LA FRAGILITA' DELLA PROVA INFORMATICA: CARATTERISTICHE GENERALI E PROBLEMATICHE EMERGENTI

1 LA CENTRALITÀ DELLA PROVA INFORMATICA NEL NUOVO CONTESTO ICT

L'evoluzione tecnologica, in particolare quella telematica, ha cambiato profondamente e radicalmente la società odierna. Il settore delle comunicazioni è stato profondamente rivoluzionato: le forme tradizionali di comunicazione hanno lasciato spazio a forme d'interazione completamente nuove e impensabili in cui gli uomini interagiscono e arricchiscono le proprie conoscenze attraverso l'utilizzo di dispositivi capaci di comunicare con loro e fra di loro. Il nuovo millennio ha consolidato quella che è stata definita tempo prima come « rivoluzione digitale", in particolare ha permesso alla nuova società dell'informazione di imporsi in quasi tutti i contesti economici e sociali. Uno dei fattori determinanti di tale cambiamento è sicuramente rappresentato dall'approdo di Internet nella società: l'accessibilità universale al sapere comune ha in un primo momento permesso la diffusione e lo scambio di un'enorme quantità di dati e informazioni, per essere, ad oggi, sempre più perfezionati e raffinati attraverso l'evoluzione del cd semantic web. In sostanza, la moderna società è retta e si sviluppa ormai sul paradigma costituito dal settore ICT (Information and Communication Technology): se da un lato, i nuovi strumenti tecnologici hanno portato e portano tuttora indubbi vantaggi alla comunità, dall'altro si è costatato come i nuovi scenari virtuali abbiano portato allo sviluppo di un «lato oscuro del progresso».

Ci si riferisce, in particolare, a quelle condotte devianti che hanno fin da subito riconosciuto le potenzialità legate ai computer e alla rete, vedendo negli stessi un terreno fertile nel quale dare vita a nuove attività illecite. Lo strumento informatico o telematico è diventato ben presto bersaglio della cd cybercriminalità la quale sostanzialmente ha sviluppato due differenti modalità operative di aggressione: la prima, dove l'azione delittuosa ha come fine quello di aggredire e compromettere sistemi informatici o telematici; la seconda, invece, che riconosce nei nuovi mezzi un veicolo attraverso il quale perpetrare, mediante modalità proprie dell'ambiente virtuale, condotte afferenti a reati tradizionali propri del "mondo fisico". Le diverse istanze di legalità e di tutela, derivanti sia dall'ambito nazionale che internazionale, hanno palesato la necessità per il legislatore di adoperarsi ai fini dell'individuazione di nuovi beni giuridici da proteggere nonché la predisposizione di misure idonee ai fini della individuazione e persecuzione dell'autore della condotta criminosa, portandolo a confrontarsi più volte con la materia informatica e le problematiche ad essa affini.

Una prima tappa fondamentale è rappresentata dalla legge n°543 del 1993 nella quale il legislatore «ha delineato implicitamente le caratteristiche dell'illecito informatico: esso è un reato plurioffensivo che aggredisce la libertà di comunicazione e di manifestazione del pensiero (artt. 15 e 21 Cost.) e, nel contempo, il patrimonio della persona offesa»[1]. Da una generale visione delle norme introdotte dal legislatore del '93 traspare la polivalenza dello strumento informatico che assume talora oggetto materiale del reato (ad esempio nei reati di intrusione come l'accesso abusivo a un sistema informatico, di danneggiamento, di frode informatica) ovvero cosa pertinente al reato in quanto strumento ed elemento consumativo della condotta (ad esempio nella diffamazione on-line). Dal punto di vista dei sostanzialisti, però, l'impianto dettato dalla legge mancava di organicità, insufficiente ai fini della nascita di un "diritto penale dell'informatica", il quale «non è stato concepito in base ad un'idea costitutiva, ma è stato costruito attraverso l'accorpamento di materiali diversi, senza la morfologia di un organismo corrispondente a un modello, vale a dire senza un disegno unitario e senza sistematicità» [2] . L'intervento, coerentemente, non si è limitato alle sole questioni sostanziali introducendo al nuovo art. 266-bis la disciplina in tema di intercettazioni di comunicazioni informatiche e telematiche, con il fine di dotare gli inquirenti di strumenti processuali idonei al perseguimento dei "nuovi" reati informatici. Sfortunatamente gli anni a seguire sono connotati da un forte crescendo della criminalità informatica, la quale da qualche tempo veniva monitorata soprattutto a livello internazionale. Infatti, già dal 1996 con la decisione dell' European Commitee on Crime Problems (CDPC) si fece largo la necessità di istituire una commissione di esperti per analizzare il fenomeno del cybercrime al fine di intervenire repentinamente in quanto «only a binding international instrument can ensure the necessary efficiency in the fight against these new phenomena»[3]. Il prodotto del lungo percorso negli anni successivi fu quello della Convention on Cybercrime, firmata a Budapest il 23 novembre 2001. Tre sostanzialmente sono gli obiettivi perseguiti dal Consiglio d'Europa: 1) armonizzare il diritto sostanziale penale nell'ottica del nuovo fenomeno del cybercrime; 2) rafforzare il sistema processuale interno in un'ottica sia investigativa sia repressiva con riguardo al perseguimento di tali reati, nonché con riguardo ai reati commessi attraverso l'utilizzo di strumenti informatici o reati le cui prove vengano ad essere formate attraverso procedure elettroniche; 3) l'istituzione di un sistema di cooperazione internazionale che sia efficiente, efficace e rapido. Il legislatore italiano, con la legge n°48 del 2008 ha dato seguito alla ratifica della Convenzione: a differenza di quanto accadde in passato però, la novella legislativa del 2008 si è concentrata perlopiù sugli aspetti processuali del tema, segno dell'ormai forte incidenza rappresentata dal dato informatico, il quale non è più mero elemento da proteggere ma sempre più preziosa risorsa a fini investigativi e processuali. In ambito sostanziale, infatti, le modifiche introdotte dalla legge n°48 non appaiono in

---

[1] G. BRAGÒ, Le indagini informatiche fra esigenze di accertamento e garanzie di difesa, in *Diritto dell'informatica* n°3, 2005, pag. 518.

