PROCESSO PENALE E PROVA INFORMATICA: PROFILI INTRODUTTIVI[*].

di Gianrico Ranaldi[**]

Sommario. 1. Sapere scientifico e libero convincimento del giudice. – 2. Titolo. – 3. (Segue): I lineamenti della prova informatica – 4. Il "ritardo" del legislatore e le spinte a matrice sovranazionale. – 5. I futuribili: l'intelligenza artificiale ed il *due process of law*.

1. Sapere scientifico e libero convincimento del giudice.

L'analisi del rapporto tra scienza e processo, in genere, e processo penale, in particolare, ha origini risalenti. Infatti, sia la dottrina, che la giurisprudenza -di merito e di legittimità- hanno tentato di definire i *contorni* di una relazione, che è di per sé complessa ed articolata, e che sconta perlomeno il disallineamento dei relativi canoni di ragionamento[1].

Segnatamente, se il sapere scientifico oramai rappresenta, con l'aumento del progresso tecnologico, uno strumento di fondamentale importanza in sede di verifica, ad opera del giudice penale, dell'ipotesi di lavoro formulata con l'atto imputativo, è chiaro che le attività del giudice e dello scienziato non siano, per dir così, "sovrapponibili"[2].

[*] *Sottoposto a referaggio*.

[**] Professore associato di Diritto processuale penale – Università degli studi di Cassino e del Lazio Meridionale.

[1] Sul necessario impiego di "esperti" per la ricostruzione del fatto contestato con l'atto imputativo, i cui elementi costitutivi riconducono a competenze tecniche particolari e specifiche, v. Damaska, *Diritto delle prove alla deriva*, trad. it., Bologna, 2003, p. 205. In materia conserva rilievo fondamentale l'opera di Stella, *Giustizia e modernità*, Milano, 2003, 11 ss.

[2] In tema, Canzio, *Prova scientifica, ragionamento probatorio e libero convincimento del giudice nel processo penale*, in *Dir. pen. proc.*, 2003, 10, p. 1195 ss.; Caprioli, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cass. pen.*, 2008, p. 3520; Dominioni, *La prova scientifica*, Milano, 2005, p. 25 ss.; *Id*., *Prova scientifica (dir. proc. pen.)*, in *Enc. Dir*., *Annali*, II, Milano, 2008, p. 976 ss.; *Id*., *In tema di nuova prova scientifica*, in *Dir. proc. pen,*; Lorusso, *La prova scientifica*, in *La prova penale*, diretto da Gaito, I, Torino, 2008, p. 295 ss.; Lupària, *Processo penale e scienza informatica: anatomia di una trasformazione epocale*, in *Investigazione penale e tecnologia informatica*. *L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, a cura di Lupària, Zaccardi, Milano, 2007, p. 127 ss.; Varraso, *La prova tecnica*, in *Trattato di procedura penale*, diretto da Spangher, II, *Prove e misure cautelari*, 1 t., *Le prove*, a cura di Scalfati, Torino, 2009, 229 ss.; Tonini, *Prova scientifica e contraddittorio*, in *Dir. pen. proc,*, 2001, 1459 ss.. Nel settore processual-civilistico, tra gli altri, v. Denti, *Scientificità della prova e libera valutazione del giudice*, in *Riv. dir. proc.*, 1972, 414; Comoglio, *Le prove civili*, Torino, 2010, 839 ss,; Taruffo, *La prova dei fatti giuridici*, Milano, 1992, 307 ss.; Id., *La prova scientifica nel processo civile*, in

Per conseguenza, la mera introduzione al tema della relazione esistente tra sapere scientifico e convincimento giudiziale abbisogna di alcune, non differibili, "regole d'ingaggio"[3].

E si spiega.

Se "non è naturalmente necessario che il giudice abbia le conoscenze scientifiche dell'esperto né che compia ex novo il percorso dal medesimo compiuto", è rilevante "che egli sia in grado di valutare la validità dei metodi scientifici utilizzati". Pertanto, "non è richiesto che il giudice sia un esperto ma che sia in grado di valutare a quali condizioni un'informazione può essere ritenuta dotata di validità scientifica"[4].

In altri termini, le principali difficoltà che emergono, in sede di valutazione degli elementi di prova a *matrice* scientifica, conseguono all'evoluzione che ha avuto il concetto di scienza nel corso degli anni.

In particolare, la prova scientifica era considerata una sorta di prova «*sui generis,* svincolata dalle regole ordinarie"[5], in quanto il giudice, in sede di ricostruzione del fatto descritto nell'editto accusatorio attraverso l'uso di leggi scientifiche di copertura, si affidava totalmente al perito, che, a sua volta, era considerato l'unico in grado di conoscere e trasmettere il sapere tecnico e specialistico.

Scritti per F. Stella, II, Napoli, 2007, 1325 ss.. Sul punto, è enorme il contributo della letteratura straniera. In proposito, nel contesto anglosassone, tra gli altri, v. Beecher-Monas, *Evaluating Scientific Evidence. An interdisciplinary framework for intellectual due process*, Cambridge, 2007, 36 ss.; L-T Choo, *Evidence*, Oxford, 2015, 313 ss.; AA.VV., *Expert evidence and scientific proof in criminal trials*, a cura di Roberts, 2017, 11 ss.; Roberts, Zuckerman, *Criminal Evidence*, Oxford, 2010, 469 ss.; Walton, Zhang, *The epistemology of scientific evidence*, in *Artificial Intelligence and Law*, 21, 2, 2013, 2 ss.

