) in secondo luogo, indicare semplicisticamente il mezzo di prova documentale penale informatico o digitale come "documento informatico" *tout court*, appare riduttivo e confusorio rispetto alle altre figure previste da altre norme del nostro ordinamento e indicate con tale espressione, ma dalle implicazioni molto diverse[271]:

2.1) nell'ambito del diritto amministrativo, l'art. 1 del Codice dell'Amministrazione Digitale (CAD)[272] così lo definisce: "*(...) p) documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;(...)"* e ciò per differenziarlo dal "*(...) p-bis) documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti; (10)"*[273]. Inoltre, all'art. 20, sotto la rubrica "*Documento informatico"* si circoscrive l'ambito dell'efficacia probatoria specificando che:*"1. Il documento informatico da chiunque formato, la memorizzazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice.*

1-bis. L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall'articolo 21."; tali norme indicano il documento informatico rilevante in ambito amministrativo[274]

2.2) in ambito penale, l'art. 491 bis c.p. disciplina i "*Documenti informatici",* prevedendo che: "*Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria,*

(Documenti anonimi), art. 241 (Documenti falsi), art. 242 (Traduzione di documenti. Trascrizione di nastri magnetofonici), art. 243 (Rilascio di copie).

[271] Sull'evoluzione della norma, v. TONINI P. (2009), Documento informatico e giusto processo, in Diritto penale e processo, 4/2009, 401–402.

[272] Cfr. Codice dell'Amministrazione Digitale (CAD), Decreto Legislativo 7 marzo 2005, n. 82.

[273] Va rilevato come il CAD e tutta la normativa di settore riguardante la documentazione informatica amministrativa, pur costituendo un *corpus* di rilevante importanza nell'ambito della disciplina dei fenomeni giuridici a contenuto informatico, non vincola il giudice penale (salvo che le norme riguardino lo stato di famiglia e di cittadinanza) in virtù del principio del libero convincimento espresso dall'art. 193 c.p.p. in tema di "*Limiti di prova stabiliti dalle leggi civili"* per cui "*1. Nel processo penale non si osservano i limiti di prova stabiliti dalle leggi civili, eccettuati quelli che riguardano lo stato di famiglia e di cittadinanza [241, 654]"*. Tuttavia, per quanto non vincolante ai fini della formazione della prova in ambito penale, il CAD e la normativa collaterale restano fonti del diritto dalle quali possono essere tratti criteri orientativi (e mai vincolanti) utili all'esegesi processual penalistica, come ad esempio quelli espressi in sede definitoria dall'art. 1 CAD.

[274] Per un *excursus* sull'evoluzione del documento informatico, v. DELFINI F., Documento informatico, forma analogica e forma elettronica: dalla scrittura privata autenticata all'atto pubblico informatico, in FINOCCHIARO G., DELFINI F., (a cura di), Diritto dell'informatica, Utet, Milano, 2014, p. 251 e ss..

si applicano le disposizioni del capo stesso concernenti gli atti pubblici.[275]. Tale norma costituisce la definizione avente valore e funzione descrittiva al fine di delineare il contenuto delle ulteriori norme del codice penale con valore prescrittivo nell'ambito della disciplina delle falsità in documenti informatici;

2.3) in ambito civile, la norma sotto la quale viene comunemente annoverato il documento informatico inteso come prova civile, è collocata nel LIBRO VI del codice civile sulla Tutela dei diritti, TITOLO II - Delle prove, Capo II - "Della prova documentale" sub art. 2712 c.c. - *Riproduzioni meccaniche,* il quale prevede che: *"1. Le riproduzioni fotografiche,* ***informatiche*** *o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime (cpc 261)*."[276];

3) pertanto, le diverse figure giuridiche non vanno confuse tra loro in quanto, seppur apparentemente riferibili allo stesso oggetto ontologicamente inteso, cioè il documento composto di dati digitali, in realtà sono figure valevoli nell'ambito dei rispettivi rami dell'ordinamento nei quali trovano specifica disciplina e operatività.

Ai fini processual penalistici, vale l'accezione del mezzo di prova documentale ex art. 234 che, per il principio di specialità, prevale sulle altre definizioni.

Sgomberato il contesto espositivo da ambiguità lessicali, ai fini processual penalistici, muovendoci nell'ambito dalla dizione dell'art. 234, con l'espressione sintetica di "documento informatico" o "mezzo di prova documentale informatica" indichiamo il documento informatico costituente mezzo di "prova documentale penale informatica o digitale".

Ai fini della disciplina del documento informatico quale mezzo di prova penale, i dati e documenti informatici rientrano nella più ampia categoria prevista dall'art. 234 e, da ultimo, nei termini che diremo, dall'art. 234 bis.

7.2 Gli elementi costitutivi della prova documentale

L'art. 234, che riguarda la più ampia categoria della "Prova documentale"[277], prevede che:"*È consentita l'acquisizione di scritti o di altri*

[275] Tale norma è stata inserita nel codice penale per effetto della l. 23 dicembre 1993, n. 547 (art. 3). L'art. 3, comma 1, lett. b), della l. 18 marzo 2008, n. 48 ha abrogato la seconda parte della disposizione che recitava: "*A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli*". L'art. 3, comma 1, lett. a), della l. 18 marzo 2008, n. 48 ha inserito il riferimento all'efficacia probatoria. L'ultima parte dell'articolo è stata modificata dal d.lgs. 15 gennaio 2016, n. 7.

[276] Comma così modificato dall'art. 23, D. Lgs. 7/3/2005 n. 82.

[277] Sulla prova documentale in generale converge l'interesse degli studiosi di ogni branca del diritto processuale in senso ampio; per tutti, v. CARNELUTTI F., La prova civile (1915),

documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo.

2. Quando l'originale di un documento del quale occorre far uso è per qualsiasi causa distrutto, smarrito o sottratto e non è possibile recuperarlo, può esserne acquisita copia.

3. È vietata l'acquisizione di documenti (191) che contengono informazioni sulle voci correnti nel pubblico intorno ai fatti di cui si tratta nel processo o sulla moralità in generale delle parti, dei testimoni, dei consulenti tecnici e dei periti (1957, 203, 240)."

La norma non traccia la definizione di prova documentale che è invece desunta dal codice[278].

Secondo una chiara distinzione[279], in relazione al "contenuto probatorio" "*si può definire documento "la rappresentazione di un fatto incorporata in una base materiale", mentre se si considera l'"oggetto in sé", si può definire documento "la base materiale che incorpora la rappresentazione di un fatto".*

Per TONINI, il concetto di documento comprende quattro elementi: il fatto rappresentato, la rappresentazione, l'incorporamento, la base materiale, così specificati:

1) il fatto rappresentato, è il concetto nel quale ricadono fatti, persone, cose, indicate dall'art. 234, ma anche pensieri, ovvero tutto ciò che può costituire oggetto di prova, ovvero un accadimento naturalistico o un atto umano, quale una dichiarazione[280];

2) la rappresentazione del fatto indica la ricostruzione di un fatto mediante un equivalente fatto di immagini, parole, suoni, in modo tale da renderlo conoscibile ad altre persone;

3) l'incorporamento è l'operazione con la quale la rappresentazione viene fissata su una base materiale che può essere la scrittura, la fotografia, la fonografia, la cinematografia e "ogni altro mezzo" che la tecnologia può realizzare in futuro, quale ad esempio la registrazione magnetica e la registrazione in una delle varie forme di digitalizzazione;

4) la base materiale, infine, costituisce il sul quale è fissata e incorporata la rappresentazione, quale ad esempio la carta, la pellicola, il supporto magnetico[281]

Giuffrè, Milano, FERRUA P., GRIFANTINI F. M., ILLUMINATI G., ORLANDI R., La prova nel dibattimento penale, Giappichelli, Torino, 2005.

[278] Cfr. TONINI P. (2003), op.cit., p. 272 .

[279] *Ibidem.*

[280] A tal proposito, TONINI P., (2003), *ibidem*, distingue tra "documento" e "documentazione", ove l'oggetto rappresentato in quest'ultima è costituito da un'attività del procedimento penale (compiuta ad es. dal giudice, dal pubblico ministero, dal difensore o dai loro ausiliari).

[281] Lo studio dell'evoluzione del documento, dei tipi di supporto, delle tecniche di scrittura e di rappresentazione grafica, fotografica, video e sonora ritenuti gli antecedenti storici dei nuovi fenomeni digitali, agevolano l'analisi delle nuove problematiche a condizione che non si incorra

7.3 La prova documentale penale informatica

Orbene, bisogna verificare se tale quadripartizione degli elementi costitutivi del mezzo di prova documentale, sia strumento idoneo a classificare anche le componenti del documento informatico e quindi a ricomprendere quest'ultimo nella categoria del mezzo di prova documentale, oppure se, presentando il documento informatico degli elementi differenzianti, non sia necessario rivedere la categoria.

Ad un primo sommario approccio mediante assimilazione dei fenomeni apparentemente simili, ogni documento informatico o un insieme di dati informatici organizzati in file, come ad esempio i file di testo, le fotografie digitali, i filmati digitali, le fotografie digitali estratte da filmati digitali, i file audio, dovrebbero essere costituiti dal fatto rappresentato, dalla rappresentazione, dall'incorporamento e dal supporto per cui si avrebbe:

1) il fatto rappresentato, costituito dal concetto oggetto di prova che, essendo esterno alla rappresentazione, risulterebbe indifferente alla digitalizzazione; tuttavia, proprio la tecnologia digitale consente la creazione fittizia di fatti rappresentati cosicché possono darsi situazioni nelle quali anche il fatto rappresentato è originariamente digitale (ad es. un videogioco, o un file di log);

2) la rappresentazione mediante dati in formato digitale, vale a dire la ricostruzione del fatto mediante un equivalente fatto di immagini, parole, suoni, in modo tale da renderlo conoscibile ad altre persone contenuto nel dato digitalizzato o nell'insieme di dati organizzati in file;

3) l'incorporamento, costituito dall'operazione di fissazione della rappresentazione sul supporto ovvero sulla memoria e che, nel caso del documento informatico, può essere realizzata con vari tipi di tecnologia di digitalizzazione dipendenti dalla tipologia di supporto sul quale viene svolta l'operazione[282], comunque rientranti nel concetto di "ogni altro mezzo" previsto dalla norma. Si avranno così vari tipi di incorporamenti: mediante registrazione magnetica [è il caso dell'operazione svolta su nastri (a bobina, cassetta DAT), dischetti estraibili (floppy disk) o dischi fissi (hard disk)], o mediante memorizzazione su dischi che si basano su tecnologie ottiche (CD-R, DVD-R) o magneto-ottiche (CD-RW, DVD-RAM)[283] o mediante registrazione elettronica che si realizza mediante memorizzazione su memorie contenute in schedine (ad es. nei formati SD, XD, MS) o in astucci di piccole dimensioni (ad es. le pen drive USB);

nelle assimilazioni fenomenologiche tra i sistemi tradizionali e il nuovo specifico tecnologico caratterizzato da tecniche totalmente innovative quali, ad esempio, il sistema di codifica binaria.

[282] Cfr. la voce Strumento registratore in *https://it.wikipedia.org/wiki/Strumento_registratore*.

[283] In questi, la registrazione delle informazioni digitali viene fatta su un sottile strato di materiale che riflette la luce di un laser in maniera selettiva.

4) la base materiale, infine, costituisce il supporto sul quale è fissata la rappresentazione che, per quanto riguarda la tecnologia digitale allo stato disponibile, possono essere costituiti dai vari tipi di memorie primarie e secondarie, quali nastri (a bobina, cassetta DAT), dischetti estraibili (floppy disk) o dischi fissi (hard disk)], dischi che si basano su tecnologie ottiche (CD-R, DVD-R) o magneto-ottiche (CD-RW, DVD-RAM), dispositivi elettronici quali schedine (ad es. nei formati SD, XD, MS) e pen drive.