[2] F. FULVI, La Convenzione cybercrime e l'unificazione del diritto penale dell'informatica in *Dir Pen e Proc*, n°5, 2009, pag. 639

[3] Explanatory report ETS n°185, disponibile al sito http://www.conventions.coe.int/Treaty/en/Reports/Html/185.htm .

realtà in linea con i precetti internazionali, anzi, rispondono «piuttosto ad autonome scelte del nostro legislatore, che ha colto l'occasione (…) per rivedere alcune parti controverse della disciplina vigente in materia»[4].

Un cambiamento importante si è avuto il tema di responsabilità amministrativa degli enti, attraverso il nuovo art. 24 bis del dlgs. n°231 del 2001. Come noto il decreto 231 disciplina le ipotesi di responsabilità degli enti per i reati posti in essere da soggetti in posizione apicale o dipendente nell'interesse o a vantaggio dell'ente stesso, e che in origine era limitata ai soli reati contro la Pubblica Amministrazione. Ne è seguita una progressiva espansione su più fronti[5] fino all'odierna estensione alle più importanti fattispecie delittuose legate alla criminalità informatica (art. 7, l. n°48/2008). Un dato sorprende: la legge prevede, infatti, che, indipendentemente dal fatto che l'ente si sia dotato di adeguati sistemi di organizzazione, possa essere comunque ritenuto responsabile per il reato informatico di cui non si è riuscito a identificare l'autore materiale. [6] Ciò comporta che i cd modelli 231[7] dovranno necessariamente prevedere un'attenta analisi dell'intera architettura dei sistemi informativi e informatici in uso, prevedendo ad esempio particolari procedure d'accesso, security policies che risultino già ex ante idonee all'eliminazione del rischio alla commissione di reati informatici. Per beneficiare dell'esimente, infatti, l'ente dovrà porre in essere una strategia che prevenga in generale la commissione di reati informatici al suo interno ma, altresì, sia idonea ad escludere la propria responsabilità nelle ipotesi in cui le misure adottate, idonee sul piano pratico, non siano state in grado di evitare la commissione del reato.

Con la legge n°48 il legislatore chiude un cerchio delineando un sistema che appresta non solo un'idonea tutela sostanziale ma altresì dota l'intero sistema processuale di strumenti atti all'acquisizione e valutazione della nascente disciplina sulla prova informatica. Ecco quindi che si fa strada sul punto il concetto digital evidence, come risultato di attività d'indagine volta sia all'identificazione dell'autore di crimini informatici, sia all'identificazione dell'autore di reati comuni, commessi col mezzo informatico e non, mediante l'impiego di procedure informatiche proprie della digital investigation. L'ambito di applicazione del nuovo sistema, infatti, si spinge oltre il terreno del cybercrime, aprendosi a qualsiasi tipologia di reato per cui si proceda, in perfetta aderenza sul punto con il dettato internazionale della Convenzione[8], generando quindi un incremento nella domanda d'analisi del dato digitale per fini di giustizia.

Se da un lato tale nuovo assetto deve essere salutato con favore avendo il merito di creare un'architettura sulla quale far riferimento, dall'altro il ritardo con il quale viene ad essere affrontato il fenomeno e la forte importanza che tende ad assumere nell'attuale panorama del diritto alle prove ha portato alcuni autori, estremizzando, a sostenere «se abbia ancora senso parlare della prova orale in termini di chiave di volta del processo accusatorio, allorché sempre più giudizi paiono fondarsi su evidenze scientifiche formatesi nella prima fase del procedimento e che, veicolate nella scansione dibattimentale, riducono il "contraddittorio per la prova" ad un mero esercizio di dialettica su materiali non facilmente decifrabili e già "preconfezionati" in sede di indagini preliminari»[9]. Da un'altra prospettiva si è avvertito il rischio verso una deriva tecnicista, soprattutto in merito a temi quali "libero convincimento del giudice" e "centralità dell'organo giudicante" a seguito del sempre più frequente ricorso a esperti in ragione della maggior specializzazione delle conoscenze scientifiche interessate che entrano in gioco nelle dinamiche processuali. È necessario quindi riuscire a ricondurre la tecnica informatico-investigativa entro i paradigmi e le maglie del processo penale. Un passo avanti rispetto al passato sicuramente è stato fatto, attraverso il ripudio alla concezione di "autonomia sistematica" delle operazioni di digital investigation, ritenute un tempo avulse rispetto all'intero corpus normativo, operando al limite della delega in bianco a favore dei tecnici, nonché un ripensamento in ordine alla qualificazione della prova informatica come prova assoluta. Sul punto il paradigma delle garanzie costituzionali e processuali ben rappresenta la luce verso cui tendere per uscire da dette oscurità, anzi com'è stato sostenuto «il più delle volte, i principi consolidati della teoria processuale possono essere sufficienti per risolvere le questioni connesse al nuovo fenomeno delle indagini informatiche e che, anzi, l'eccessivo scostamento dallo ius commune iudiciale (...) finisce col provocare pericolosi scostamenti tecnicisti e fenomeni di aggiramento delle garanzie processuali»[10].

2 CARATTERISTICHE: IMMATERIALITÀ E FRAGILITÀ DEI DATI INFORMATICI

Per il giurista adattare il tradizionale mondo giuridico alla realtà virtuale non è operazione di per sé agevole: riflettere sul concetto di prova informatica lo è ancora di più, soprattutto da un punto di vista processuale, poiché da sempre il processo penale vive di elementi materiali rappresentati da oggetti fisici il cui tratto decisivo è rappresentato dalla loro concretezza. Il reperto fisico può essere toccato con mano, studiato, confrontato, analizzato nelle sue componenti per risalire ad esempio, al soggetto che lo ha utilizzato mediante l'analisi del dna, delle impronte o delle tracce biologiche ivi rinvenute.