[3] Scienziato e giudice ricercano, entrambi, elementi ed informazioni utili per conoscere un fenomeno, così da comprenderne le possibili cause e gli effetti. Mentre il compito «*dello scienziato è quello di esaminare un fatto ripetibile nel senso che è riproducibile o, comunque, si è riprodotto in modo da essere osservato. La finalità è quella di ricavare le leggi della natura che ne regolano lo svolgimento*», anche in considerazione della circostanza che lo specifico «*fenomeno fisico o chimico obbedisce a leggi della natura che sono uniformi, poste le medesime condizioni*», il compito del giudice consiste nell'esaminare «*un fatto umano* […] *che è avvenuto nel passato* […] *non è ripetibile* […] *e non è determinato da leggi*». L'attività giurisdizionale tende all'accertamento di un fatto «*al fine di valutare la responsabilità penale di una persona in relazione ad un'imputazione formulata* […] *da un organo di accusa*»; lo scienziato «*può dichiarare che un problema al momento non è risolvibile con dati controllabili e misurabili. Di contro il giudice deve decidere al termine di un processo che si svolge in tempi predeterminati*» (Tonini, *La prova scientifica: considerazioni introduttive*, in *La prova scientifica nel processo penale*, a cura di Tonini, in *Dir. pen. e proc. Dossier*, 2008, 6, 7-8).

[4] Brusco, *La valutazione della prova scientifica*, in *La prova scientifica nel processo penale*, a cura di Tonini, cit., 28.

[5] Conti, Iudex peritus peritorum *e ruolo degli esperti nel processo penale*, in *La prova scientifica nel processo penale*, a cura di Tonini, cit., 29.

Quanto detto valeva quale corollario applicativo alla concezione positivistica della scienza che era invalsa in passato ed ha avuto dirette conseguenze anche nella concezione del rapporto tra scienza e processo penale.

Infatti, i sostenitori della specifica impostazione teorica ritenevano che la scienza fosse infallibile[6]: ne conseguiva, per quanto in questa sede interessa, che nel processo penale era, per così dire, sufficiente che il giudice nominasse un perito, il quale avrebbe *rivelato* "la scienza idonea a spiegare il fenomeno oggetto di indagine"; per l'effetto, non sarebbe residuato spazio alcuno per il libero ed autonomo convincimento del giudice che, in sede di valutazione della *prova tecnica*, si sarebbe dovuto limitare a prendere atto della legge scientifica introdotta nel processo dal perito[7], motivando *per relationem* rispetto, per l'appunto, a quanto contenuto nella relazione peritale[8].

Sennonché, l'imprescindibile osmosi tra metodo scientifico ed epistemologia giudiziaria ha avuto eco anche nella *riscrittura* dei canoni ideali di relazione tra sapere scientifico ed attività valutativa e decisoria del giudice.

Infatti, non essendo la scienza più ritenuta euristicamente infallibile[9], si ritiene che qualsiasi inferenza -ad eccezione di quelle derivanti da leggi scientifiche a carattere generale o da leggi statistiche con margine di errore pressoché nullo- rivesta "comunque un carattere probabilistico e che anche il processo tecnologico e il metodo scientifico più avanzato o

---

[6] «*Era* illimitata *perché si riteneva che ogni singola legge scientifica aveva un valore generale e assoluto. La scienza era* completa *nel senso che la singola legge era idonea a spiegare interamente l'andamento del fenomeno. La scienza era* infallibile *perché era unica e non poteva sbagliare*» (Tonini, *La prova scientifica: considerazioni introduttive*, in *La prova scientifica nel processo penale*, a cura di Tonini, cit., 9).

[7] L'idea di libero convincimento affiorò, in ambito continentale, solo verso la fine del XVIII secolo, allorché i costituenti della Francia rivoluzionaria, con i decreti 16-29 settembre 1791 e 8/9 ottobre-3 novembre 1789, decisero di affidare la decisione della *quaestio facti* a una giuria di ispirazione anglosassone, dunque dotata di piena autonomia valutativa (*intime conviction*) e non gravata da obbligo di motivazione. In tale ipotesi, tuttavia, la scelta non costituì una reazione al sistema ordalico, ma al regime di valutazione probatoria che lo aveva soppiantato in Europa a partire dal XIII secolo, il regime delle prove legali positive. Su tale fase storica e sui suoi sviluppi successivi, v. Nobili, *Il principio del libero convincimento*, Milano, 1974, 145-266.

[8] Conti, Iudex peritus peritorum *e ruolo degli esperti nel processo penale*, in *La prova scientifica nel processo penale*, a cura di Tonini, cit., 29, la quale precisa, altresì, che «*in un quadro del genere si poteva affermare a buon diritto che la perizia era per definizione una prova neutra, come neutra era la scienza* […] *Si configurava, dunque, la perizia come una sorta di* prova legale».