7.3.1 L'applicabilità del modello tradizionale di prova documentale penale alla prova documentale informatica

Tale classificazione mediante assimilazione dei fenomeni, per quanto apparentemente applicabile anche al documento informatico, mostra la sua inadeguatezza nel momento in cui non riesce a ricomprendere altri elementi peculiari pur presenti e caratterizzanti il documento informatico, soprattutto in considerazione della sua utilizzabilità come mezzo di prova. Difatti:

1) quanto al fatto rappresentato, la tecnologia digitale ha sviluppato un'impressionante gamma di strumenti che consentono un'infinità di artifizi capaci di trasformare il verosimile in "vero" e quindi di "creare" il fatto rappresentato come frutto di totale artificio[284] (si tenga presente, ad esempio, il fenomeno della realtà virtuale e della realtà aumentata). Pertanto, allorquando si inferisca dalla rappresentazione al fatto rappresentato, si rende necessario verificare la "realtà" del fatto ignoto rappresentato fittiziamente, nonché i suoi confini e l'eventuale commistione con elementi totalmente fittizi. Tale sfida mette in crisi la concezione tradizionale di tale componente che sino all'avvento del fenomeno digitale era concentrata sulla distinzione accadimento naturalistico-dichiarazione;

- quanto alla rappresentazione, se questa è costituita dalla ricostruzione del fatto mediante un equivalente fatto di immagini, parole, suoni in modo tale da renderlo conoscibile ad altre persone, ma in formato digitale. Una delle conseguenze più rilevanti della particolarità delle rappresentazioni digitali, che in ambito processuale condiziona la questione del rapporto tra originale e copia è che la tecnologia digitale dà la possibilità di avere non una sola

[284] Si tenga presente, ad esempio, il fenomeno della realtà virtuale (VR, *Virtual Reality*) nella quale il verosimile appare vero, nonchè quello della realtà aumentata (AR, *Augmented Reality*) nella quale alla percezione sensoriale si sovrappongono informazioni fornite dalla tecnologia ancora distinguibili, o iperaumentata, dimensione nella quale tra il vero e il fittizio non vi è soluzione di continuità; tutto ciò in attesa dell'affermazione del *wetware*, quale sistema di interazione diretta tra il cervello umano e il software. Per alcune riflessioni sull'impatto della realtà virtuale nella dimensione sociale, culturale e cognitiva, v. GALLARINI S., La realtà virtuale, Xenia Edizioni, Milano, 1994, JACOBELLI J. (a cura di), La realtà del virtuale, Editori Laterza, Bari, 1998, CADOZ C., Le realtà virtuali, Milano, il Saggiatore, 1998, MALDONADO T., Reale e virtuale, Feltrinelli, Milano, 1998; per un esempio di realtà iperaumentata, v. *http://www.focus.it/tecnologia/digital-life/una-vita-in-realta-aumentata-ecco-come -potrebbe-essere*; sul wetware, v. *https://it.wikipedia.org/wiki/Wetware*.

rappresentazione, bensì molteplici rappresentazioni dello stesso fatto quale risultato della sua riproducibilità in un numero -n di copie del file tutte identiche tra di loro. Orbene, ove si consideri un qualunque documento, l'unico documento che ne sia copia in senso digitale non è il file che ha lo stesso nome o estensione o che contenga la stessa rappresentazione di un altro file, bensì è solo quello (o quelli) che abbiano lo stesso hash, che cioè siano formati da sequenze di bit perfettamente identiche tra loro. Ove ciò accada, si verificherà il caso di due documenti entrambi originali. Si potrebbe rendere necessario stabilire quale dei due documenti costituiti da file aventi la stessa sequenza di bit sia venuto ad esistenza per primo (essendo magari l'uno copia dell'altro); in tal caso si dovrà fare riferimento al dato temporale di creazione dell'uno rispetto all'altro in modo tale da stabilire quale dei due documenti sia quello "originario"[285]. Se invece due documenti non avranno lo stesso hash, allora saranno due documenti diversi che differiscono in qualche dato, anche minimo, ma ciò fa sì che essi siano due documenti diversi anche sul piano sostanziale e rappresentativo. Distinzioni di tale tipo, solo apparentemente speciose, trovano rilevante importanza in sede pratico-empirica, sia sul piano sostanziale che su quello processuale. Sul piano sostanziale, ad esempio, la determinazione del rapporto di anteriorità di due file con lo stesso hash rileva sia nella determinazione del *tempus* e *locus commissi delicti*, sia (e soprattutto) nella determinazione degli elementi ricostruttivi di un fatto costituente reato (dall'elemento oggettivo, all'elemento soggettivo, ad eventuali circostanze, sino alla ricorrenza di scriminanti), sia sulla determinazione della legge penale applicabile. Sul piano processuale, invece, la determinazione del rapporto tra originale e copia incide, ad esempio, sul regime dell'utilizzabilità della copia ex art. 234 c. 2 e sull'accesso alle copie dei reperti oggetto di sequestro.

Da ciò deriva che tra più rappresentazioni apparentemente simili, grazie alla funzione di hash andrà matematicamente calcolato il rapporto di originalità e, ove possibile, l'eventuale rapporto di originarietà.

Orbene, tale problematica non si pone (o si pone in termini diversi) per le copie di documenti analogici in quanto esse, per quanto uguali, saranno caratterizzate da elementi distintivi anche quando si tratterà di due documenti c.d. originali riportanti la stessa rappresentazione mentre, in realtà, si tratterà di due documenti distinti.

Quanto all'incorporamento, i processi di fissazione sono realizzati grazie ad attività ad alto contenuto tecnologico controllate dal *medium* costituito dal

[285] La verifica del momento di creazione di un file rispetto ad un altro avente medesimo hash non è affatto semplice: i riferimenti cronologici presenti tra i metadati di un file sono normalmente creati dall'orologio gestito dal sistema operativo installato sullo stesso dispositivo e quindi da un sistema di misurazione del tempo relativo e non assoluto. La questione si complica nel caso di confronto tra i dati temporali di due file con lo stesso hash ma creati da due sistemi diversi.

sistema informatico che si interpone tra l'autore dell'incorporamento e il supporto. E tuttavia, mentre alcune operazioni richiedono un atto volontario dell'autore della rappresentazione, altre operazioni vengono svolte automaticamente dal sistema operativo (ad es. l'aggiornamento del file di log, la modifica dei metadati dei file, la creazione dei file di backup). Durante tale fase, il sistema operativo crea automaticamente altri dati - i c.d. metadati - che vengono incorporati al documento al quale si riferiscono, ma pur facendone parte non appaiono automaticamente insieme alla rappresentazione. I metadati, a loro volta, possono essere considerati documenti relativi alla rappresentazione incorporata e alla quale si riferiscono, cosicché a loro volta rappresentano un fatto. Vi sono anche altre tipologie di dati che vengono creati automaticamente dal sistema operativo, contenuti a loro volta in documenti o in parti di documenti ma che normalmente non appaiono immediatamente, come ad es. gli *header* dei messaggi di posta elettronica[286]. Tali tipologie di documenti, ben lungi dall'esaurire la fenomenologia dei dati accessori ai dati costituenti la rappresentazione di interesse processuale, in qualche modo ampliano la portata del concetto di incorporamento.

Quanto infine al supporto, la concezione tradizionale tiene fino a quando ci si occupa di documenti formati da bit staticamente archiviati su una memoria, mentre entra in crisi quando si tratta di valutare i documenti in fase dinamica durante la trasmissione che avviene, appunto senza supporto o, ad essere più analitici, mediante passaggio dei pacchetti da un supporto all'altro dei sistemi informatici e telematici costituente i nodi della rete che attuano la trasmissione dei dati.

All'esito del tentativo di compressione degli elementi costitutivi della prova documentale informatica nella quadripartizione della prova documentale tradizionale, restano senza risposta alcuni dubbi relativi alla classificazione di altri elementi della prova informatica:

1) appare poco agevole classificare le tecnologie di decodifica (hardware e software) indispensabili per l'intellegibilità del documento, che invece non è contemplata dal modello classificatorio degli elementi costitutivi i documenti non digitali; in altre parole, ove il documento digitale non venga decodificato, resta limitato ad una successione di bit che condiziona la fruizione della rappresentazione[287]; pertanto, il concetto di rappresentazione e incorporamento non risulta sufficiente a spiegare il fenomeno;

2) la classificazione in esame difficilmente è applicabile ai casi in cui un medesimo fatto venga rappresentato con due diversi strumenti di codifica (ad

[286] Sugli *header* delle email, v. *https://it.wikipedia.org/wiki/Posta_elettronica* e *https://it.wikipedia.org/wiki/Header*.

[287] In realtà, tale aspetto non sarebbe nuovo in quanto verificatosi anche a proposito dei documenti fonografici e cinematografici che, per essere intellegibili, necessitano di un *medium* meccanico "di lettura".

esempio due diversi software applicativi) che così realizzano due documenti diversi sia per quanto riguarda la rappresentazione sia per ciò che attiene ai relativi incorporamenti;

3) poco agevole è altresì la classificazione dei documenti che vengono trasmessi telematicamente, assimilabili al modello tradizionale solo sino a quando si trovano staticamente archiviati su una memoria, di partenza o di arrivo; quando invece gli stessi documenti si trovano dinamicamente in fase di trasmissione, i dati, e quindi i bit di cui sono composti, cambiano la loro stessa natura fisica in conseguenza del diverso sistema di codifica. Pertanto, il documento che in partenza è caratterizzato da un certo fatto, rappresentazione, incorporamento e supporto, durante la fase dinamica subisce una variazione in relazione almeno a tre elementi:

1. alla rappresentazione, in quanto possono aggiungersi i dati del sistema telematico necessari alla trasmissione,
2. all'incorporamento, in quanto cambia la tecnica di trasmissione che sfrutta le proprietà tensionali dell'energia;
3. al supporto, in quanto dal supporto di partenza, ai mezzi di trasmissione telematica (talvolta in assenza di supporto, come nei casi di telecomunicazione radio o mediante onde elettromagnetiche), sino al supporto di destinazione le variazioni di stato sono molteplici e rilevanti.

Sulla base di tali considerazioni, il modello classificatorio tradizionale non sembra più adeguato a svolgere la sua funzione in quanto la complessità e l'articolazione delle componenti del documento informatico sfuggono alle coordinate classiche.

Pertanto, il modello dottrinale quadripartito andrebbe rivisto annoverando e dando pieno conto delle caratteristiche del documento digitale[288].

7.3.2 Documento, rappresentazione e incorporazione

Il problema della confusione tra il documento informatico e la rappresentazione in esso incorporata, come se fossero entità tra loro interscambiabili, si amplifica sul piano pratico in quanto in sede processuale si attribuisce valore probatorio alla mera rappresentazione.

Infatti, è invalsa una ingiustificata tendenza a ritenere fungibili diversi documenti informatici, incorporanti rappresentazioni apparentemente simili[289],

[288] La necessità di riclassificare gli elementi costitutivi del documento digitale è stata lucidamente avvertita e intrapresa da TONINI P., Documento informatico e giusto processo, op.cit., p 401 e ss., per quanto limitata all'ambito delle medesime categorie, mediante differenziazione tra incorporamento analogico e incorporamento digitale. La rilevanza delle ulteriori peculiarità rende attuale il problema della revisione del modello normativo e classificatorio.

obliterando il rapporto con la loro genesi, formazione, riproduzione su diversi supporti materiali mediante una tecnologia che caratterizza il documento informatico, differenziandolo completamente dal documento tradizionalmente inteso.

Ne deriva la questione della fungibilità o meno di documenti con rappresentazioni apparentemente identiche ma incorporate a supporti ontologicamente diversi.