---

[4] L.PICOTTI, Ratifica della Convenzione di Budapest e nuovi strumenti di contrasto contro la criminalità informatica e non solo, in *Diritto dell'Internet*, n°5, 2008, pag. 437.

[5] A titolo d'esempio sono estesi: falsi nummari, reati societari (sanzioni raddoppiate nel 2005), delitti in materia di terrorismo ed eversione, delitti contro la personalità individuale, abusi di mercato, cd reati transnazionali, delitti di omicidio colposo da violazione norme antifortunistiche/sicurezza sul lavoro, delitti ricettazione, riciclaggio.

[6] La scelta di introdurre tale estensione è stata imposta da un lato dagli artt 12 e 13 della Convenzione sul Cybercrime, dall'altro dall'art. 9 della decisione quadro 2005/222/GAI che ne ha completato l'aspetto punitivo.

[7] Assimilabili per certi aspetti al Documento Programmatico sulla Sicurezza prescritto come misura minima di sicurezza dall'allegato B del Codice della Privacy.

[8] Così l'art. 14 Convenzione di Budapest: «(…) each Party shall apply the powers and procedures reffed 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; c) the collection of evidence in electronic form of a criminal offence».

[9] LUPÀRIA, ZICCARDI, *Investigazione penale e tecnologia informatica. L'accertamento del reato fra progresso scientifico e garanzie fondamentali*, Giuffrè Editore 2007, pag. 128.

[10] LUPÀRIA, ZICCARDI *Investigazione penale e tecnologia informatica*, Giuffrè Editore 2007 pag. 136.

La prova informatica, di contro, possiede in re ipsa la caratteristica dell'immaterialità: ciò ovviamente non implica che sia in sé assente la componente fisica. Anzi, gli elementi costitutivi della prova sono, in via approssimativa, impulsi elettrici che rispondono a una sequenza prestabilita di bit (0;1 cd linguaggio macchina) che a seguito di codifica vengono ad essere rappresentati in un linguaggio comprensibile all'uomo per essere poi, eventualmente, incorporati all'interno di supporti magnetici (cd-rom, hard-disk, memorie esterne). Ciò che crea il distacco dalla fisicità è l'indipendenza del dato rispetto al supporto che lo contiene: ai fini della fruibilità delle informazioni in esso contenute rileva infatti la rappresentazione, come operazione di elaborazione che dal linguaggio macchina rende l'informazione intellegibile che risulta, appunto, indipendente. Tale aspetto si lega ulteriormente alla possibilità di riprodurre anche infinite volte lo stesso dato senza che ciò ne pregiudichi la qualità della rappresentazione, sfumando fino quasi all'eliminazione la distinzione fra copia e originale. Per non parlare poi della paternità, anch'esso aspetto controverso, giacché in via di massima un dato di per sé nulla dice rispetto il soggetto che l'ha generato[11], ma solo al più quando e come è stato creato. Ulteriore differenza rispetto al reperto materiale, è dato dalla sua fragilità. Il dato informatico, infatti, per quanto possa portare con sé un alone di vischiosità (cd stickiness), è comunque caratterizzato da fragilità stante l'alto rischio di alterazione tipico dell'ambiente virtuale. Tale aspetto rileva non solo, come vedremo in seguito, in sede di corretta acquisizione del dato, ma anche e soprattutto in sede di conservazione, considerato l'alto rischio di dispersione della prova rappresentato ad esempio, dalla possibile smagnetizzazione delle memorie.

Per quel che concerne la nostra trattazione, è importante far notare fin da subito come l'ausilio della scienza informatica applicata al processo possa condurre essenzialmente due risultati differenti. È opportuno, infatti, operare un distinguo interno alle digital evidence fra la cd computer generated evidence e la cd computer derived evidence. La prima ha come scopo principale la rappresentazione dell'accadimento di fatti oggetto d'accertamento attraverso l'elaborazione informatica mediante software, concretandosi quindi in una rappresentazione virtuale (si pensi ad esempio ad animazioni, simulazioni o ricostruzioni). La seconda, invece, ha a oggetto l'elaborazione di dati contenuti all'interno di dispositivi, strumenti o componenti informatiche costituendo, quindi, prove dirette o indirette legate a elementi costitutivi della regiudicanda. Possono, infatti, assumere il differente ruolo di "corpo del reato" ad esempio, in caso di accesso abusivo a un sistema informatico, nella pedopornografia come materiale illegittimamente detenuto, ovvero di dati rilevanti e pertinenti a ricostruire le attività compiute dal dispositivo come ad esempio nella ricostruzione dei cd alibi informatici. Ed è su questa seconda categoria che questo lavoro si concentrerà nel prosieguo.