[9] «*La scienza è* limitata: *di un fenomeno è possibile cogliere un numero limitato di aspetti e rappresentarli con una legge scientifica. La scienza è* incompleta*: non appena altri aspetti del medesimo fenomeno sono conosciuti, la legge scientifica deve, se possibile, essere aggiornata e modificata per rappresentare anche tali aspetti; se non è possibile aggiornarla o modificarla, la legge deve essere abbandonata. La scienza è* fallibile*: ogni legge scientifica ha un tasso di errore che deve essere ricercato; la conoscenza del tasso di errore è l'unico indice che una teoria è stata seriamente testata.* […] *Una legge, per poter essere ritenuta scientifica, deve essere sottoposta a tentativi di falsificazione*» (Tonini, *La prova scientifica: considerazioni introduttive*, in *La prova scientifica nel processo penale*, a cura di Tonini, cit., 9).

connotato da scarsi margini di errore» sia «in grado di offrire risposte, nel processo, solo in termini di probabilità, talora bassa o medio-bassa, altre volte alta o medio-alta"[10].

Stando così le cose, gli elementi di conoscenza promananti dall'impiego giudiziale di metodologie scientifiche, lungi dall'assumere valenza privilegiata e legale rispetto alla propria capacità di *spiegazione* del fatto di reato, devono essere valutati in maniera analoga agli elementi di prova, per così dire, ordinari: infatti, il giudice è chiamato a valutare la legge scientifica *indotta* nel processo dal c.d. *testimone esperto* al fine di comprenderne la specifica affidabilità ricostruttiva rispetto al fatto storico oggetto dell'imputazione, anche alla stregua delle ulteriori risultanze probatorie assunte nel corso del processo.

Pertanto, il giudice -in analogia con quanto avviene con tutte le fonti di prova e, quindi alla stregua del tradizionale *modello della motivazione legale e razionale* – ha l'onere di chiarire – anche con riferimento alla valutazione delle risultanze riconducibili all'assunzione di una prova scientifica- il proprio convincimento in merito all'accertamento del fatto di reato e, per l'effetto, di esporre il ragionamento logico giuridico che ha determinato, per quello che qui rileva, l'adesione alla specifica legge di copertura.

In altri termini, in sede di valutazione della prova scientifica *valgono* le ordinarie disposizioni normative relative al procedimento probatorio, con particolare riferimento al combinato disposto degli artt. 192, 546, 1° comma, lett. e), c.p.p.

Infatti, è la legge del processo ad imporre che "ogni passaggio argomentativo dal fatto probatorio al fatto da provare (oggetto della prova: art. 187 c.p.p.), principale o secondario, sia giustificato dal giudice che 'valuta la prova (l'elemento di prova) dando conto nella motivazione del risultati (probatori) acquisiti e dei criteri (d'inferenza) adottati', con riferimento alla regola d'inferenza probatoria applicata"[11].

---

[10] Canzio, *La motivazione della sentenza e la prova scientifica:* "Reasoning by probabilities", in *Prova scientifica e processo penale*, a cura di Canzio, Luparia, Padova, 2017, 13.

[11] Canzio, *Prova scientifica, ragionamento probatorio e libero convincimento del giudice nel processo penale*, cit., 1195. Inoltre, sul punto, si v. Conti, *Iudex peritus peritorum e ruolo degli esperti nel processo penale*, cit., 33-34, la quale chiarisce che «*come è noto, in un sistema come quello italiano il principio del libero convincimento significa che la sentenza è valida in quanto la motivazione è convincente. E questo comporta che non esistono prove più autorevoli di altre. Le prove valgono in ragione del loro contenuto. Pertanto, appare illogico riconoscere al perito in quanto tale un* quid pluris *di affidabilità, a pena di un ritorno alla prova legale*». Inoltre, «*occorre tener presente che nel processo penale non esiste il criterio della* best evidence *(prevalenza della prova migliore): ben può accadere che una prova dichiarativa prevalga sulla prova scientifica. In un sistema informato al principio del contraddittorio, la scienza non è attendibile in quanto tale ma in quanto sia in grado di dare una spiegazione convincente del fatto da accertare*».

Sennonché, la suspecificata impostazione sconta una difficoltà di fondo: il giudice è spesso privo delle conoscenze specialistiche necessarie per valutare in modo adeguato le leggi scientifiche *proposte* dal perito o dal consulente tecnico di parte.

Ne consegue -anche al fine di evitare il rischio di un sostanziale appiattimento sulle conclusioni dell'*esperto*, con le conseguenti ricadute negative in tema di autonoma valutazione del giudice- la necessità di individuare criteri e parametri idonei a garantire l'effettività dell'attività giurisdizionale di controllo e, per così dire, di validazione della legge scientifica di copertura.

Vale a dire.

Se la scienza non è in grado di garantire un determinato risultato probatorio con assoluta certezza e se, per l'effetto, lo scienziato deve procedere attraverso continui tentativi di falsificazione dell'ipotesi congetturale formulata[12], allora il giudice penale non può che assimilare lo specifico *modus operandi* valorizzando il più possibile il metodo del contraddittorio per la prova anche in sede di esame e analisi del grado di affidabilità della metodologia impiegata dall'*expert witness*, in sede di elaborazione ed assunzione della prova scientifica "raccolta" nel corso del giudizio.