La giurisprudenza maggioritaria, sia di merito che di legittimità, tranne qualche diversa pronuncia rimasta marginale, ritiene che i dati digitali, una volta stampati, possano essere trattati alla stregua di qualsiasi prova documentale e a tutti gli effetti processuali.

Tale approccio oblitera completamente l'esistenza di rilevanti problematiche che l'esperienza ha dimostrato essere centrali: la specificità del rapporto tra la teorica classica della prova documentale e la tecnica informatica che invece basa l'essenza del valore probatorio sull'analisi della rappresentazione in stretto rapporto con la modalità di rappresentazione, la tecnica di incorporamento e la natura del supporto[290].

Si può quindi affermare che la giurisprudenza[291] è generalmente incline "a limitarsi" ad un esame "sensoriale" della rappresentazione dei mezzi di prova documentale a contenuto informatico, senza procedere ad una preventiva e adeguata analisi su base tecnico-scientifica di tutti gli altri elementi del documento, unica procedura che possa autorizzare una corretta valutazione della prova documentale informatica[292]. Inoltre, non solo viene escluso o trascurato l'esame preliminare di tutti gli elementi del documento informatico, ma dove compulsato dalle parti, ad es. tramite la richiesta di effettuazione di un esame peritale, tale verifica viene scoraggiato e respinta.

La semplificazione operata dalla giurisprudenza nega la stessa sussistenza di tali problematiche che l'esperienza empirica e scientifica ha invece dimostrato essere centrali.

L'erroneità di tale approccio si evidenzia ove si approfondisca il rapporto tra rappresentazioni risultato di dati apparentemente simili, tra dati originali e dati originari, nonché tra copie di dati e altre forme di *output* che consentono di avere la medesima rappresentazione riprodotta con tecniche diverse.

---

[289] APRILE E., Sulla utilizzabilità processuale della riproduzione a stampa di documenti informatici effettuata nel corso di una operazione di polizia giudiziaria, Commento a Trib. Pescara, 6 ottobre 2006, in "Diritto dell'Internet", 2007, pp. 271 e ss..

[290] Cfr. TONINI P., La prova penale, op.cit.

[291] In merito alla superfluità di verifiche peritali sui dati oggetto di documenti informatici, v la giurisprudenza analizzata negli altri capitoli.

[292] L'approccio alla valutazione della prova in base alla mera rappresentazione del documento informatico rievoca l'antico problema della conoscenza oltre l'apparenza delle cose descritta da Platone nel Mito della caverna; v. PLATONE, La Repubblica, Libro VII, 514 – 520, in Volume II, BUR, Milano, 1981, p. 243-250.

La questione si comprende più facilmente sul piano empirico con una breve sequenza sperimentale:

a) verifica delle differenze tra rappresentazioni apparentemente simili:

1) si crei un testo, ad esempio il seguente: "Il problema della confusione tra il documento informatico e la rappresentazione in esso incorporata, si amplifica sul piano pratico in quanto in sede processuale si attribuisce valore probatorio alla mera rappresentazione".

.2) se con un programma[293] si calcola l'hash con tre algoritmi diversi (md5, sha-1 e sha512), si avrà:

Result for md5: fbe39292d029b975c0bd5f5ac5096740

Result for sha1: 53f46f25a91a9a3f4746f8247e7e11c127036501

Result for sha512: de1d2df2bc9479f850d660cec4034f5c8cf244c9ff15281 d008ba4b9036d89569fe72f3c80a66e56ffad2fdd3d4e4a873a3d4747ff489ec9ac8 0d1cb8bc57b7f

.3) si cambi il testo togliendo solo il punto finale e si ricalcoli l'hash con gli stessi algoritmi:

Result for md5: 1858c67959b1256486f1d7d386e17fd3

Result for sha1: 73be5499bffd38c0f8f4cc19870b23e96742e6e3

Result for sha512: e505fbebf7627a420f7d90c5596a4d2e2672d3f838e2a68d 914e3eeb58361df14142785e7efe5f15ac41e47bd5da4e47d0f21cfe1d4236c084b 9c427723bb049

.4) eliminando un punto è stato eliminato anche il relativo byte (00101110) e quindi anche l'hash è cambiato;

.5) può la rappresentazione considerarsi cambiata? In questo caso, non ha subito cambiamenti rilevanti, ma nel caso di sostituzione del punto con un punto interrogativo e quindi con il relativo byte (00111111) che dal punto cambia solo di soli due bit, il senso della frase cambia completamente passando da un'affermazione perentoria ad una domanda.

Il fenomeno è tanto più amplificato quanto più il testo è complesso e lungo.

Analoghe considerazioni possono essere svolte per documenti costituiti da file sonori o grafici.

La questione si complica nell'esperimento seguente in cui il cambio non viene effettuato nel testo rappresentato, bensì nelle operazioni riguardanti il file che incorpora la rappresentazione.

b) Verifica delle variazioni nel documento senza variazioni della rappresentazione:

1) si inserisca lo stesso testo creato ad hoc sub 1) in un documento digitale realizzato con il programma di scrittura Writer di OpenOffice versione 4.1.2[294];

[293] Per questo esperimento è stato usato un calcolatore di hash molto semplice, libero, disponibile su http://www.sha1-online.com/ .

[294] Cfr. http://www.openoffice.org/it/ .

2) si calcoli l'hash dell'intero file con un programma di calcolo[295], ad es. con i tre diversi algoritmi md5, sha-1 e sha512:
md5: de071bf7dc3ef8411969c7f3113c76bd
sha1: 97223782cf49ceb4eec0b8685e7bf4b29378d1d6
sha512: 0dd10190ebfd952984c6b984c761b5f3de69b272ea21dc75960f1e132f37153e588f71ea68fc59038a61324fe624ca1fefdd541e61248ef119ec2594b5a483fb
3) si apra il file e senza apportare modifiche al contenuto, si risalvi il file e se ne calcoli l'hash; si avrà:
md5: 67a0ee091295e11c70e5588676eaa4ac
sha1: 9c32ce747ea98543964df6306278c296cbf6ed4f
sha512: 9da5863e04c00a7e2c9244145cdf1ed2c436169fdde061344754142397c0d71b51f0f15bc16baf79ec946ce628b01f4093a6b65c4459fa229d4ac881479a2618

Come si può verificare, pur non avendo alterato la rappresentazione contenuta nel file, l'hash, calcolato con tre diversi algoritmi, risulta diverso a causa della semplice interazione con il file a seguito della quale il sistema operativo ha variato i dati di ultimo accesso e di ultimo salvataggio del file testimoniato dalla modifica dell'hash del file. Pertanto:

1) sono cambiati i metadati del file, ovvero quella tipologia di dati dai quali le parti del procedimento traggono maggiori informazioni per il procedimento, e che quindi spesso sono più importanti più delle stesse rappresentazioni contenute nei file;
2) i dati non sono stati cambiati direttamente dall'operatore che ha interagito con il file, bensì dal sistema operativo;
3) l'operatore dell'interazione è solo autore mediato della variazione dei dati attuata dal sistema informatico interposto;
4) partendo dall'hash non è possibile risalire ai dati modificati;
5) partendo dai dati (o dall'hash) non è possibile risalire all'autore del cambiamento, se non attraverso ulteriori attività induttive, solo parzialmente ricostruibili con le dinamiche del sistema.

c) Verifica del rapporto tra dati originali e dati originari di due file, l'uno generato come copia dall'altro:
1) si prenda il documento digitale realizzato con il programma di scrittura Writer di OpenOffice versione 4.1.2 e senza aprirlo lo si copi in una directory diversa da quella iniziale;
2) calcolando l'hash dell'intero file con un programma di calcolo[296], si ottiene:
md5: 67a0ee091295e11c70e5588676eaa4ac
sha1: 9c32ce747ea98543964df6306278c296cbf6ed4f

[295] V. ad es. http://www.slavasoft.com/zip/hashcalc.zip .
[296] Ad es. http://www.slavasoft.com/zip/hashcalc.zip .

sha512: 9da5863e04c00a7e2c9244145cdf1ed2c436169fdde061344754142397c0d71b51f0f15bc16baf79ec946ce628b01f4093a6b65c4459fa229d4ac881479a2618

3) in questo caso, gli hash dei due file sono perfettamente identici e quindi avremo due copie entrambe originali, ma solo uno dei due è la copia originaria ed è quella creata nell'esperimento n. 2.

Pertanto:

1. i metadati del secondo file non sono cambiati;
2. le sequenze di bit dei due file, l'uno copia dell'altro, sono perfettamente identiche e quindi generano lo stesso hash;
3. i due file sono entrambi originali, ma il file originario è quello che è venuto ad esistenza per primo rispetto all'altro che ne è copia;
4. l'operatore che ha interagito con il file può essere diverso da quello che ha generato il secondo file;
5. partendo dai dati (o dall'hash) non è possibile risalire all'autore della copia, se non attraverso ulteriori attività induttive, solo parzialmente ricostruibili con le dinamiche del sistema.

D) Documento informatico e forme diverse di rappresentazione e incorporamento.

Nel corso dei procedimenti penali, spesso si verifica che una parte, in luogo di un documento informatico costituito dal file originale o originario, fornisca una rappresentazione incorporata su supporto diverso da quello originario.

Tale fenomeno si verifica in particolar modo con l'acquisizione di documenti in formato o su supporti diversi da quelli originari, come ad esempio:

1) documento digitale costituito da file di testo in formato .txt, acquisito come documento digitale costituito da testo in formato .PDF; Tale situazione si verifica ad esempio nei casi in cui un fornitore di servizi telefonici acquisisca i dati originari prodotti in formato .txt dal sistema informatico e telematico che gestisce le operazioni di fatturazione dei servizi di telecomunicazione e di ripartizione tra vari gestori, converta i dati in formato .PDF e poi li invii in formato digitale al richiedente a fini procedurali; ebbene in tali casi, le operazioni di acquisizione e conversione determinano variazioni dei dati che possono indurre informazioni errate e quindi errori di valutazione;
2) documento digitale costituito da file di testo in formato .txt, acquisito come documento stampato su supporto cartaceo; tale situazione si verifica ad esempio nei casi in cui un fornitore di servizi telefonici acquisisca i dati originari prodotti in formato .txt dal sistema informatico e telematico che gestisce le operazioni di

fatturazione dei servizi di telecomunicazione e di ripartizione tra vari gestori, li stampi su supporto cartaceo e li invii al richiedente a fini procedurali; ebbene in tali casi, le operazioni di acquisizione e stampa determinano variazioni dei dati che possono indurre informazioni errate e quindi errori di valutazione;

3) documento cartaceo acquisito dalla fotocopiatura analogica della rappresentazione visualizzata sullo schermo di un dispositivo digitalizzato; tale situazione si verifica ad esempio nei casi in cui una parte acquisisca ad un procedimento la fotocopia dei messaggi digitali visualizzati sullo schermo di uno smartphone; ebbene in tali casi, le operazioni di acquisizione e conversione determinano perdita di metadati che possono indurre informazioni errate e quindi errori di valutazione;
4) documento cartaceo acquisito come documento digitalizzato costituito da file di testo in un formato arbitrario (.jpg, .txt, .PDF, ecc.) su un supporto magnetico; tale situazione si verifica ad esempio nei casi in cui una banca acquisisca da un documento originariamente generato su supporto cartaceo, come ad esempio un assegno bancario o una ricevuta, la sua immagine digitalizzata (mediante foto digitale o scansione) e la invii in formato digitale al richiedente a fini procedurali; ebbene in tali casi, le operazioni di acquisizione e conversione determinano generazione o variazione di dati che possono indurre informazioni errate e quindi errori di valutazione[297].

Ebbene, tali casi, che non esauriscono l'amplissima varietà di situazioni che si verificano nell'interscambio di formati, tecniche, tecnologie di riproduzione della rappresentazione, non avremo più lo stesso documento, ma avremo documenti ogni volta diversi, per una o più componenti, oltre alle caratteristiche proprie dei documenti digitali che andranno correttamente rapportati ai documenti derivati.