Le considerazioni fin qui fatte devono, tuttavia, essere confrontate con il dato normativo che, soprattutto in tema di documento informatico, ha creato non poche difficoltà interpretative in passato. La novella del 2008 ha previsto, in primis, la soppressione del secondo periodo del comma 1° dell'art 491 bis, contenente la definizione di documento informatico introdotta con la legge n° 547/93. Il legislatore del tempo aveva seguito, in mancanza di definizioni a livello civile o amministrativo, un criterio fortemente tradizionalista, ancorato alla tipica definizione di "documento" legata al supporto cartaceo e che nella nuova veste veniva ad essere definito, in sostanza, come supporto che contiene dati[12]. La limitatezza di tale definizione è evidente, la quale non tiene per nulla in considerazione, come abbiamo visto prima, quelle che sono le caratteristiche fondamentali del documento informatico: da un lato, la fragilità dei dati in esso contenuti, dall'altro la facilità di alterazione e corruttibilità del contenuto stante l'impossibilità materiale di distinguere fra copia e originale. La giurisprudenza sul punto si è mostrata ancora più retrograda rispetto al legislatore del '93, affermando in più occasioni come «la definizione non avrebbe carattere innovativo o costitutivo, ma solo interpretativo od esplicativo dell'estensione (…) della nozione unitaria di documento»[13], sottolineando come la modalità informatica di rappresentazione dei fatti debba essere considerata più una species della tradizione, che una categoria nuova e a sé stante. Da un punto di vista penalistico tale impostazione risulta altresì carente con riguardo all'effettività della tutela: anziché privilegiare il dato in esso contenuto, si concentra sul supporto, il quale risulta irrilevante in quanto il dato digitale, al di là dei limiti imposti dal particolare formato con il quale è salvato, potrà essere sempre riprodotto e reso intellegibile attraverso l'utilizzo di programmi atti all'elaborazione, indipendentemente quindi dal contenitore. In seguito il legislatore sembra ripensarci, introducendo una nuova nozione di documento informatico all'interno della normativa contenuta nel Codice dell'Amministrazione digitale del 2005, in cui in sostanza rovescia la definizione precedente definendolo come «rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti»[14]. Ad oggi, quindi, a seguito della modifica introdotta dalla legge n°48/2008 si ha un rimando alla norma extrapenale contenuta nel Codice dell'Amministrazione Digitale (C.A.D.) , la quale si caratterizza per la presenza di elementi definitori per così dire elastici, rinviando da un lato, all'evoluzione informatica il concetto di rappresentazione, dall'altro, alle fonti giuridiche in tema di rilevanza dei contenuti oggetto della rappresentazione stessa. Sempre all'interno del C.A.D. si prevede, attraverso la disciplina sulle firme

[11] Si veda la distinzione fra dato generato dall'uomo al cui interno si distingue fra interazione *human to human* (es *e-mail*) e *human to pc* (es. creazione di un *file* di videoscrittura); dato generato dal sistema informatico (es *file system*, utilizzo di *software antivirus*); dati generati da relazioni reciproche fra uomo e macchina (es. analisi di dati mediante l'impiego di fogli di calcolo come *Excel*).

[12] Art. 491-bis Documenti informatici. Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende *qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli*.

[13] L.PICOTTI, Ratifica alla Convenzione cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo, in *Diritto dell'internet*, n°5, 2008, pag. 439.

[14] Art. 1, comma 1, lett p del dlgs n°82/2005 Ai fini del presente codice si intende per (….) *p)* documento informatico: *la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.*

elettroniche, un sistema atto a garantire la paternità dei documenti informatici, fissando i requisiti di autenticità e genuinità essenziali per una completa disciplina della materia che possa soddisfare anche l'ambito processuale. In particolare, si prevede che il documento informatico se non è sottoscritto con firma elettronica (art. 1 lett q) non può avere alcuna efficacia probatoria, ma, al limite e secondo discrezione del giudice, integrare il requisito della forma scritta (art. 20, comma 1-bis) o ancora, ancorché firmato con firma elettronica semplice, rectius non qualificata, potrà conferirsi efficacia probatoria solo se potranno essergli ricondotti i requisiti oggettivi di qualità, sicurezza, integrità ed immodificabilità dal parte del giudice. In linea con tale impostazione, il legislatore del 2008 con la legge n°48 va oltre le prescrizioni internazionali imposte dalla Convenzione di Budapest, mostrando una forte attenzione al problema della circolazione di documenti informatici, in particolare l'aspetto legato alla certezza e alla paternità, introducendo ex artt 3 e 5 della legge n°48 due fattispecie delittuose connesse al sistema di certificazione delle firme elettroniche. Da un lato viene inserito l'art 495 bis c.p. prevedendo il nuovo delitto di «falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o qualità personali proprie o di altri», reato comune realizzabile da chiunque rilasci dichiarazioni o attestazioni false ideologicamente (ossia non veritiere) o materialmente (ossia non genuine) stante la necessità ai fini della generazione della firma, di accertare all'interno del certificato qualificato «gli elementi identificativi del titolare» e del certificatore, nonché eventuali limitazioni all'uso della stessa (art. 24, comma 4, C.A.D.) Dall'altro viene a essere collocato fra i delitti contro il patrimonio mediante frode, il nuovo art. 640 quinquies c.p. il quale prevede una particolare forma di frode informatica del «soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato». Sul punto si è obiettato come tale previsione risulti inadeguata e imprecisa, per certi aspetti volta alla moltiplicazione delle fattispecie incriminatrici. La relazione di accompagnamento alla legge n°2807 giustifica la creazione di tale fattispecie giacché la semplice frode informatica (art. 640 ter c.p.) non sarebbe stata in grado di coprire la condotta delittuosa del certificatore, difficilmente riconducibile alle condotte di alterazione o intervento senza diritto ivi previste. Tale necessità tuttavia non giustifica la creazione, denominazione e collocazione di tale nuovo delitto all'interno della più ampia categoria della truffa, tenuto conto altresì che «la nuova fattispecie legale è priva di qualsivoglia requisito di "fraudolenza", riducendosi alla mera violazione di obblighi di fonte extrapenale, senza neppure che sia richiesto un qualsivoglia elemento consumativo di lesione patrimoniale»[15] portato avanti dal certificatore "qualificato".

Al di là di questi particolarismi sostanziali, ad oggi nessuno più dubita dell'esistenza della prova digitale indipendentemente dal supporto che la contiene, il quale processualmente parlando assume ormai completa irrilevanza. È bene fin da subito sottolineare uno dei limiti di cui soffre la prova informatica e che, nella prassi, spesso non è stato considerato o comunque tralasciato. Ci si riferisce in particolare a una sorta di "mito da sfatare" sulle potenzialità dimostrative della prova informatica. Si pensi ad esempio una ricostruzione condotta attraverso l'analisi di dati contenuti all'interno di un computer: ciò che gli inquirenti potranno certamente stabilire è la concreta modalità con cui si è sviluppata la condotta criminosa, per ipotesi accesso abusivo ad un sistema informatico, e da quale dispositivo è stata originata. Diversamente non vi sarà certezza sull'autore materiale dell'illecito che resta celato dietro lo schermo stante la facilità ad esempio di duplicazione o rottura delle credenziali d'accesso se non opportunamente mantenute, l'incerta paternità dei dispositivi riconducibili per presunzione ai proprietari o a chi ne abbia, di fatto, la materiale disponibilità. Tali considerazioni portano a sostenere come di per sé la prova informatica difficilmente potrà condurre da sola a costruire un impianto probatorio che possa reggere di fronte al paradigma della «colpevolezza al di là di ogni ragionevole dubbio» (art 533 c.p.p.). Si rende quindi necessaria una simbiosi fra investigazione tradizionale e investigazione 2.0 affinché le due attività possano completarsi vicendevolmente.