Infatti, sta nei canoni modali del *giusto processo* la *best practice* per dare ausilio al giudice al fine di orientarsi e selezionare -tra le molteplici leggi scientifiche in astratto applicabili nella ricostruzione dei fatti oggetto dell'imputazione-quella adeguata alla spiegazione causale del caso concreto: se il *metodo dialettico* (*rectius*: il contraddittorio in senso forte ossia per la formazione della prova) è inteso come lo strumento elettivo per la ricostruzione del fatto contestato – e, quindi, per la *ricerca* della verità processuale – allora anche la

[12] Ferrua, *Metodo scientifico e processo penale*, in *La prova scientifica nel processo penale*, a cura di Tonini, cit., 12-13, secondo il quale il c.d. metodo scientifico -ossia l'insieme delle procedure di formulazione delle leggi scientifiche- è quello volto alla costituzione di un sapere certo e giustificato. Tuttavia, «*se il metodo può dirsi scientifico solo in quanto garantisca una conoscenza indebitamente certa, allora il metodo scientifico non esiste*», salvo che nel caso delle scienze formali o analitiche. Infatti, «*non esiste un metodo in grado di garantire l'assoluta certezza o verità delle conclusioni, le quali restano soltanto più o meno probabili (anche se convenzionalmente sono presentate come certe). La fallibilità è la contropartita per l'accrescimento di conoscenza che le conclusioni producono rispetto alle premesse, a differenza dei sistemi formalizzati dove le dimostrazioni sono tra-sformazioni sintattiche e le conclusioni sono già logicamente contenute negli assiomi di partenza*». Ne deriva, pertanto, che «*per quanto solida, ogni teoria scientifica ha pur sempre carattere congetturale*» e che, quindi, «*esiste sempre una pluralità di teorie in grado di spiegare i medesimi fatti empirici*».

prova scientifica dovrà essere sottoposta alla procedura di controllo e falsificazione processuale coincidente, per l'appunto, con l' assunzione nel contraddittorio tra le parti[13]. Stando così le cose, garantire la pienezza della dialettica tra le parti in sede assunzione della prova, in genere, e di quella scientifica, in particolare, rappresenta il *viatico* imprescindibile attraverso il quale il giudice potrà acquisire i mezzi necessari per adempiere alla propria "difficile e autonoma opera di decostruzione delle assunzioni sottostanti alle proposizioni scientifiche, secondo le peculiari esigenze di giustizia e nell'interesse pratico di risolvere la controversia"[14]. Infatti, il giudice, al fine di accertare, come accennato in precedenza, l'affidabilità e la validità scientifica di una data teoria e, soprattutto, la sua rilevanza rispetto al fatto contestato nell'imputazione- dovrà compiutamente valutare: la controllabilità e falsificabilità della teoria di specie; la conoscenza del tasso di errore che ne caratterizza le implicazioni; la sottoposizione di essa al controllo della comunità scientifica; la generale accettazione di essa presso la comunità degli esperti[15].

[13] Ferrua, *Metodo scientifico e processo penale*, in *La prova scientifica nel processo penale*, a cura di Tonini, cit., 17, il quale precisa che «*si sarebbe tentati a questo punto di considerare il contraddittorio come la traduzione processuale della falsificazione popperiana; ma, a ben vedere, i termini dell'equazione vanno invertiti. Sono la falsi-ficazione delle teorie, il metodo delle congetture e confutazioni a discendere dal contraddittorio proces-suale, a rappresentarne la trasposizione nella scienza, come ha sempre riconosciuto lo stesso Popper con i suoi frequenti richiami alla procedura accusatoria per i giurati. Secoli di processo inquisitorio ci hanno indotti a vedere nella discussione tra scienziati il modello ideale, lo specimen del contraddittorio, ma in realtà è stato l'antico processo accusatorio ad ispirare la moderna visione della scienza*».

[14] Canzio, *La motivazione della sentenza e la prova scientifica:* "Reasoning by probabilities", cit., 12.