Per ognuna di queste tipologie, prima ancor di procedere alla valutazione del fatto rappresentato, bisognerà valutare la metamorfosi del documento e quindi le variazioni – in termini di aggiunta, perdita, modifica dei dati interni e dei metadati, originari o derivati – a causa e durante le operazioni di passaggio da una tecnica di incorporamento all'altro, da un supporto all'altro, e delle eventuali modifiche nella rappresentazione.

Tali questioni apparentemente teoriche, hanno ricadute dirette in tutti gli ambiti procedimentali, ad iniziare dal principio di preferenza dell'originale del documento previsto dall'art. 234, c. 2, secondo il quale: "*Quando l'originale di*

[297] Problematiche analoghe ma diverse possono essere causate mediante la sua fotocopia o fotoriproduzione in quanto basate su tecniche analogiche.

un documento del quale occorre far uso è per qualsiasi causa distrutto, smarrito o sottratto e non è possibile recuperarlo, può esserne acquisita copia.". Difatti, poiché tutte le modalità tecniche introdotte dalla L. 48/08 prevedono sempre la conservazione dei dati originali[298], ove l'acquisizione non venga svolta nelle forme partecipate e della perizia, è giocoforza dover ammettere le copie e i surrogati potranno essere acquisiti (e valutati come prova) solo in mancanza assoluta dei documenti originali, rectius: originari.

Inoltre, la verifica dei dati originali è strumentale all'esercizio del diritto di difesa sin dalle prime fasi dell'individuazione e acquisizione di dati informatici (*rectius*: documenti) rilevanti per il procedimento, alla valutazione della catena di custodia, al corretto svolgimento del dibattimento, alla formazione della regiudicanda.

Alla presa di coscienza del fenomeno consegue che alla documentabilità amplificata dalla tecnologia, deve corrispondere l'amplificazione del diritto per ciascuna parte del procedimento di verificare i dati originari, nel formato originario di ciascun documento digitale, se non si vuole che il procedimento si trasformi in un'antologia di documenti verosimili.

A tal proposito, tra le lacune più gravi rilevabili nella L. 48/08, vi è quella di non aver rivisto l'istituto della prova documentale informatica, quale archetipo di ogni documento informatico, caratterizzata da principi e tecniche di trattamento peculiari rispetto alla prova documentale tradizionale.

In secondo luogo, il legislatore ha omesso anche la specifica previsione di assicurare le garanzie di integrità e immodificabilità al mezzo di prova documentale informatica pur costituendo questo l'oggetto delle attività disciplinate dai mezzi di ricerca della prova informatica (ispezione, perquisizione, sequestro, ecc.).

Pertanto, proprio per la prova documentale informatica, non sono state previste quelle precauzioni introdotte dalla L. 48/08 per il trattamento dei dati digitali oggetto di attività di indagine e attività ad iniziativa della polizia giudiziaria che hanno come fine ultimo quello di proteggere l'oggetto delle attività acquisitive e il patrimonio informativo dei dati.

7.3.3 Il nuovo art. 234 bis sui documenti e dati informatici.

Di recente, nel codice di procedura penale, subito dopo l'art. 234 riguardante la Prova documentale, è stato introdotto l'art. 234-bis (Acquisizione di documenti e dati informatici), il quale prevede che "*1. È sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche*

[298] D'altronde, l'obbligo di conservazione dei dati originali previsti dalla Convenzione di Budapest e riversato nella L. 48/08 e nel Codice di procedura penale, è finalizzato proprio a consentire in ogni momento la verifica della conformità dei dati acquisiti al procedimento a quelli originali. Ove una qualunque parte del procedimento non sia stata coinvolta nel procedimento di acquisizione, avrà la facoltà di chiedere tale verifica.

diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare.».[299]

Come per la maggior parte dei casi di intervento normativo ad oggetto informatico, anche tale norma risente della fretta con la quale si è proceduto a delineare la reazione normativa ai recenti gravi fatti di terrorismo[300], per cui il risultato è un testo ancora oscuro ed apparentemente privo di utilità.

La rubrica, "Acquisizione di documenti e dati informatici", caratterizzata dall'uso dell'aggettivo "informatici" palesemente riferito ad entrambi i termini, "documenti e dati", preannuncerebbe una reale novità in tema di prova documentale informatica avente ad oggetto "documenti informatici" e "dati informatici".

In realtà, la rubrica mantiene meno di quanto prometta: non si tratta della disciplina dell'acquisizione di documenti e dati informatici, bensì di una particolare previsione tutt'altro che chiara.

Superato l'esordio letterale ricalcato su quello dell'art. 234 ma rinforzato dal pleonastico "sempre" forse per sgomberare il campo dalla tentazione di ammissioni a fasi alterne, la norma genera alcuni effetti poco chiari:

1. non si comprende se con il termine "conservati" si intenda dati informatici "archiviati" o "accessibili";
2. il riferimento all'acquisibilità di documentazione conservata all'estero suscita perplessità sul piano applicativo in quanto non si comprende per quali motivi la norma sia indirizzata solo ai documenti e ai dati informatici situati all'estero, mentre dalla portata della norma siano esclusi quelli situati in Italia; la risposta sarebbe da rinvenire nel fatto che per questa seconda ipotesi vale già la norma generale dell'art. 234?

---

[299] Articolo inserito dall'art. 2, comma 1 bis del D.L. 18 febbraio 2015 n. 7, convertito con modificazioni nella L. 17 aprile 2016, n. 43, "Integrazione delle misure di prevenzione e contrasto delle attività terroristiche". Per un commento al provvedimento, v. KOSTORIS R. E.,VIGANÒ, F., (a cura di), Il nuovo 'pacchetto antiterrorismo, G. Giappichelli Editore, Torino, 2015.

[300] Gli interventi "di reazione" contraddistinguono la normazione d'urgenza sulle norme penalistiche ad oggetto informatico e telematico. E' stato così per i c.d. "Pacchetti Sicurezza", per le numerose modifiche periodicamente intervenute (e che interverranno) sull'art. 132 D. Lgs. 196/2003, per le norme del c.d. Decreto Pisanu, per la modifica dell'art. 612 bis c.p. in tema di *cyberstalking*. Sul piano della politica criminale, si tratta di interventi che si pongono l'obiettivo dichiarato di reagire ai gravi fatti di criminalità, terroristica, organizzata, o comune e che sul piano simbolico indurrebbero l'illusoria sensazione di una pronta reazione ai gravi fatti che destano allarme sociale. Sul piano della tecnica normativa, invece, gli interventi, assecondando la domanda di strumenti (e poteri) di controllo sui dati ritenuti indispensabili a realizzare un'azione di contrasto prospettata come più efficace, si traducono per lo più in innesti di incisi nell'impianto normativo preesistente al di fuori di ogni preventiva valutazione di impatto sistemico. In realtà, esaminando i provvedimenti successivi al varo di tali norme, non emergono elementi dai quali si possa concludere in favore dell'efficacia di tale impostazione. Pertanto, non si può evitare di rilevare che la bulimia di dati e il mito del controllo totale in nome della prevenzione deprimono le libertà civili senza alcun altro beneficio in termini di maggior sicurezza.

3. inoltre la norma si estende ai dati informatici "anche diversi da quelli disponibili al pubblico", il che significa che possono essere acquisiti sia quelli disponibili che quelli non disponibili al pubblico;
4. ma nel caso in cui si tratti di dati "anche diversi da quelli disponibili al pubblico", cioè di "dati non disponibili al pubblico", l'acquisizione è sempre consentita ma "previo consenso del legittimo titolare". Orbene, per tale eventualità non si comprende su richiesta di chi, con quali modalità e forme ed entro quale termine il legittimo titolare della documentazione e dei dati possa o debba esprimere il consenso preventivo, così come non si comprende quale sia il regime e le conseguenze nel caso in cui il titolare rifiuti di prestare il preventivo consenso, né quale sia la *ratio* della richiesta del consenso per i dati all'estero non disponibili al pubblico rispetto a quelli disponibili o che siano "conservati" in Italia.

Il risultato della lettura complessiva della norma è francamente oscuro e se da un lato non si comprende quale fattispecie applicativa abbia ispirato il legislatore, la chiave esegetica sarà probabilmente palesata dalle prime applicazioni pratiche.

A tal proposito sono interessanti i rilievi di chi[301] ha rinvenuto nella norma la possibilità che si sia voluto attuare tardivamente l'art. 32 della Convenzione di Budapest[302] il quale prevede quanto segue:

"Articolo 32 – Accesso transfrontaliero ai dati informatici archiviati, con il consenso o dove accessibili al pubblico

Una Parte può, senza l'autorizzazione di un'altra Parte:

a accedere ai dati informatici archiviati accessibili al pubblico (sorgente aperta), indipendentemente da dove i dati sono geograficamente localizzati; o

---

[301] cfr. SPECCHIO G., Il nuovo mezzo di «prova digitale», 2015, in *http://thinkinginforensics.net/2015/05/il-nuovo-mezzo-di-prova-digitale/#more-1624*.

[302] Nel testo inglese, la norma è la seguente: "*Article 32 – Trans-border access to stored computer data with consent or where publicly available. A Party may, without the authorisation of another Party:*
a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system".
Nel testo francese, la medesima norma è la seguente:"*Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public*
Une Partie peut, sans l'autorisation d'une autre Partie :
a accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou
b accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique."

b accedere a o ricevere, per mezzo di un sistema informatico situato nel suo territorio, a dati informatici archiviati situati in un altro Parte, se la Parte ottiene il consenso legittimo della persona che ha il legittimo potere/facoltà di divulgare i dati alla Parte per mezzo del sistema informatico."

Il motivo per il quale avevamo escluso l'ipotesi in esame è data dal fatto che nella Relazione accompagnatoria al Disegno di legge n. 2807 per la Ratifica ed esecuzione della Convenzione poi attuata con la L. 48/08[303], era stato espresso a chiare lettere che le previsioni delle norme previste dall'art. 23 sino all'art. 34 della stessa, fossero già attuate dalla normativa codicistica: "*(...) D'altra parte, l'apparato normativo contenuto nel libro undicesimo del codice di procedura penale – più volte aggiornato in attuazione di strumenti internazionali sottoscritti dal nostro Paese – è perfettamente idoneo ad attuare le disposizioni di cooperazione internazionale contenute nella Convenzione, tanto più che si tratta di disposizioni di tipo tradizionale, comuni a molte altre convenzioni. Lo stesso può dirsi per gli articoli in materia di giurisdizione, con riferimento al nostro codice penale.*

Per motivi di chiarezza, peraltro, si è deciso di indicare in questa relazione, oltre che le nuove disposizioni introdotte con la legge di autorizzazione alla ratifica, le principali corrispondenze tra le disposizioni della Convenzione in materia di giurisdizione e cooperazione internazionale e la nostra normativa interna. (...)".

In particolare, per le norme relative alle misure di collaborazione internazionale, quanto all'art. 31 della Convenzione in punto di "*Assistenza in materia di poteri di investigazione",* la Relazione riteneva che "(...) *L'articolo 31 della Convenzione è attuato dagli articoli 737 e 737-bis del codice di procedura penale. Quanto all'articolo 32, sembra pacifica la possibilità per chiunque di accedere a dati pubblici ovvero a dati messi a disposizione da chi è autorizzato a divulgarli. I dati così ottenuti verranno utilizzati secondo le norme esistenti in materia di utilizzabilità della prova. (...)".*

Ebbene, il legislatore sul punto ha avuto un ripensamento postumo, ma il risultato non è stato all'altezza nemmeno delle pur discutibili modifiche introdotte dalla L. 48/08, atteso che:

1) la Convenzione parla solo di dati informatici (*computer data*) mentre l'art. 234 *bis* aggiunge anche i documenti a conferma della consueta incertezza che muove il legislatore e che lo induce ad ampliare la portata della fattispecie ad espressioni pleonastiche; tuttavia, vanno riconosciuti sintomi di miglioramento rispetto alla formulazione delle norme della L. 48/08 che ai "*dati*" abbinava sempre anche le "*informazioni e programmi informatici*";

[303] Cfr. Atti Parlamentari — 9 — Camera dei Deputati — 2807 XV LEGISLATURA — DISEGNI DI LEGGE E RELAZIONI — DOCUMENTI.