3 UN ASPETTO CONTROVERSO: LA NATURA SCIENTIFICA DELLA PROVA

Le problematiche legate all'utilizzo della prova informatica in campo penale possono essere ricondotte in parte al dibattito sull'utilizzo della prova scientifica a livello processuale, che negli ultimi tempi ha vissuto un nuovo vigore legato alle moderne tecniche d'analisi impiegate su vari fronti. Da tempo, infatti, la scienza ha fatto un ingresso pressoché costante, in taluni casi anche prepotente, all'interno delle dinamiche processuali generando effetti differenti a seconda dell'angolo di visuale con cui si guarda il fenomeno. Se da un lato l'apporto della scienza risulta oggi necessario nel quotidiano svolgersi delle attività investigative e di accertamento, dall'altro molte sono le obiezioni e le criticità che emergono in sede attuativa circa i metodi e le tecniche seguiti, non sempre perfettamente coesi alla disciplina processuale vigente.

Il tema quindi può essere in primo luogo analizzato con riguardo alla cd prova penale scientifica, come particolare tipologia probatoria la cui caratteristica essenziale risiede nel momento acquisitivo caratterizzato dall'ausilio di conoscenze e metodologie attinenti al sapere scientifico e tecnico[16]. In primis è essenziale cogliere le peculiarità della prova scientifica ma al tempo stesso è necessario operare una distinzione fra le tradizionali prove scientifiche e le cd prove scientifiche "nuove" caratterizzate a loro volta da un alto contenuto tecnologico per gli strumenti ad elevata specializzazione che richiedono in sede d'acquisizione. Delle prime molto si è scritto contribuendo quindi alla consolidazione di linee di tendenza e prassi condivise (si pensi ad esempio alle modalità di rilevazione di impronte digitali) di contro delle nuove molto si discute, soprattutto con riguardo ai protocolli extragiuridici (ossia la scienza

[15] L.PICOTTI, Ratifica della Convenzione cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo, in *Diritto dell'internet*, n°5, 2008, pag. 341.

[16] O. DOMINIONI, *La prova penale scientifica*, Giuffrè, Milano, 2005.

ma soprattutto il grado di scientificità che ne sta alla base) arrivando spesso a metterne in discussione l'applicabilità e la loro validità. È la cd Novel Science ad alimentare le questioni che impegnano la giurisprudenza e la letteratura, prima fra tutti quella statunitense, in cui la prova scientifica è da tempo oggetto di studio. Il quadro del problema, si complica ulteriormente, coinvolgendo da un lato le questioni attinenti all'epistemologia giudiziaria, e dall'altro le questioni squisitamente processualistiche volte al connubio fra nuova scienza e paradigma legale sull'acquisizione della prova; in altri termini come coniugare epistemologia giudiziaria al "diritto alle prove"[17].

La prima dottrina in tema di prova scientifica è tutt'altro che risalente potendo essere preso come punto di riferimento il saggio ad opera di V. Denti «Scientificità della prova e libera valutazione del giudice» del 1972. L'Autore afferma che «i metodi scientifici non possono offrire nuove categorie di prove, ma possono servire a una migliore ricerca della verità», sottolineando i problemi fra scienza e processo soprattutto con riguardo alla classificazione della cd prova scientifica.[18] Si può osservare come la scientificità della prova deve essere valutata non con riguardo ai singoli mezzi di prova (documento, testimonianza) che di per sé sono neutri, nel senso che non hanno in re ipsa elementi di scientificità o ascientificità, ma piuttosto con riguardo al risultato della prova, come percorso valutativo della stessa a cui il giudice perviene accertando l'esistenza o meno del factum probandum. Possiamo quindi definire scientifica la prova « (…) che partendo da un fatto dimostrato, utilizza una legge scientifica per accertare l'esistenza di un'ulteriore fatto da provare. Poiché il rapporto fra fatto noto e quello da provare è espresso da una regola, la prova scientifica
rientra nella più vasta categoria della prova critica o indizio»[19]. La dottrina tradizionale, infatti, è concorde nella distinzione da operarsi all'interno del generale concetto di "prova" fra prove dirette, ossia quelle prove che mettono direttamente di fronte al giudice il fatto da provare, rispetto alle prove indirette, ossia fatti collegati al fatto principale in maniera indiretta rendendosi necessaria un'operazione di tipo induttivo fondata su regole logiche o massime d'esperienza da parte del giudice. Altra classificazione attiene alle prove storiche o rappresentative, in cui il fatto da provare è immediatamente riprodotto di fronte al giudice, e, prove critiche o non rappresentative, in cui risulta necessaria un'inferenza del giudice. Si noti come le due classificazioni non siano convergenti, ma si basino piuttosto su differenti criteri distintivi: nella prima il discrimine è dato dal riferimento diretto o indiretto al thema probandum, mentre nella seconda il riferimento è al processo logico seguito dal giudice a seguito del quale si perviene al risultato probatorio. Le distinzioni menzionate non hanno funzione meramente dottrinale, anzi, ci aiutano ad approfondire le metodiche di ragionamento giudiziale.