[15] La specifica elencazione è stata enucleata dalla giurisprudenza italiana, che -in analogia a quanto chiarito dai giudici americani- ha individuato specifici criteri ermeneutici in grado di orientare il giudice in sede di valutazione delle diverse teorie scientifiche. Il riferimento è, come è noto, a Court of appeals of District of Columbia, 3 dicembre 1923, n. 293, Frye v. United States, in Federal Report, 1923, 1013, nonchè a Supreme Court of the United States 28 giugno 1993, Daubert v. Merrel Dow Pharmaceuticals, Inc., in Minnesota Law Review, 1994, 1345. Per quanto concerne la giurisprudenza italiana, v., su tutte, Cass., Sez. IV, 17 settembre 2010, Cozzini, in *Guida al dir.*, 2011, 6, 93, secondo cui «*l'affermazione del rapporto di causalità tra le violazioni delle norme antinfor-tunistiche ascrivibili ai datori di lavoro e l'evento-morte (dovuta a mesotelioma pleurico) di un lavorato-re reiteratamente esposto, nel corso della sua esperienza lavorativa (esplicata in ambito ferroviario), all'amianto, sostanza oggettivamente nociva, è condizionata all'accertamento: (a) se presso la comunità scientifica sia sufficientemente radicata, su solide e obiettive basi, una legge scientifica in ordine all'effetto acceleratore della protrazione dell'esposizione dopo l'iniziazione del processo carcinogenetico; (b) in caso affermativo, se si sia in presenza di una legge universale o solo probabilistica in senso statistico; (c) nel caso in cui la generalizzazione esplicativa sia solo probabilistica, se l'effetto acceleratore si sia deter-minato nel caso concreto, alla luce di definite e significative acquisizioni fattuali; (d) infine, per ciò che attiene alle condotte anteriori all'iniziazione e che hanno avuto durata inferiore all'arco di tempo com-preso tra inizio dell'attività dannosa e l'iniziazione della stessa, se, alla luce del sapere scientifico, possa essere dimostrata una sicura relazione condizionalistica rapportata all'innesco del processo carcinogenetico*». In proposito, v., inoltre, Dominioni, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi di elevata specializzazione*, Milano, 2005, 115 ss.; Gennari, *I criteri di ammissione della prova scientifica nel contesto internazionale*, in *Prova scientifica e processo penale*, a cura di Tonini, cit., 165 ss.; Naimoli, *Principio di falsificazione tra prova indiziaria e prova scientifica*, Ospedaletto, 2017, 79 ss..

In altre parole, è lecito ritenere che il giudice potrà assolvere al suo fondamentale ruolo di *gatekeeper* -ossia di *custode del metodo scientifico* – solo se optasse per il delineato *percorso di validazione*, che tende a verificare la coerenza esterna del ragionamento tecnico articolato e, quindi, a scongiurare il rischio dell'autoreferenzialità limitatrice di esso.

Pertanto, il convincimento del giudice in ordine all'affidabilità ermeneutica e ricostruttiva della teoria formulata dal perito o dal consulente tecnico non può conseguire, in esclusiva, alla semplice verifica di coerenza interna della relazione peritale o di consulenza, ma deve anche risultare da un percorso che conduca il giudice stesso ad interrogarsi sulla validità, estrinseca ed intrinseca, del ragionamento che l'*expert witness* ha ritenuto idoneo, nel caso concreto, in chiave esplicativa.

Per tirare le fila del discorso: il giudice deve informarsi sui presupposti di validità del metodo scientifico utilizzato nel processo, così da "essere pronto a esaminare visioni scientifiche diverse o anche contrapposte e a scegliere - dando logicamente conto della scelta - quella più convincente non in base ad un opzione pregiudiziale e immotivata ma, dopo aver dato il più ampio spazio al contraddittorio, quella fondata su una dimostrata attendibilità scientifica e su argomentazioni che non abbiano trovato obiezioni insuperabili"[16]; infatti, è solo attraverso lo specifico *modus operandi* che il giudice sarà in grado, tra l'altro, di selezionare le leggi scientifiche, sin dalla fase della loro *ammissione* nel processo, e di distinguerle dalla c.d. "scienza spazzatura"[17].

[16] Brusco, *La valutazione della prova scientifica*, in *La prova scientifica nel processo penale*, a cura di Tonini, cit., 28. Inoltre, in tema di valutazione della prova scientifica, con particolare riferimento alla necessità per il giudice di calare nel caso concreto la legge scientifica di riferimento al fine di escludere ogni ragionevole dubbio sulla ricostruzione del fatto per cui è processo, v. Cass., Sez. un., 10 luglio 2002, Franzese, in *Foro it.*, 2002, II, 601, secondo cui «*la conferma dell'ipotesi accusatoria sull'esistenza del nesso causale non può essere dedotta automaticamente dal coefficiente di probabilità espresso dalla legge statistica, poiché il giudice deve verificarne la validità nel caso concreto, sulla base delle circostanze del fatto e dell'evidenza disponibile, così che, all'esito del ragionamento probatorio che abbia altresì escluso l'interferenza di fattori alternativi, risulti giustificata e processualmente certa la conclusione che la condotta omissiva del medico è stata condizione necessaria dell'evento lesivo con "alto o elevato grado di credibilità razionale" o "probabilità logica". L'insufficienza, la contraddittorietà e l'incertezza del riscontro probatorio sulla ricostruzione del nesso causale, quindi il ragionevole dubbio, in base all'evidenza disponibile, sulla reale efficacia condizionante della condotta omissiva del medico rispetto ad altri fattori interagenti nella produzione dell'evento lesivo, comportano la neutralizzazione dell'ipotesi prospettata dall'accusa e l'esito assolutorio del giudizio*».

[17] Cfr. Naimoli, *Principio di falsificazione tra prova indiziaria e prova scientifica*, cit., 104.

2. La prova scientifica: rilievi minimi.

Descritto, con consapevole autolimitazione, l'articolato rapporto intercorrente tra sapere scientifico e processo penale, va delineato -seppur per cenni- il concetto, che rileva a fini processualpenalistici, di prova scientifica, tenuto conto che tra esso e la nozione di prova informatica intercorre un rapporto di *genus* a *species*.

Procediamo con ordine.