2) nel formulare la norma, oltre a comprendere il termine "dati" come previsto dall'art. 32 della Convenzione, con un'artificiosa operazione lessicale, è stato affiancato anche il termine "documenti" creando così l'occasione per collocare la norma nell'ambito dei mezzi di prova documentale. L'operazione è tanto più discutibile quanto più si osserva che l'art. 32 della Convenzione è invece collocato sotto "Capitolo III – Cooperazione internazionale" della Convenzione, nell'ambito del "Titolo 2 – Mutua assistenza relativa ai poteri investigativi[304]. Quindi, l'art. 32 della Convenzione non intendeva specificare un mezzo di prova, che infatti la L. 48/08 non aveva toccato, bensì inserire uno strumento di cooperazione internazionale volto a regolare i rapporti tra Paesi aderenti ed a superare sia le giurisdizioni nazionali, sia la necessità di ricorrere allo strumento della rogatoria internazionale anche per le attività investigative che necessitino di superare i confini virtuali. Se questa è la *ratio* del disposto di cui all'art. 32 della Convenzione della norma, allora la sua naturale collocazione sarebbe stata non nell'ambito dei mezzi di prova - a tutto concedere - nell'ambito del Libro XI del codice di procedura penale, magari quale deroga alla previsione generale dell'art. 727. Al contrario, il legislatore italiano ha operato una mutazione genetica volgendolo da strumento di cooperazione a mezzo di prova documentale valevole tra le parti.

Il dubbio che legittimamente sorge, e che allo stato rimane solo una supposizione, è che tale previsione stia invece preparando la strada a norme ben più preoccupanti in tema di acquisizione di documenti, anche all'estero, mediante accesso da remoto ai dispositivi mediante l'uso di captatori informatici di cui si è già detto sopra.

Per concludere, la prassi applicativa mostrerà il vero volto di tale norma ed in quale misura si collocherà nella trama procedimentale.

Tenuto conto che la natura fisica di tali documenti è costituita da bit, anche in relazione a tale strumento si pongono tutti i problemi affrontati sino ad ora in relazione al trattamento dei dati digitali, con la complicazione dell'acquisizione all'estero, circostanza che articolerà ulteriormente la complessità delle problematiche sino ad ora affrontate.

[304] L'art. 32 della Convenzione è collocato *sub* "*Chapter III – International co-operation (...) Title 2 – Mutual assistance regarding investigative powers"* .

8 L'esperimento giudiziale

Tuttavia, vi sono casi nei quali le stesse tecnologie digitali che mal usate determinano le criticità sopra esaminate, in altri ambiti del processo penale rivitalizzino istituti sino ad oggi quiescenti.

Ciò accade allorquando la tecnologia informatica venga utilizzata per replicare virtualmente fatti accaduti nella realtà. Tale potenzialità può trovare ampia applicazione nell'ambito di un procedimento penale al fine di accertare le dinamiche di un fatto processualmente rilevante, secondo la forma giuridica dell'esperimento giudiziale, un mezzo di prova previsto dall'art. 218 che così recita: "*Presupposti dell'esperimento giudiziale*

1. L'esperimento giudiziale è ammesso [392 1 lett. f] quando occorre accertare se un fatto sia o possa essere avvenuto in un determinato modo.

2. L'esperimento consiste nella riproduzione, per quanto è possibile, della situazione in cui il fatto si afferma o si ritiene essere avvenuto e nella ripetizione delle modalità di svolgimento del fatto stesso".

Tale mezzo di prova consente di "replicare" artificialmente la dinamica di un determinato fatto per verificarne le modalità di accadimento, mediante una ricostruzione verosimile rispetto a quanto riferito da testimoni o dalle altre parti del processo in relazione alla dinamica affermata o supposta, seguita dalla sua replica.

Con tale mezzo di prova, può essere ad esempio ricostruita e replicata fittiziamente la dinamica di un sinistro, di una rapina, di un omicidio, ma anche di grandi eventi catastrofici.

Quanto alle modalità di espletamento di tale mezzo di prova, l'art. 219 prevede quanto segue: "*Modalità di espletamento dell'esperimento giudiziale*

1. L'ordinanza che dispone l'esperimento giudiziale contiene una succinta enunciazione dell'oggetto dello stesso e l'indicazione del giorno, dell'ora e del luogo in cui si procederà alle operazioni. Con la stessa ordinanza o con un provvedimento successivo il giudice può designare un esperto per l'esecuzione di determinate operazioni.

2. Il giudice dà gli opportuni provvedimenti per lo svolgimento delle operazioni, disponendo per le rilevazioni fotografiche o cinematografiche o con altri strumenti o procedimenti.

3. Anche quando l'esperimento è eseguito fuori dell'aula di udienza, il giudice può adottare i provvedimenti previsti dall'articolo 471 al fine di assicurare il regolare compimento dell'atto.

4. Nel determinare le modalità dell'esperimento, il giudice, se del caso, dà le opportune disposizioni affinché esso si svolga in modo da non offendere

sentimenti di coscienza e da non esporre a pericolo l'incolumità delle persone o la sicurezza pubblica."

È quindi il giudice che stabilisce con ordinanza l'oggetto dell'esperimento e, con lo stesso provvedimento o successivo, può designare un esperto per l'esecuzione di determinate operazioni. Si può trattare di esperto incaricato di eseguire parte dell'esperimento, ad esempio mediante la ricostruzione della scenografia, o l'allestimento di mezzi e strumenti per la replica della dinamica, anche a contenuto tecnico; ma può anche trattarsi di un esperto che, ad es., replichi determinati comportamenti e quindi "reciti" una parte nell'ambito della più ampia ricostruzione di un evento.

Poiché la norma affida al giudice la conduzione dell'esperimento, questo "*dà gli opportuni provvedimenti per lo svolgimento delle operazioni",* mentre il ruolo del tecnico (o di più tecnici), può essere quello, si passi la metafora cinematografica, di "aiuto regista", di tecnico (macchinista, luci, suoni, armi, effetti speciali) o di attore.

Le operazioni devono essere oggetto di rilevazioni fotografiche o cinematografiche o con altri strumenti o procedimenti, al fine di costituire una forma di documentazione del contenuto dell'esperimento per gli atti del processo, ma anche per consentire alle parti di valutare a posteriori gli esiti dell'esperimento che, di per sé, sono connotati dall'irripetibilità.

Infine, quando l'esperimento viene svolto all'esterno dell'aula, il giudice deve adottare i provvedimenti per il regolare svolgimento dell'attività costituente a tutti gli effetti udienza pubblica (art. 471), dando disposizioni affinché le operazioni non offendano sentimenti di coscienza e non creino rischi per l'incolumità delle persone o la sicurezza pubblica.

Affinché la ricostruzione sia quanto più verosimile rispetto ai dati accertati o da verificare, e per riprodurre più verosimilmente le condizioni ambientali e le dinamiche del fatto, possono essere usati contesti e luoghi reali o artificiali che riproducano quelli reali.

Lo strumento dell'esperimento giudiziale, pur essendo mezzo di prova di innegabile utilità nella ricostruzione delle dinamiche dei fatti oggetto di procedimento, richiede notevoli risorse economiche ed organizzative, peraltro a fronte dell'alea di incertezza circa la proficuità dell'esito in termini di accrescimento del patrimonio informativo.

Pertanto, in passato, l'utilizzo che si è fatto di tale strumento è stato particolarmente modesto e limitato a fatti di rilevante gravità e connotati da un alto grado di incertezza circa le modalità di accadimento.

8.1 L'esperimento giudiziale informatico

L'evoluzione tecnologica consente oggi di riprodurre la dinamica dei fatti oggetto di procedimento con modalità virtuali, realizzate sostanzialmente con due diverse tipologie di strumenti messi a disposizione dall'informatica.

Ad una prima categoria[305], appartengono quei programmi informatici di simulazione che ricreano una realtà virtuale e consentono di rappresentare fittiziamente una dinamica svoltasi nella realtà.

Tali programmi sono molto utili per molteplici aspetti:

1) consentono di ricreare situazioni che per le loro modalità di svolgimento sono caratterizzate da fenomeni di enorme ampiezza che sarebbe impossibile replicare nella realtà, come ad esempio la rovina del fianco di una montagna in un bacino idrico delimitato da una diga, o il crollo di due grattacieli provocato dall'impatto di due aerei, o la collisione di due navi, o un omicidio con una dinamica complessa;

2) consentono di creare modelli virtuali nei quali le dinamiche possibili possono essere replicate più volte, verificando i diversi effetti derivanti dal cambio di ogni singolo parametro di impostazione;

3) consentono di documentare, archiviare e riutilizzare i modelli e i risultati ottenuti.

Vi è poi una seconda categoria di esperimenti giudiziari informatici che non sono realizzati virtualizzando la realtà, bensì virtualizzando fatti svoltisi già originariamente in ambito informatico e riprodotti in un ambiente informatico artificiale chiamato "macchina virtuale" o *Virtual Machine* (VM).

Secondo una notoria definizione:"*In informatica il termine macchina virtuale (VM) indica un software che, attraverso un processo di virtualizzazione, crea un ambiente virtuale che emula tipicamente il comportamento di una macchina fisica grazie all'assegnazione di risorse hardware (porzioni di disco rigido, RAM e risorse di processamento) ed in cui alcune applicazioni possono essere eseguite come se interagissero con tale macchina (...)*"[306].

Infine, vi è un'ulteriore forma di un ambiente informatico virtuale chiamato Parallel Virtual Machine (PVM), nel quale una pluralità di sistemi informatici concorre alla creazione di di un unico sistema virtuale. Secondo la definizione:"*Se nella sua accezione originaria il concetto di virtual machine indicava la suddivisione di un singolo computer tra più utenti, la potenza sempre crescente dei computer ha fatto sorgere l'esigenza inversa: far percepire come unica entità un sistema composto da molti computer distinti. In*

[305] Tali applicazioni rientrano nella categoria conosciuta come *Computer generated evidence*, per la quale v. SBISÀ F., Le computer generated evidence da strumento a prova scientifico-tecnica nel processo penale statunitense, in CONTI C. (a cura di) Scienza e processo penale. Nuove frontiere e vecchi pregiudizi, Giuffrè, Milano, 2001.

questo caso si parla di Parallel Virtual Machine. L'uso più classico di questa tecnologia è quello della creazione di cluster di centinaia, se non migliaia, di elaboratori per sostenere carichi di lavoro massicciamente parallelizzabili. (...)"[307].

Le PVM sono particolarmente utili per simulare fatti informatici di particolare complessità o per ricostruire dinamiche complesse per le quali si renda necessario elaborare rilevanti quantità di dati che richiedano una potenza di calcolo particolarmente elevata.

Le basi scientifiche e tecniche di funzionamento delle macchine virtuali sono note, studiate e applicate, per quanto in continua evoluzione in dipendenza dell'evoluzione tecnologica, così come sono note le applicazioni di tali tecnologie nell'Informatica forense[308].

Le VM possono costituire una sorta di "laboratorio informatico" nel quale replicare artificialmente le dinamiche svoltesi originariamente in ambiente informatico o telematico, come ad es. per la ricostruzione di scambi di file a contenuto illecito o protetto dal diritto d'autore, e soprattutto per simulare l'azione di virus nei reati di danneggiamento informatico, o un attacco informatico mediante *botnet*[309].