L'accertamento del fatto a rilevanza penale cui tende la celebrazione del processo, avviene in un momento successivo all'accadimento del fatto stesso: la ricerca è tesa all'accertamento della "verità processuale", come ricostruzione giudiziale del fatto comprovata da una serie di elementi e di prove che hanno basato e condotto il convincimento giudiziale verso un dato risultato. Da qui il parallelismo fra attività ricostruttiva di fenomeni passati operata dallo storico e attività ricostruttiva del fatto da parte del giudice. Lo storico tende a ricostruire un fatto accaduto nel passato, di per sé non ripetibile, in cui fondamentali sono le tracce e le testimonianze degli uomini: gli strumenti quindi consistono in prove rappresentative (testimone oculare, documento o filmato) e prove indiziarie (le tracce presenti). Sì è affermato, tuttavia, come l'attività del giudice, non si limiti all'attività storica ma possa estendere l'ambito d'indagine anche al sapere scientifico, adottando quindi metodologie simili a quelle dello scienziato. Tuttavia nel proprio agire il giudice non è libero ma vincolato dalla legge: accoglierà le due metodiche nei limiti impostogli dal diritto perché dovrà sempre permettere la verifica di affidabilità e attendibilità del metodo seguito. Senza volersi addentrare nelle tematiche attinenti il ragionamento giudiziale, è comunque opportuno accennare al bagaglio di conoscenze impiegate dal giudice in sede di valutazione di tali elementi. Tradizionalmente[20] si è soliti far riferimento al "sapere comune" come bagaglio di conoscenze attinenti alla "cultura dell'uomo medio": ove l'analisi riguardi aspetti attinenti a tale conoscenza il giudice è in possesso di strumenti di controllo, fuori da tale confine si ritiene necessario l'apporto di esperti. Tuttavia nell'odierna prassi giudiziaria non tutto ciò che va oltre la conoscenza dell'uomo medio necessariamente viene a essere provato o comporti l'ausilio della prova per esperto. Ciò in forza del fatto che il parametro di conoscenza non è da rapportarsi al solo giudice ma anche alle parti, ed è su tali soggetti che l'analisi deve concentrarsi. Si passa quindi ad un concetto di "sapere comune endoprocessualizzato", come cultura istituzionale richiesta al giudice e alle parti nell'esercizio della loro attività professionale nel contesto processuale. È strumento che veicola in maniera diretta il principio ex art. 111 Cost. della formazione in contraddittorio dapprima "per la prova" e poi "sulla prova". La realtà processuale in ogni caso ci insegna come tale conoscenza, nonostante gli aggiornamenti degli operatori non sia del tutto sufficiente a fronteggiare le sfide poste dalla prova scientifica, specie se "nuova". A riprova di tale possibilità il codice prevede strumenti giuridici ad hoc come la perizia ex art. 220 c.p.p. cui giudice, e, specularmente per le altre parti processuali con le figure della consulenza tecnica ex art. 225 c.p.p., possono avvalersi di figure specializzate permettendo l'adozione di metodi e tecniche basate su principi scientifici durante le operazioni probatorie a seconda dei compiti che possono essergli assegnati («La perizia è ammessa quando occorre svolgere indagini o acquisire dati o valutazioni che richiedono specifiche competenze tecniche, scientifiche, artistiche. » art. 220, 1°c c.p.p.). L'esperto, quindi, integra il patrimonio di conoscenze del

[17] O. DOMINIONI, *La prova penale scientifica*, Giuffrè, Milano, 2005, pag. 12.
[18] G. MARANDO, *L'acquisizione della prova penale scientifica*, Tesi dottorato a.a. 2009-2010, Università di
Trieste.
[19] P. TONINI. La prova scientifica: considerazioni introduttive, in *Dir. Pen.e Proc.*, n°7, 2008, Dossier la prova scientifica nel processo penale, pag. 2.
[20] V. DENTI, Scientificità della prova, in *Riv dir proc*, 1972, pag. 415.

giudice e delle parti[21]: il giudice non è peritus peritorum ma allo stesso tempo non può e non deve essere succube del "verdetto dello scienziato", non può accettare passivamente i risultati ma deve necessariamente valutarne attendibilità delle procedure impiegate e, conseguentemente, dei risultati ottenuti. Anzi proprio perché in taluni casi «lo strumento tecnico scientifico diventa spesso strumento di ricerca e formazione della prova»[22] tale controllo diventa essenziale per garantire il contraddittorio dibattimentale sulla prova stessa.

Come garantire quindi un controllo effettivo delle parti e del giudice sull'operato dell'esperto tenuto conto che questi impiegherà nello svolgimento del compito assegnatoli conoscenze specifiche? Partendo dalla concezione post-positivista della scienza innanzitutto possiamo sottolineare come il binomio scienza-verità sia del tutto inadeguato, soprattutto con riguardo agli ultimi decenni in cui l'evoluzione scientifica sembrerebbe non arrestarsi mai. Il rischio connesso potrebbe quindi configurarsi come un incauto affidamento alla "scienza cattiva maestra". Come è stato notato da Caprioli F. (2008) «la scienza può diventare cattiva maestra del giudice penale per tre ragioni: 1) quando è cattiva scienza, cioè quando si vogliono impiegare (...) strumenti tecnico- scientifici che non garantiscono in sé e per sé (…) un margine sufficiente di affidabilità e attendibilità; 2) quando è una buona scienza ma applicata male, cioè applicata al caso concreto da cattivi scienziati; 3) quando è una buona scienza correttamente applicata in sede processuale che viene, tuttavia, utilizzata in modo improprio o fuorviante dal giudice in sede di decisione»[23]. Il rischio di affidarsi alla "scienza spazzatura", cd bad science o junk science americana, è fortemente presente soprattutto con riguardo alle nuove prove scientifiche. Emblematica sul punto la sentenza della Corte Suprema statunitense Daubert , leading case che ha dato il via ad importanti riflessioni sul tema, in particolare sulla necessaria valutazione critica da parte del giudice dei metodi e delle procedure adottate dall'esperto[24]: egli dovrà, in sostanza, valutare il tasso di scientificità della tecnica probatoria attraverso la cd cultura dei criteri. Si è notato, infatti, come in tale sede di controllo si celi il paradosso del giudice, inesperto, che valuta e giudica l'operato dell'esperto, atteso che anche qui operi la conoscenza e il sapere comune di cui si è detto. In realtà qui la cultura da impiegare ha un contenuto differente rispetto alla prima, in sede di ricostruzione del fatto: ciò che rileva è lo schema concettuale che ne sta alla base, «indici applicando i quali è dato al giudice e alle parti di controllare se i principi e le tecniche adottate dall'esperto siano assistite da un fondamento di validità e se la loro applicazione nel caso concreto sia stata corretta »[25]. L'uscita del paradosso viene quindi a essere assicurata per un verso, dal fatto che in sede di controllo non si richiede al giudice di ripetere la consulenza portata avanti dall'esperto ma semplicemente di valutarla ed eventualmente di discostarvisi, e, per altro, che si tenga distinta la cd cultura di merito operante in sede di ricostruzione del fatto, dalla cd cultura dei criteri, come insieme di schemi concettuali e logici necessari per scrutinare l'affidabilità e integrità delle procedure utilizzate.