Può definirsi scientifica la prova che «*partendo da un fatto dimostrato, utilizza una legge scientifica per accertare l'esistenza di un ulteriore fatto da provare*»[18]: infatti, essa si indentifica con il complesso di «*operazioni probatorie per le quali, nei momenti dell'ammissione, dell'assunzione e della valutazione, si usano strumenti di conoscenza attinti alla scienza e alla tecnica, cioè a dire principi e metodologie scientifiche, metodiche tecnologiche, apparati tecnici il cui uso richiede competenze esperte*»[19].

Sotto il profilo strumentale, il mezzo attraverso il quale le suspecificate competenze specialistiche -ove non già possedute dal giudice- possono essere introdotte all'interno del processo penale, è rappresentato dal mezzo di prova della perizia (o della consulenza tecnica) -disciplinato dagli artt. 220 ss. c.p.p.- che è ammissibile, per l'appunto, «*quando occorre svolgere indagini o acquisire dati o valutazioni che richiedono specifiche competenze tecniche, scientifiche o artistiche*».

Vale rilevare che, per un verso la perizia è considerata un "mezzo di prova del giudice", nella misura in cui il perito può essere nominato, in esclusiva, proprio dal giudice, che provvede in tal senso anche d'ufficio nel corso del dibattimento, mentre durante la fase delle indagini preliminari la nomina relativa può avvenire solo su richiesta di parte, qualora sussistano profili di urgenza ai sensi dell'art. 392 c.p.p.; per un altro verso, il sistema processuale riconosce alle parti un generale diritto alla prova tecnico scientifica, che si traduce, in buona sostanza, nella possibilità di nominare propri consulenti tecnici, sia nel caso in cui il giudice abbia già disposto l'assunzione di una perizia (art. 225 c.p.p.), sia nel caso in cui, di contro, essa non sia stata disposta (art. 233 c.p.p.).

[18] Tonini, *La prova scientifica: considerazioni introduttive*, cit., 8.
[19] Dominioni, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi di elevata specializzazione*, Milano, 2005, 12.

D'altronde, il riconoscimento in favore delle parti e dei soggetti processuali del diritto alla prova scientifica emerge, in via diretta, anche alla stregua dei contenuti – tanto degli artt. 359 e 360 c.p.p. – con riguardo all'attività di indagine condotta dal pubblico ministero – quanto degli artt. 391-*sexies* e 391-*decies* c.p.p. – in relazione alle investigazioni difensive dell'indagato e della persona offesa[20]; si aggiunga, poi, che – in sede di udienza preliminare – nell'ambito dell'attività di integrazione probatoria di cui all'art. 422 c.p.p., il giudice – quando ritiene di non poter decidere allo stato degli atti (art. 421, 4° co., c.p.p.) ovvero quando non adotta un'ordinanza interinale di integrazione delle indagini (art. 421-*bis* c.p.p.) – può disporre, anche d'ufficio, l'assunzione delle prove delle quali appare evidente la decisività ai fini della sentenza di non luogo a procedere e disporre la citazione, tra gli altri, dei periti e dei consulenti tecnici[21].

Last but not least.

Va segnalato, da un lato che – come già detto in precedenza – per quanto concerne le fasi dell'ammissione e della valutazione di una prova scientifica, occorre richiamare non solo le disposizioni generali in materia di probatoria – con particolare riguardo agli artt. 187, 189 e 190 c.p.p- ma anche i suspecificati criteri interpretativi enucleati dalla giurisprudenza; mentre, dall'altro lato l'assunzione della prova scientifica – analogamente a quanto prescritto rispetto alle altre fonti di prova- avviene in maniera dialettica, ossia esaminando -nel contraddittorio delle parti- i periti ed i consulenti tecnici nel rispetto delle disposizioni codicistiche relative all'esame dei testimoni.

3. (Segue): I lineamenti della prova informatica.

Lo sviluppo tecnologico ha *accresciuto*, sia qualitativamente che quantitativamente, gli strumenti conoscitivi a disposizione del giudice e delle parti per condurre la verifica di fondatezza dell'ipotesi di lavoro delineata nell'imputazione e per ricostruire la relativa spiegazione causale.

[20] «*Ciò comporta che tutte le parti hanno il diritto di ricercare le fonti e gli elementi di prova; hanno il diritto di presentare dati scientifici al giudice; hanno il diritto di nominare consulenti tecnici e di chiedere la loro ammissione; hanno il diritto di interrogare i propri consulenti e di contro-interrogare quelli della controparte*» (Tonini, *Prova scientifica e contraddittorio*, cit., 1462).

[21] Varraso, *La prova tecnica*, cit., 245 ss.

In tale contesto speculativo, allora, si colloca la nascita e la diffusione applicativa delle *computer forensics* o delle investigazioni digitali[22], che concernono le "tecniche e [gli] strumenti utilizzati per recuperare gli elementi di prova (digitali) all'interno di un computer"[23].

Sennonché, la rilevanza dello studio dei sistemi informatici deriva dalla constatazione che essi pervadono capillarmente le singole attività umane, tanto che possono diventare, a seconda dei casi, strumenti necessari per la commissione di reati o, per quanto in questa sede interessa, mezzi attraverso i quali accertare e/o dimostrare l'integrazione di un determinato comportamento penalmente antigiuridico.