L'efficacia tecnica dell'uso delle VM dipende da diversi fattori:

1. dalla scientificità delle procedure e delle tecniche seguite in fase di acquisizione e conservazione dei dati, secondo i migliori standard disponibili;
2. dalla qualità degli strumenti hardware e software, con una particolare preferenza per gli strumenti *open source* che consentono lo studio e la verifica delle modalità di trattamento dei dati durante l'esperimento;
3. dalla competenza del tecnico, che dovrà essere esperto non solo di informatica, ma anche di informatica forense;
4. da un effettivo contraddittorio su tutte le attività prodromiche, concomitanti e successive, all'esperimento giudiziale e in tutte le sue fasi.

[306] Cfr. voce Macchina virtuale, in *https://it.wikipedia.org/wiki/Macchina_virtuale*.
[307] *Ibidem*
[308] BEM, D., Virtual Machine for Computer Forensics – the Open Source Perspective, in HUEBNER E., ZANERO S. (a cura di), Open Source Software for Digital Forensics, Springer, New York, 2010, p. 25 ; NICOSIA G., CACCAVELLA D.E., Macchine virtuali e sistema della prova nel processo civile e epenale, In Diritto dell'Internet, 2008, p. 527.
[309] Una *botnet* è una rete formata da dispositivi informatici collegati ad Internet e infettati da malware, controllata da un'unica entità, il *botmaster*. A causa di falle nella sicurezza o per mancanza di attenzione da parte dell'utente e dell'amministratore di sistema, i dispositivi vengono infettati da virus informatici o *trojan* i quali consentono ai loro creatori di controllare il sistema da remoto. I controllori della botnet possono in questo modo sfruttare i sistemi compromessi per scagliare attacchi distribuiti del tipo *distributed denial of service* (DDoS) contro qualsiasi altro sistema in rete oppure compiere altre operazioni illecite, in taluni casi agendo persino su commissione di organizzazioni criminali. I dispositivi che compongono la botnet sono chiamati *bot* (da roBOT) o *zombie*; cfr. *https://it.wikipedia.org/wiki/Botnet*.

A mio parere, proprio tale mezzo di prova, sino ad oggi raramente disposto per le evidenti implicazioni organizzative, procedurali e, non da ultimo, economiche, troverà motivi di rivalutazione e nuova vita proprio in relazione ai reati informatici propriamente detti.

È proprio in quest'ultimo settore che le VM troveranno un ottimo strumento di replica e documentazione a fini processuali delle dinamiche informatiche, anche in conseguenza della convergenza tra tecnologie sempre più sofisticate, ed aumento dei casi di applicazione.

Tuttavia, la complessità di tale strumento e la sua suggestività si presta ad errori e strumentalizzazioni che amplificano, volontariamente o indirettamente, gli effetti distorsivi della rappresentazione artificiale. Per tale motivo, tutti gli attori processuali sono investiti della gravosa responsabilità di comprenderne i meccanismi e governarne l'applicazione.

L'esperimento giudiziale non costituisce solo il paradigma di un nuovo approccio applicativo delle tecnologie al processo sul quale si misureranno le capacità degli operatori forensi, ma anche il banco di collaudo delle norme sul giusto processo e sull'effettivo esercizio del diritto di difesa di fronte alle sfide dell'innovazione.

Conclusioni

Quanto esposto conferma gli assunti iniziali ovvero che, secondo i principi sistematizzati dall'Informatica forense, i dati digitali sono di per sé neutri e per mantenere integre le informazioni che se ne possono trarre, devono essere trattati secondo le modalità introdotte dalla L.48/08, con le tecniche scientifiche che ne rispettano le caratteristiche fisiche a vantaggio di tutte le parti del processo e nel quadro di procedure che riconoscano alle stesse il diritto a partecipare sin dal primo momento alle operazioni tecniche che li riguardano.

Solo l'adozione delle opportune metodologie tecnico-scientifiche, nel quadro di procedure che impediscano la strumentalizzazione degli accertamenti per fini di parte, assicura il maggior grado possibile di oggettività e certezza dei dati, nonchè garantisce a tutte le parti coinvolte nel procedimento – giudice incluso – lo svolgimento delle rispettive attività.

Al contrario, i dati assunti al di fuori di tali criteri, sotto il profilo giuridico prestano il fianco al rischio di inutilizzabilità, mentre sotto il profilo del merito legittimano informazioni erronee o inattendibili, in ogni caso inidonee a costituire la base di sentenze capaci di superare il limite minimo "al di là di ogni ragionevole dubbio".

Nonostante tali assunti, la disamina della giurisprudenza di merito e di legittimità ha dimostrato la progressiva riduzione della portata delle innovazioni della L. 48/08 e quindi la difficoltà che emergano orientamenti che inquadrino correttamente i fatti digitali nella cornice delle norme giuridiche e tecniche che sovrintendono alle operazioni di trattamento dei dati digitali a fini probatori.

Ove tale tendenza dovesse consolidarsi, si assisterebbe ad un'anacronistica regressione dello sforzo riformatore e interpretativo teso ad assicurare che i dati digitali siano trattati in modo tale da garantire a tutte le parti del processo il corretto esercizio delle proprie prerogative processuali, alla luce delle norme costituzionali in punto di Giusto processo.

Sul piano dei correttivi, l'ideale sarebbe quello di evitare l'interpolazione del modello pre-informatico riproducendo quindi in formato digitale le dinamiche analogiche, con il risultato di amplificare le incertezze e, per molti aspetti, le inefficienze del sistema preesistente. Al contrario, gli algoritmi delle sequenze processuali dovrebbero esser riformulati *ex novo* secondo logiche digitali native.

Tuttavia, alla luce della consapevolezza che anche in ambito giuridico la storia raramente procede per salti, sul piano dei correttivi praticabili, il corso in atto potrebbe essere rettificato intraprendendo decise iniziative di aggiornamento normativo e quindi:

- riconoscendo al dato informatico la dignità e la tutela di autonomo bene giuridico;

- aggiornando le norme in punto di Giusto Processo, riconoscendo la necessità di adeguare modi, tempi e condizioni per la preparazione della difesa alle peculiarità imposte dalle innovazioni tecnologiche;

- rivisitando il sistema processuale per valorizzare il ruolo, ormai preponderante, della tecnologia digitale e della prova documentale informatica;

- stabilendo che il *thema probandum* ad oggetto informatico sia soggetto alla formazione in contraddittorio sin dal momento dell'acquisizione dei dati;

- riconoscendo la centralità del metodo scientifico e tecnico che garantisce il corretto trattamento dei dati e della prova documentale informatica, secondo gli Standard internazionali;

- fissando la sanzione dell'inutilizzabilità o della nullità alle prove acquisite in violazione delle norme introdotte dalla L. 48/08.

* * *

Le innovazioni dell'era dell'informazione in campo socio-economico si riflettono anche sul piano giuridico e il processo penale è specchio privilegiato della società e dei tempi.

Allo stato, le questioni affrontate riguardano ancora poche norme rispetto alle restanti che compongono l'edificio processuale.

Tuttavia, all'esito del presente lavoro, a fianco dei molti dubbi riguardanti l'esito di tali questioni, permane un'unica certezza sul futuro stesso del processo penale: un giorno, non molto lontano, la dimensione digitale sarà forma e contenuto dell'intero procedimento penale, cosicché gli istituti estranei alla digitalizzazione ed alle regole dell'Informatica forense saranno quelli residuali.

Pertanto, va raccolta la sfida di governare l'ammodernamento del sistema processuale penale, e se necessario di reingegnerizzarlo, per dare risposte giuridiche al passo con le peculiarità della nuova era digitale, coniugando la necessità di accertare e reprimere i reati, con il metodo scientifico nel trattamento dei dati digitali, nel quadro dei diritti fondamentali delle parti coinvolte nel procedimento.

Bibliografia

AA.VV, Inside attack. Tecniche di intervento e strategie di prevenzione.Manuale di ricerca e di intervento sul computer crime nelle organizzazioni. Nuovo studio tecna, Roma, 2005.

AA.VV. Decisione giudiziaria e verità scientifica, Giuffrè, Milano, 2005.

AA.VV., Crimes & computers (Delitti e computers), Presidenza del Consiglio dei Ministri, Dipartimento per l'Informazione e l'Editoria, Roma, Istituto Poligrafico e Zecca dello Stato, 2004.

AIRALA A. D., Argentina: a las puertas de una Nueva Especializacion: La Informatica Forense, "Alfa – Redi Revista de Derecho Informatico", n. 055, 2003, in *http://www.alfa-redi.org/revista/data/57-10.asp*.

AMARELLI G., Furto (art. 624 c.p.), in FIORE, S., (a cura di), Reati contro il patrimonio, Utet, Torino, 2010.

AMATO G., DESTITO V. S., DEZZANI G., SANTORIELLO, C., I reati informatici, Cedam, Milano, 2010; LUPARIA L., (a cura di), Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest, Giuffrè, Milano, 2009.

AMMIRATI D., (a cura di), Internet e la legge penale, Giappichelli, Torino, 2001.

ANASTASI J., The new forensics, John Wiley & Sons, 2003.

ANGELETTI R., Le invalidità delle prove e dei mezzi di prova, Giappichelli, Torino, 2005.

ANTOLA A., MEZZALIRA L., NEGRINI R., SCARABOTTOLO N., Nuovo dizionario di informatica, Mondadori, Milano, 1996.

ANTOLISEI F., Manuale di diritto penale, Parte generale, Giuffrè, Milano, 1987.

APRILE E., SILVESTRI P., La formazione della prova penale, Giuffrè, Milano, 2002.

APRILE E., Sulla utilizzabilità processuale della riproduzione a stampa di documenti informatici effettuata nel corso di una operazione di polizia giudiziaria, Commento a Trib. Pescara, 6 ottobre 2006, in "Diritto dell'Internet", 2007.

ASARO C., Ingegneria della conoscenza giuridica applicata al diritto penale, Aracne, Ariccia, 2012.

ATERNO S., CAJANI F., COSTABILE G., MATTIUCCI M., MAZZARACO G., (a cura di), Computer forensics e indagini digitali Experta, Forlì, 2011.

ATERNO S., MAZZOTTA P., La perizia e la consulenza tecnica. Cedam, 2006.

AUSTIN J.L., How to do Things with Words, Second Edition (Oxford: Oxford University Press, 1975).

BANERJEE A., BRIDGES C.A., YAN J.-Q., ACZEL A. A., LI L., STONE M. B., GRANROTH G. E., LUMSDEN M. D., YIU Y., KNOLLE J., BHATTACHARJEE S., KOVRIZHIN D. L., MOESSNER R., TENNANT D. A., MANDRUS D. G., NAGLER S. E., Proximate Kitaev quantum spin liquid behaviour in a honeycomb magnet, 2016, in *http://www.nature.com/nmat/ journal/ vaop/ncurrent/full/nmat4604.html#access*.

BARBARISI M., Diritto e informatica, Edizioni Simone, Napoli, 1997.

BEM, D., Virtual Machine for Computer Forensics – the Open Source Perspective, in HUEBNER E., ZANERO S. (a cura di), Open Source Software for Digital Forensics, Springer, New York, 2010.

BLAK, H. C., Blak's Law Dictionary, West Publishing CO, St. Paul, Minnesota (USA), 1990.

BONI M., Informatica, Apogeo, Milano, 2005, p. 7.

BONOMO, A., "Le investigazioni con l'impiego di intercettazioni di comunicazioni e di flussi informatici o telematici. I nuovi strumenti di comunicazione telematica ed informatica: aspetti tecnici e questioni giuridiche coordinatore", CONSIGLIO SUPERIORE DELLA MAGISTRATURA, Incontro di studi sul tema "Tecniche di indagine e rapporti tra p.m., polizia giudiziaria, consulenti tecnici e difensori", Roma, 4-8 luglio 2011, in *http://docplayer.it/5178908-Consiglio-superiore-della-magistratura-le-investigazioni-con-l-impiego-di-intercettazioni-di-comunicazio ni-e-di- flussi-informatici-o-telematici.html*.