Le considerazioni fin qui fatte a livello generale per la prova scientifica classica, si arricchiscono di successive problematiche legate al crescente utilizzo in ambito processuale di prove scientifiche "nuove", caratterizzate dall'uso di strumenti ad alta specializzazione di cui si discute la natura nonché la validità e applicabilità. L'elemento di novità può essere letto da un punto di vista prettamente scientifico, come novità nel campo del sapere umano e scientifico. La formulazione di una nuova teoria scientifica, la cui applicazione potrebbe portare a esiti applicativi importanti, finanche alla messa in discussione di teorie consolidate, deve essere necessariamente studiata e vagliata dalla comunità scientifica di riferimento a garanzia dell'essenza stessa della legge (sperimentabilità, generalità, controllabilità) onde evitare la caduta nella bad or junk science. Oppure la novità può essere letta da un punto di vista prettamente applicativo, legata al nuovo impiego a livello processuale che se ne fa. Si pensi ad esempio alle discusse tecniche legate alla tanatologia, alla bloodstrain pattern analysis (BPA), al luminol, allo stub, alla computer forensics. È proprio su quest'ultime tipologie che la dottrina ha manifestato le più forti perplessità in quanto con esse «si manifesta in tutta la sua nettezza il paradosso del giudice inesperto che si trova a dover controllare l'operato dell'esperto»[26].

Ai fini della nostra indagine, vediamo come l'informatica forense rappresenti la "nuova" scienza di riferimento nel campo in quanto è la disciplina avente ad oggetto lo studio delle attività di individuazione, conservazione, protezione, estrazione, documentazione ed ogni altra forma di trattamento ed interpretazione del dato digitale memorizzato su supporto informatico, al fine di essere valutato come prova nel processo. In parallelo è doveroso altresì fornire una definizione di prova informatica: nel farlo ci si affida al noto studioso di computer forensics Casey[27] il quale definisce digital evidence qualsiasi dato che possa stabilire che un crimine è stato commesso o che può fornire un collegamento tra un crimine e la sua vittima o tra un crimine e chi l'ha commesso. Dalle due definizioni si comprende come non solo l'attività di acquisizione dei dati sia connotata da un alto tasso di scientificità, ma, altresì, il risultato da esso originato ne è al tempo stesso pervaso. Essendo poi l'evidenza risultato della procedura acquisitiva seguita, i metodi con i quali tali risultati vengono in luce non possono e non devono essere tralasciati, se non a scapito di una perdita legata al diritto di difesa. Ciò che sorprende agli occhi di un giurista attento, però, è il diverso atteggiamento mostrato dalle Corti con riguardo alle evidenze elettroniche rispetto ad ulteriori

[21] O. DOMINIONI, *La prova penale scientifica*, Giuffrè, Milano, 2007, pag. 68.
[22] F. CAPRIOLI, La scienza cattiva maestra in *Cass. Pen*, n° 9, 2008, pag. 3525.
[23] F. CAPRIOLI, La scienza cattiva maestra in *Cass Pen*, n° 9, 2008, pag. 3524.
[24] La dottrina contraria (Cfr. U. UBERTIS) sostiene, di contro, come la prova non autenticamente scientifica sarebbe manifestamente irrilevante, in quanto i periti e i consulenti tecnici che si servano di una cattiva scienza non sarebbero neppure nominabili i fini del conferimento dell'incarico, in difetto quindi dei requisiti previsti per la nomina.
[25] O. DOMINIONI, *La prova penale scientifica*, Giuffrè, Milano, 2007
[26] E. BARGIS, Note in tema di prova scientifica nel processo penale, in *Riv. Dir. proc.* n°1, 2011, pag. 8.
[27] E. CASEY, *Digital evidence and computer crime*, 3° edizione, Elsevier Inc, 2011 pag. 7.

nuove prove scientifiche come ad esempio il Dna. Se in quest'ultimo caso l'atteggiamento dei giudicanti fu tutt'altro che fiducioso, con la prova informatica si è assistito spesso ad una cieca fiducia alle risultanze prodotte mediante l'impiego di strumentazioni informatiche, quasi come se "le macchine non potessero mentire". In realtà, proprio in ragione delle potenzialità (talvolta altamente intrusive dei diritti di libertà dell'indagato o di terzi) insite in tali procedure e l'alto tasso di distorsione dei risultati dovrebbe esserci una più attenta riflessione. Ci si riferisce in particolare a quell'atteggiamento superficiale di parte di quella giurisprudenza che, soprattutto nei tempi che hanno preceduto la ratifica alla Convenzione sul Cybercrime, hanno ritenuto legittimo avallare prassi non sorrette da un accettabile grado di scientificità finanche alla distorsione di procedure classiche legate ad istituti tradizionali [28] . Peraltro il dibattito dottrinale sul tema è vivo; ciò che manca, invece, è un confronto reale con le Corti che con ritardo iniziano ad affrontare le problematiche insite nella "nuova" prova. Un possibile appiglio ci viene offerto da un punto di vista di diritto comparato, dal lungo percorso intrapreso dalle Corti americane, paese fra l'altro che ha visto la genesi della digital evidence e che quindi ha da tempo consolidato principi e valori di fondo in materia.