Infatti, un sistema informatico, "un computer portatile e uno *smartphone* conservano nella memoria interna una ingente massa di dati relativi al loro utilizzo, che consentono di risalire ad ogni attività che è stata espletata con il dispositivo"[24].

Stando così le cose, è d'uopo, anzitutto, essere consapevoli della complessità dell'inquadramento concettuale delle medesime prove digitali[25], considerata l'intrinseca specificità delle fonti di prova in esame, che pur rientrando nel novero delle prove scientifiche[26] presentano, come nel prosieguo si vedrà, tratti assai peculiari, tanto che necessiterebbero di una "rivisitazione delle categorie processuali tradizionali"[27].

---

[22] Ziccardi, *L'origine della* computer forensics *e le definizioni*, in *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, cit., 35 ss.

[23] Aterno, *Acquisizione e analisi della prova informatica*, in *La prova scientifica nel processo penale*, a cura di Tonini, cit., 61, il quale precisa, altresì, che lo specifico ambito scientifico si riferisce, più in generale, al mondo delle «*forensics sciences*», ossia alle «*scienze forensi applicate al mondo dei computer*». Ne consegue che «*l'ambito di applicazione di questa scienza dipende in parte dall'oggetto delle sue attenzioni: vi è la* computer forensics *con riferimento all'analisi dispositivi e supporti fisici e statici, la* network forensics *che ha come oggetto l'analisi forense di server e di reti, la* mobile forensics *che analizza i dispositivi cellulari e mobili, la* PDA forensics *che invece esamina con modalità forensi i telefoni palmari di ultima generazione*».

[24] Cuomo, *La prova digitale*, in *Prova scientifica e processo penale*, a cura di Canzio, Luparia, cit., 672, il quale afferma, altresì, che «*le prove che i sistemi informatici contengono al loro interno non sono altro che cariche elettromagnetiche, perché le informazioni come una immagine, un suono, una sequenza video, un testo o un'altra rappresentazione del pensiero umano subiscono un processo di conversione in una sequenza di bit, risultanti dalla magnetizzazione o smagnetizzazione della superficie di un supporto o dalla variazione dello stato fisico della materia*».

[25] «*Sul punto occorre intendersi fin da subito. Ben può utilizzarsi la formula digital evidence, o prova digitale, quale recipiente ove includere ogni forma di utilizzo a fini procedimentali, in senso lato, di dati originariamente contenuti in supporti informatici o telematici, oppure ancora trasmessi in modalità digitale. A patto, però, di tenere a mente che si tratta di un fenomeno con diverse sfaccettature, che mal si presta a inquadramenti a priori ed è difficilmente conciliabile con le tradizionali distinzioni in tema di prova. Più in particolare, la natura multiforme del dato digitale sconsiglia generalizzazioni aprioristiche*» (Pittiruti, Digital evidence *e procedimento penale*, cit., 8).

[26] Sul rapporto tra prova scientifica e prova informatica s v. Pittiruti, Digital evidence *e procedimento penale*, Torino, 2017, 14 ss..

[27] Conti, *La prova informatica e il mancato rispetto delle* best practice: *lineamenti sistematici sulle conseguenze processuali*, in *Cybercrime*, diretto da Cadoppi, Canestrari, Manna, Papa, Milano, 2019, 1329.

Segnatamente, sotto il profilo definitorio, le prove informatiche -o anche, seppur in via esemplificativa, *digital evidence*- rappresentano "il complesso di informazioni digitali in grado di stabilire se un crimine è stato commesso o che possono rappresentare un collegamento tra un crimine e le sue vittime o i suoi esecutori»[28], tanto che può considerarsi digital evidence «ogni informazione probatoria la cui rilevanza processuale dipende dal contenuto del dato o dalla particolare allocazione su di una determinata periferica, oppure dal fatto di essere stato trasmesso secondo modalità informatiche o telematiche"[29].

Sennonché, le specifiche fonti di prova risultano, come già accennato, di difficile collocazione all'interno delle ordinarie categorie probatorie.

Per un verso -stante la natura "multiforme" delle *digital evidence*- sussiste una sostanziale difficoltà nel ricondurre il relativo risultato probatorio nell'ordinaria bipartizione tra prove rappresentative e prove indiziarie o critiche.

Infatti, "la natura informatica del dato da cui trarre il risultato probatorio può vertere sia direttamente sul *thema probandum* sia su un fatto secondario da cui risalire al fatto principale: quale esempio del primo tipo v'è l'immagine pedopornografica in formato digitale il cui possesso è contestato all'imputato; quale esempio del secondo tipo possono addursi i file di log circa l'avvenuto accesso ad un social network per mezzo di un computer localizzato sulla *scena criminis* ove è stato commesso un omicidio nella medesima finestra temporale"[30].

Per altro verso, è disagevole anche collocare la prova informatica all'interno dei mezzi di ricerca atipici o innominati ai sensi dell'art. 189 c.p.p.

E si spiega.