BOVIO, L., Prova informatica e processo penale, inserto in Polizia Moderna, marzo 2015.

BOZZETTI, M., POZZI, P., (a cura di), Cyberwar o sicurezza? Secondo Osservatorio Criminalità ICT, FTI, Franco Angeli, Milano, 2000.

BRESCIA G., Il consulente tecnico e la perizia nel processo civile e penale, IV ed., Maggioli, Rimini, 2006.

BREZINSKI D., KILLALEA T., Guidelines for evidence collection and archiving, RFC 3227, Best Current Practice 55 della Internet Engineering Task Force, 2002, in *https://tools. ietf.org/html/rfc3227*.

BUFFA F., Il processo civile telematico. La giustizia informatizzata, Giuffrè, Milano, 2002.

BUFFA F., Informatica, internet e diritto penale, II ed., Giuffrè, Milano, 2003.

CACCAVELLA D. E., FERRAZZANO M., BONORRI F., L'implementazione dei processi organizzativi finalizzati alla gestione del rischio nell'ambito di strutture sanitarie, in FARALLI C., BRIGHI R., MARTONI M., (a cura di), Strumenti, diritti, regole e nuove relazioni di cura, Giappichelli, Torino, 2015.

CADOZ C., Le realtà virtuali, Milano, il Saggiatore, 1998.
CAJANI F., La Convenzione di Budapest nell'insostenibile salto all'indietro del legislatore italiano: quello che le norme non dicono... in "Ciberspazio e Diritto", 2010, Vol. 11, n. 1.
CAMON, A., art. 266 c.p.p., in AA.VV., Commentario breve al codice di procedura penale, a cura di CONSO G., ILLUMINATI, G., II ed., Cedam, Padova, 2015.
CARNELUTTI F., La prova civile (1915), Giuffrè, Milano.
CARNELUTTI F., Principi del processo penale, Morano, Napoli, 1960 e La prova civile (1915), Giuffrè, Milano.
CARNEVALI D., CONTINI F., FABRI M., (a cura di) Tecnologie per la Giustizia. Isuccessi e le false promesse dell'E-Justice, Giuffrè, Milano, 2006.
CASEY E., Digital Evidence and Computer Crime - Forensic Science, Computer and the Internet, Academic Press, 2004.
CASEY E., Handbook of Computer Crime Investigation: Forensic Tools and Technology, Academic Press, 2001 e Handbook of Computer Crime Investigation, Academic Press, 2002.
CASSANO G., (a cura di), Diritto delle nuove tecnologie informatiche e dell'Internet, Ipsoa, Milano, 2002.
CATULLO F. G., Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova penale digitale. Profili sostanziali, in Diritto dell'Internet, 2006, n. 2.
CECCACCI, G., Computer Crimes – La nuova disciplina sui reati informatici, Edizioni FAG, Milano, 1994.
CERQUA F., Ancora dubbi e incertezze sull'acquisizione della corrispondenza elettronica, 2015, in *http://www.penalecontemporaneo.it/upload/1437560206*.
CERQUA_F._2015a.pdf; CACCAVELLA D., E., Gli accertamenti tecnici in ambito informatico, in ATERNO S., MAZZOTTA P., La perizia e la consulenza tecnica. Cedam, Padova, 2006, p. 195.
CEVENINI C., DI COCCO, C., SARTOR, G., Lezioni di informatica giuridica, Gedit, Bologna, 2005.
CHELO A., Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria, Cedam, Padova, 2014.
CHIAVARIO M. (a cura di), Nuove tecnologie e processo penale, Giappichelli, Torino, 2006.
CHICCARELLI S., MONTI A., Spaghetti hacker - Storie, tecniche e aspetti giuridici dell'hacking in Italia, Apogeo, Milano, 1997.
CHURCH G. M, GAO Y., KOSURI S., Next-Generation Digital Information Storage in DNA, in *http://arep.med.harvard.edu/pdf/Church_Science_12.pdf*.
CIACCI G., Le fonti del diritto dell'informatica, in VALENTINO, D., (a cura di) Manuale di diritto dell'informatica, II ed., ESI, Napoli, 2011.

CINTI M., Quantificazione ed individuazione delle alterazioni dei dati nell'ambito di indagini di Informatica Forense, tesi di laurea, a.a. 2010-2011, Facoltà di Scienze matematiche, fisiche e naturali, Alma Mater Studiorum · Università di Bologna, in *http://amslaurea.unibo.it/2736/1/cinti_mariagrazia_tesi.pdf*.

COLLIN S.M.H., Dictionary of Computing, Teddington, 1988.

COLOYANNIDES M. A, Computer Forensics and Privacy, Norwood, 2001.

Commissione Europea – Direzione Generale Giustizia Libertà e Sicurezza - Progetto AGIS 2005/AGIS/119 su "The Admissibility of Electronic Evidence at Court: Fighting against High Tech Crime", atti in Cybex, (a cura di), conclusioni del Programma, in *www.cybex.es*.

CONTI C. (a cura di), Scienza e processo penale. Nuove frontiere e vecchi pregiudizi, Giuffrè, Milano, 2011.

CORASANITI G., CORRIAS LUCENTE G., (a cura di), Cybercrime, responsabilità degli utenti, prova digitale, Cedam, Padova, 2009.

CUOMO L., RAZZANTE R., La nuova disciplina dei reati informatici, Giappichelli, Torino, 2009.

CURTOTTI NAPPI D., SARAVO L., Le indagini sulla scena del crimine. Discrasia legislativa, 2011, in *http://www.carabinieri.it/editoria/rassegna-dell-arma/anno-2011/n-2---aprile-giugno/studi/le-indagini-sulla-scena-del-crimine-discrasia-legislativa-*.

DE CATALDO NEUBURGER, L. (a cura di) La prova scientifica nel processo penale, Cedam, Padova, 2007.

DE FRANCESCO A., Il principio del contraddittorio nella formazione della prova nella costituzione italiana, Giuffrè, Milano, 2005.

DE FRANCHIS F., Dizionario Giuridico. Inglese-Italiano, Giuffrè, Milano, 1984.

DE RUGGERIIS, Effetti delle innovazioni tecnologiche sul processo penale, in MAIOLI C., (a cura di), Questioni di Informatica forense, Aracne, Ariccia, 2015.

DELFINI F., Documento informatico, forma analogica e forma elettronica: dalla scrittura privata autenticata all'atto pubblico informatico, in FINOCCHIARO G., DELFINI F., (a cura di), Diritto dell'informatica, Utet, Milano, 2014.

DOMINIONI O., La prova penale scientifica, Giuffrè, Milano, 2005.

DONATO F., Indagini e acquisizione di dati probatori sulla scena del crimine. Protocolli operativi e utilizzabilità della prova: aspetti criminalistici , in Archivio penale, n. 2, 2012.

ESPOSITO G., Un PC per Sherlock Holmes, 2012, in *http://www.carabinieri.it/editoria/il-carabiniere/anno-2012/febbraio/scienza/un -pc-per-sherlock-holmes*.

F.B.I. HANDBOOK OF FORENSICS SERVICES, 1999, in *http://www.fbi.gov /hq/lab/handbook/forensics.pdf*.

FAGGIOLI, G., Computer Crimes, Edizioni Simone, Napoli, 1998.

FALLETTI E., E-Justice. Esperienze di diritto comparato, Giuffrè, Milano, 2008.

FERRAJOLI L., Diritto e ragione. Teoria del garantismo penale, Laterza, Bari, 1989.

FERRAZZANO M., Indagini forensi in tema di scambio di file pedopornografici mediante software di file sharing a mezzo peer-to-peer, Tesi di dottorato XXVI ciclo Università di Bologna. 2014, in http://amsdottorato.unibo.it/6697/.

FERRUA P., GRIFANTINI F. M., ILLUMINATI G., ORLANDI R., La prova nel dibattimento penale, Giappichelli, Torino, 2005.

FINOCCHIARO G., DELFINI F., (a cura di), Diritto dell'informatica, Utet Giuridica, Milano, 2014.

FOCARDI F., La consulenza tecnica extraperitale delle parti private, Cedam, Padova, 2003.

Forensic Examination of Digital Evidence: A guide for Law Enforcement, National Institute of Justice (NIJ), Washington D.C., 2004, in *https://www.ncjrs.gov/pdffiles1/nij/199408.pdf*.

FRATTALLONE S., La mera estrazione dei dati da un computer non è atto irripetibile, in *http://www.frattallone.it/penale/561-penale-la-mera-estrazione-dei-dati-da-un-computer-non-e-atto-irripetibile*.

FROSINI V., Cibernetica, diritto e società, Edizioni di comunità, Milano, 1968.

FROSINI V., Informatica diritto e società, Giuffrè, Milano, 1992.

FTI, Forum per la Tecnologia dell'Informazione, Osservatorio sulla criminalità informatica. Rapporto 1997, Franco Angeli, Milano, 1997.

GAI S., MONTESSORO P.L., NICOLETTI P., Reti Locali. Dal cablaggio all'internetworking, Scuola Superiore G. Reiss, L'Aquila, 1995.

GALDIERI P., Teoria e pratica nell'interpretazione del reato informatico, Giuffrè, Milano, 1997.

GALLARINI S., La realtà virtuale, Xenia Edizioni, Milano, 1994.

GAMMAROTA A., CACCAVELLA D. E., "L'Informatica forense per l'E-Healt", in FARALLI C., BRIGHI R., MARTONI M., (a cura di), Strumenti, diritti, regole e nuove relazioni di cura, Giappichelli, Torino, 2015.

GAMMAROTA A., Danneggiamento di sistema informatico della P.A. e informatica forense: un caso, in POZZI P., MASOTTI R., BOZZETTI M., (a cura di), Crimine virtuale, minaccia reale, Franco Angeli, Milano, 2004.

GAMMAROTA A., MAIOLI C., A steganography based proposal for the detection of hidden data, Convegno Internazionale RIS su Indagini in Internet, Roma, 2005, in *http://www.carabinieri.it/Internet/Arma/Oggi/Convegni/Roma 23052005/May+23/04_p.htm*.