Il leading case più famoso risale al 1993 con la sentenza Daubert vs Merrell Down Pharmaceuticals il quale ha segnato una decisiva svolta nel campo di ammissione della prova scientifica fino a quel momento retta dal principio del general acceptance test al tempo generatosi nella vicenda Frye vs United States[29]. Il caso Daubert[30] portò allo sviluppo di quattro punti, ancora oggi fondamentali per valutare in maniera conforme il tasso di affidabilità delle procedure impiegate. Benché il parallelo fra expert witness e perito possa sembrare improprio, stante il diverso tenore delle due figure nei due contesti processuali, si deve comunque prendere atto dell'eco che detta pronuncia ha avuto nel contesto italiano che ha portato dottrina e giurisprudenza ad orientarsi in tal senso. Per il giudicante valutare se il perito o il consulente tecnico abbiano applicato correttamente la "buona" scienza richiesta dal caso non è cosa semplice. Se di fronte alla testimonianza, ad esempio, egli è in possesso di indici di affidabilità quali la credibilità del dichiarante o dalla conferma delle dichiarazioni da parte di soggetti esterni o di elementi materiali, di fronte alle prove scientifiche può trovarsi disarmato. La dottrina propone, quindi, anche sulla base dei principi d'oltreoceano, la necessità per lo stesso di porre in essere "contromisure preventive" che si esplicano principalmente nel momento del conferimento dell'incarico. Egli, infatti, dovrà non solo verificare il possesso della specializzazione richiesta ma altresì dovrà vagliarne la specifica qualificazione in rapporto all'oggetto dell'accertamento, ricavandola dalle precedenti esperienze di natura professionale, didattica e giudiziaria, dalle pubblicazioni su riviste specializzate, dallo standard professionale dei laboratori in cui andrà a operare.

Sul piano della scienza perseguita, viene in luce, un primo aspetto legato al testing della procedura: l'utilizzo di una fase di sperimentazione del prodotto volta alla validazione della procedura seguita porterà sicuramente a un risultato migliore in termini di output. In campo forense sono due i test principali che possono essere impiegati per l'individuazione di eventuali falle nel sistema. I test sui falsi negativi assicurano che la ricerca impostata dal forenser con una determinata impostazione (ad esempio la visualizzazione di tutti i file contenuti in memoria, compresi quelli cancellati) avvenga secondo l'ordine ricevuto; i test sui falsi positivi assicurano, invece, che i tool in uso non compromettano il sistema target mediante la creazione di file estranei al contenuto originario del dispositivo. Il secondo requisito è rappresentato dall'error rates ovvero se è conosciuto e in quale misura è presente il tasso di errore. Questo è sicuramente uno dei aspetti che maggiormente interessa le operazioni di digital forensics che viene costantemente tenuto in considerazione mediante tecniche di error management. A chiusura troviamo la publication e l'acceptance. Il primo aspetto legato alla pubblicazione dei risultati riecheggia in parte vecchio principio del Frye Test; il secondo, invece, delega alla comunità scientifica di riferimento l'autorevolezza di riconoscere come valida e generalmente accetta la procedura utilizzata per operazioni simili. Su quest'ultimo punto le operazioni di forensics sono ancora "giovani" anche se, per alcune ipotesi di lavoro, sono andati a svilupparsi standard operating procedure che sembrerebbero muoversi su questa strada.

Per quanto riguarda il panorama processuale italiano si è detto come il nostro paese soffra di un ritardo legato all'affiorare del problema nelle Corti. Una prima sentenza sul punto è rappresentata dal caso Vierika[31] in cui si affermava correttamente come «non è compito di questo Tribunale determinare un protocollo relativo alle procedure informatiche forensi, ma semmai verificare se il metodo utilizzato dalla p.g. nel caso in esame abbia concretamente alterato alcuni dei dati ricercati. (…) Non è permesso 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 (…)».

[28] Cfr CAJANI, *La ricezione della notitia criminis: i primi passi verso una corretta individuazione ed acquisizione degli elementi di prova di natura informatica*, dove a pag. 93 riporta la posizione della Cassazione che ha ritenuto legittimo l'operato degli agenti di polizia giudiziaria i quali, ottenuta la disponibilità di un telefono cellulare costituente mezzo per la commissione del reato, rispondevano alle chiamate ricevute al fine di utilizzare le notizie così raccolte come assunzione di sommarie informazioni, non intervenendo in tale frangente alcuna relazione fra le intercettazioni telefoniche e la segretezza costituzionale delle comunicazioni *ex* art. 15 Cost.

[29] Il caso s'incentrava intorno alla questione riguardo all'ammissibilità o meno della cd "macchina della verità", la quale partendo dalla misurazione della pressione sanguigna delle sistole e attraverso l'analisi della variazione della stessa a seguito delle domande e delle risposte fornite dal soggetto sottoposto al test, sarebbe stata in grado di indicare il grado di veridicità delle affermazioni. La Corte non ammise tale strumento, riconoscendone tuttavia il carattere di novità. Nello specifico formulò il cd principio del *general acceptance test*, nel quale venivano assunti come fattori e indici di affidabilità: la validità del principio scientifico, la validità tecnica e procedurale seguita nelle operazioni, l'appropriata funzionalità degli strumenti, l'uso corretto di procedure, le qualifiche specializzate della persona che esegue il test e ne analizza i risultati. La portata innovativa del principio fu applicata in prima battuta alle sole prove scientifiche sperimentali, e solo in un secondo momento esteso anche alle ipotesi di uso delle cd *soft science*. Il principio nonostante venne accolto con favore per la sua portata innovativa e garantista entrò in crisi intorno agli anni '60-'70.

[30] Cfr anche gli sviluppi successivi rappresentati dalla successiva sentenza *Kumho Tire vs Carmichael*.

[31] Tribunale di Bologna, sent. n° 1823.