GIANNANTONIO E., Manuale di diritto dell'informatica, Cedam, 1997.
GIUNCHEDI F., Le malpractices nella digital forensics. Quali conseguenze sull'inutilizzabilità del dato informatico? in Arch. Pen., 3, 2013, in *http://www.archiviopenale.it/apw/wp-content/uploads/2013/09/Confronto.Giunchedi.pdf*
GONZALEZ R. C., WOODS R. E., Digital Image Processing, III ed., Prentice Hall, 2008.
GRIFANTINI F. M., ILLUMINATI G., ORLANDI R., La prova nel dibattimento penale, Giappichelli, Torino, 2005.
GUBITOSA C., ASSOCIAZIONE PEACELINK, Italian crakdown, BBS amatoriali, volontari telematici, censure e sequestri nell'Italia degli anni '90, Apogeo, Milano, 1999.
HANCE O., Internet e la legge, McGraw-Hill, Milano, 1997.
HUEBNER E, ZANERO S., Open Source Software for Digital Forensics, Springer, New York, 2010.
IANULARDO M., Processo "Vierika", c'è la sentenza, Punto Informatico, Anno X, n. 2460.
IASILLO A., Agenti provocatori e sequestro probatorio. Male captum, (non) bene retentum? in D & G. Diritto e giustizia, n. 40/2004.
INDOVINA B., Accertamenti tecnici informatici: atti ripetibili o irripetibili, 2012, in *http://www.medialaws.eu/accertamenti-tecnici-informatici-atti-ripetibili-o-irripetibili/*.
INTERNATIONAL ORGANIZATION ON COMPUTER EVIDENCE (IOCE), G8 Proposed Principles For The Procedures Relating To Digital Evidence, 2002, in *http://www.ioce.org*.
JACOBELLI J. (a cura di), La realtà del virtuale, Editori Laterza, Bari, 1998.
JASANOFF S., La scienza davanti ai giudici, Giuffrè, Milano, 2001.
KRUSE II W. G., e HEISER J.G., Computer Forensics: Incident Response Essentials, Addison-Wesley, Boston, USA, 2002.
LARONGA A., Le prove atipiche nel processo penale, Cedam, Padova, 2002.
LOMBARDO V., VALLE A., Audio e multimedia, ed. 4. Apogeo, Milano, 2014.
LONGO G. O., VACCARO A., Bit Bang, La nascita della filosofia digitale, Maggioli, Santarcangelo di Romagna, 2013.
LORENZETTO E., Utilizzabilità dei dati informatici incorporati su computer in sequestro; dal contenitore al contenuto passando per la copia e in Dir. pen proc., 2009.
LOSANO M. G, La computer forensics e l'insegnamento dell'informatica giuridica in NERHOT P., (a cura di), "L'identità plurale della filosofia del diritto, Atti del XXVI Congresso della Società Italiana di Filosofia del Diritto" (Torino, 16-18 settembre 2008), ESI, Napoli, 2009.

LOSANO M., Informatica per le scienze sociali. Corso di informatica giuridica, Einaudi, Torino, 1985.
LUPARIA L., "Vierika": un'interessante pronuncia in materia di virus informatici e prova penale digitale. I Profili processuali, in Diritto dell'Internet, 2006, n. 2.
LUPARIA L., ZICCARDI G., Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali, Giuffrè, Milano, 2007.
LUPARIA, L., La ratifica della Convenzione Cybercrime del Consiglio d'Europa. I profili processuali, in Diritto penale e processo, n. 6, 2008.
MAIOLI C., (2002) Elementi di Informatica per l'Informatica Giuridica, Pioda, Roma, 2002.
MAIOLI C., CANESTRARI S., On the preparation of better law graduates and ICT jurist, in Eleventh International Conference on Substantive Technology in Legal Education and Practice, (atti del Convegno SubTech 2010, Saragozza, 1-3 luglio 2010) University of Zaragoza Press, Saragozza, 2010.
MAIOLI C., Dar voce alle prove: elementi di Informatica forense, in POZZI P., MASOTTI R., BOZZETTI M., (a cura di), Crimine virtuale, minaccia reale, Franco Angeli, Milano, 2004.
MAIOLI C., L'insegnamento dell'informatica giuridica: il contributo dell'Università di Bologna, in PERUGINELLI G., RAGONA M., (a cura di), L'informatica giuridica in Italia, Napoli, ESI, 2014.
MAIOLI C., ORTOLANI C., La cyber law non è la horse law. L'informatica giuridica nelle Facoltà di Giurisprudenza, Gedit, Bologna, 2007.
MALDONADO T., Reale e virtuale, Feltrinelli, Milano, 1998.
MANTOVANI F., Diritto Penale, Parte generale, Cedam, Padova, 1992.
MARCELLA A.J., GREENFIELD R.S., Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, USA, Auerbach, 2002.
MAZZA O., I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione, in Diritto Penale Contemporaneo, in *http://www.penalecontemporaneo.it/upload/1355813018-Mazza%20Milano.pdf*.
MENDOZA R., MARCON G., MARCON L., La perizia e la consulenza nel processo penale, Padova, Cedam, 1994.
MERCONE M., Diritto Processuale Penale, Simone, Napoli, 2001.
MIYAMACHI T., GRUBER M., DAVESNE M., BOWEN M., BOUKARI S., JOLY L., SCHEURER F., ROGEZ G., KAZU YAMADA T., OHRESSER P., BEAUREPAIRE E., WULFHEKE W., Robust spin crossover and memristance across a single molecule, 3/7/2012, in *http://www.nature.com/ncomms/journal/v3/n7/full/ncomms1940.html*.

MOFFA S., Verso il processo penale telematico, in MAIOLI C., (a cura di), Questioni di Informatica forense, Aracne, Ariccia, 2015.
MOSCARINI P., Principi delle prove penali, Giappichelli, Torino, 2014.
NAPPI A., Guida al Codice di Procedura Penale, Giuffrè, Milano, 2000.
NATIONAL INSTITUTE OF JUSTICE (NIJ), Electronic Crime Needs Assessment for State and Local Law Enforcement, Washington, D.C., 2001, in *https://www.ncjrs.gov/pdffiles1/nij/ 186276.pdf*.
NEGROPONTE, N., Essere digitali, Sperling e Kupfer, Milano, 1995.
NERI G., Criminologia e reati informatici. Profili di diritto penale dell'economia, Jovene, Napoli, 2014.
NESPOR S., Internet e la legge, Hoepli, Milano, 1999.
NICOSIA G., CACCAVELLA D.E., Macchine virtuali e sistema della prova nel processo civile e epenale, In Diritto dell'Internet, 2008.
NOBLETT M. G., POLLITT M.M., PRESLEY L.A., Recovering and Examining Computer Forensic Evidence, in Forensic Science Communications, 2000, Vol. 2 n. 4, in *https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2000/index.htm/com puter.htm*.
NOVARIO F., Le prove informatiche nel processo civile, Giappichelli, Torino, 2014.
PALERMO G. B., STRONARDI V., AGOSTINI S., Il processo investigativo e accusatorio negli Stati Uniti d'America e in Italia, in Rivista di Psichiatria, Supplemento, 2012, 47.
PARDOLESI R., voce Energia, in Digesto delle Discipline Privatistiche, sez. civ., vol VIII, Utet, Torino, 1991.
PATTARO E., (a cura di), Manuale di diritto dell'informatica e delle nuove tecnologie, Cedam, Padova, 2000.
PATTARO E., Diritto, scrittura, informatica, in PATTARO E., (a cura di), Manuale di diritto dell'informatica e delle nuove tecnologie, Cedam, Padova, 2000.
PECORELLA C., Il diritto penale dell'informatica, Cedam, Padova, 2000.
PERRI P., voce Computer forensics (indagini informatiche), in Digesto delle discipline penalistiche, UTET, Torino, 2011.
PICA G., Diritto penale delle tecnologie informatiche, Utet, Torino, 1999.
PICOTTI L., La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto sostanziale, in Diritto penale e processo, n. 6, 2008.
PICOTTI L., Reati informatici in Enciclopedia giuridica, Aggiornamento VIII, Istituto della Enciclopedia italiana, Roma, 2000.
PLATONE, La Repubblica, Libro VII, 514 – 520, in Volume II, BUR, Milano, 1981.
PUTIGNANO D. S., L'errore scientifico nel processo penale, Giuffrè, Milano, 2007.

RFC 3227 - Guidelines for Evidence Collection and Archiving, Internet Society, 2002, in *http://www.rfc-base.org/rfc-3227.html*.

RICCI A.E, Digital evidenze e irripetibilità delle operazioni acquisitive, in
Dir. pen. proc., 2010, 3.

RUGGIERI F., Profili processuali nelle indagini sui reati informatici, in PASCUZZI, G. (a cura di), Diritto e informatica, Giuffrè, Milano, 2002.

SARTOR, G. L'informatica giuridica e le tecnologie dell'informazione, Giappichelli, Torino, 2012.

SARZANA DI S. IPPOLITO, C., Informatica, Internet e diritto penale, Giuffrè, Milano, 2003.

SCARDINO P., Nota a Sentenza Trib. Penale di Bologna, I Sez. Giudice Monocratico, Sent. 21.07.05 in *http://www.computerlaw.it/entry.asp?ENTRY_ID=176*.

SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE (SWEDGE), International Organization on Digital Evidence (IOCE), Proposed Standards for the Exchange of Digital Evidence, 1999, in Forensic Science Communications, 2000, Vol. 2 n. 2, in *https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/*.

SERRA C., STRANO M., Nuove frontiere della criminalità – La criminalità tecnologica, Giuffrè Editore, Milano, 1997.

SIRACUSANO D., Prova, in Enc. Giur. Treccani, XXIV, Roma, 1991.

SOI, G., Tracce informatiche, in Polizia Moderna, novembre 2010.

SOLA L., FONDAROLI D., A proposito della criminalità informatica, Editrice CLUEB, Bologna, 1992.

SOLA L., FONDAROLI D., La nuova normativa in tema di criminalità informatica: alcune riflessioni, Editrice CLUEB, Bologna, 1993.

SPECCHIO G., Attività Investigativa in Internet, in *http://www.carabinieri.it/editoriarassegna-dell-arma/anno-2012/n-1---gennaio-marzo/studi/attivit% C3 %A0-investigativa-in-internet*.

SPECCHIO G., Il nuovo mezzo di «prova digitale», 2015, in *http://thinkinginforensics.net/2015/05/il-nuovo-mezzo-di-prova-digitale/#more-1624*.

STELLA F., Il giudice corpuscolariano. La cultura delle prove, Giuffrè, Milano, 2005

STRANO M., Computer crime, Apogeo, Milano, 2000.

TADDEI ELMI G., Corso di informatica giuridica, Simone, Napoli, 2003.

TANENBAUM A. S., AUSTIN T., Structured Computer Organization, VI ed., Pearson, Milano, 2013, p. 74.

TARUFFO M., La prova dei fatti giuridici, Giuffrè, Milano, 1992.

TECHNICAL WORKING GROUP FOR ELECTRONIC CRIME SCENE INVESTIGATION (TWGECSI), Electronic Crime Scene Investigation: A

guide for First Responders, National Institute of Justice (NIJ), Washington D.C., 2001, in *https://www.ncjrs. gov/pdffiles1/nij/187736.pdf*.

TESTAGUZZA M., I Sistemi di Controllo Remoto: fra normativa e prassi, in Dir. pen. proc., 2014.

TONINI P. (a cura di) La prova scientifica nel processo penale, Dossier di Diritto e processo penale, Milano, 2008.

TONINI P., CONTI C., Il diritto delle prove penali, II ed., Giuffrè, Milano, 2014.

TONINI P., Documento informatico e giusto processo, in "Diritto penale e processo", 2009.

TONINI P., La prova penale, Cedam, Padova, 2000.

TORRE M., Il virus di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali, in Dir. pen. proc., 2015.

UBERTIS G., La prova penale. Profili giuridici ed epistemologici. Utet, Torino, 1995.

UNITED STATES DEPARTMENT OF JUSTICE, Searching and Seizing Computers ad Otaining Electronic Evidence in Criminal Investigations, 2002, in *http://www.finer-bering.com/ GULAW_PDFs/s&smanual2002.pdf*.

USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001), in *https://www. gpo.gov/fdsys/ pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf*.

VACCA J. R., Computer Forensics – Computer Crime Scene Investigation, Charles River Media, Hingham, Massachusetts, 2002.

VACIAGO G., Digital Evidence, Giappichelli, Torino, 2012.

VETTORI, G., Reati connessi a Internet: profili processuali penali e tutela dell'indagato, in GAUDENZI SIROTTI, A., (a cura di), Internet e diritto. Problemi e soluzioni, Gedit, Bologna, 2001.

VILLECCO BETTELLI A., Appunti sul nuovo processo tecnologico, in CEVENINI C., DI COCCO C., SARTOR G., Lezioni di informatica giuridica, Gedit, Bologna, 2005.

VILLECCO BETTELLI A., L'efficacia delle prove informatiche, Giuffrè, Milano, 2004.

ZAN S., (a cura di), Tecnologia, Organizzazione e Giustizia. L'evoluzione del Processo Civile Telematico, Il Mulino, Bologna, 2004.