Se -contestualmente all'emersione della relativa problematica definitoria e di collocazione sistematica- non sembrarono esserci dubbi sull'inserimento della prova digitale tra le prove atipiche: infatti, l'art. 189 c.p.p. si prestava a raccogliere tutti gli strumenti d'indagine diversi da quelli espressamente tipizzati, di seguito, però, emersero non poche perplessità in ordine alla possibilità di inquadrare la *digital evidence* nell'ambito specifico.

Segnatamente, l'impostazione, che negò la relativa compatibilità di inquadramento, derivò da un duplice ordine di ragioni: da un lato, l'entrata in vigore della l. 18 marzo 2008, n. 48,

[28] Casey, Digital evidence and Computer crime, in Academic Press, 2000, 196.
[29] Marafioti, Digital evidence *e processo penale*, in *Cass. pen.*, 2011, 12, 4509.
[30] Pittiruti, Digital evidence *e procedimento penale*, cit., 8-9.

determinò la modifica di istituti preesistenti, che vennero in parte rimodellati, assecondando *modi* e *maniere* che rendessero essi compatibili con il progresso tecnologico così che potessero essere impiegati anche per l'acquisizione, la raccolta e l'esame di dati informatici; dall'altro lato, si impose, in maniera problematica, il tema della congruità/adeguatezza della disciplina dettata dall'art. 189 c.p.p. rispetto alle peculiarità proprie della prova informatica[31].

Pertanto, in un contesto comunque colmo di incertezze, si comprese -nel tentativo di inquadrare compiutamente il fenomeno probatorio in esame, e, per l'effetto, di procedere alla sua classificazione e regolamentazione processuale- che occorreva muovere dalle peculiarità del c.d. *documento informatico* (*id est*, dell'elemento probatorio da acquisire e valutare nel corso del procedimento).

Vale a dire.

La prova informatica si caratterizza principalmente perché ha ad oggetto *dati* che, per loro natura, sono immateriali: le informazioni digitalizzate, infatti, prescindono dal supporto su cui sono originariamente memorizzate[32] e, per diretta conseguenza, sono agevolmente alterabili, in quanto possono essere facilmente modificate o addirittura cancellate qualora

[31] Pittiruti, Digital evidence *e procedimento penale*, cit., 18 ss., il quale precisa che «*la natura digitale dell'informazione da apprendere al procedimento non appare, di per sé, tale da consentire una classificazione preventiva della fonte di prova. Il che impone di verificare, caso per caso, se lo strumento probatorio relativo al dato digitale utilizzato nel caso di specie sia estraneo o meno – e, se sì, sotto quale profilo: fonte di convincimento del tutto nuova, oppure diverse modalità operative di mezzo già noto – al catalogo legale*» Pertanto, è «*pienamente legittimo, allora, in astratto, immaginare attività investigative su dati digitali da ricomprendere nel paradigma della prova atipica. Difatti, se è vero che, a seguito della L. n. 48/2008, gran parte delle verifiche sul dato digitale sono ora ricomprese all'interno delle tradizionali attività d'indagine, è altrettanto vero che lo sviluppo della scienza informatica fornisce l'occasione agli investigatori di coniare sempre nuove modalità di ricerca delle informazioni rilevanti*».

[32] In realtà, «*le informazioni rilevanti ai fini investigativi sono, nel caso della* computer forensics, *conservate e trasmesse in un linguaggio diverso, ovverosia quello digitale. Seppure i dati digitali, nel loro contenuto informativo, possono essere immediatamente percepiti da colui che viene in contatto con essi, ciò non significa che siano dotati di una materialità immediatamente percepibile. Essi vivono, piuttosto, quali frammenti di elettricità veicolati attraverso contenitori, dai quali il dato può essere estratto mediante complesse operazioni tecniche*» (Pittiruti, Digital evidence *e procedimento penale*, cit., 4). A tal proposito, si v, anche Tonini, *L'evoluzione delle categorie tradizionali: il documento informatico*, in *Cybercrime*, diretto da Cadoppi, Canestrari, Manna, Papa, cit.,1313, il quale sostiene che «*il tratto caratterizzante del documento informatico non sta nella immaterialità; non è questo il fulcro della differenza rispetto al documento tradizionale. La vera diversità è stata colta da quegli studiosi che hanno definito "dematerializzato" il documento informatico; ed in effetti l'aggettivo si adatta alla particolarità di questo tipo di documento. Infatti, l'incorporamento digitale costruisce un documento che esiste indifferentemente dal supporto fisico sul quale è incorporato, anche se per la sua esistenza richiede comunque l'incorporamento su di una qualche base materiale. La caratteristica ed anche la peculiarità del documento informatico è quella di essere veicolato su di uno strumento virtuale, il file, ed è questo ad essere incorporato su di una base materiale. Ecco perché il documento informatico deve essere definito come "dematerializzato"*».

non siano *trattate* con le competenze adeguate[33].

Per conseguenza, è connaturato allo specifico mezzo di prova il rischio di relativa dispersione e/o di danneggiamento del contenuto rappresentativo, con evidenti riflessi negativi in punto di genuinità del relativo risultato probatorio e, quindi, della sua attendibilità ai fini decisori.

Pertanto, è incontestabile che l'informatica forense si presenti come una scienza in costante e veloce mutamento, che necessità di una regolamentazione compiuta del relativo fenomeno probatorio nella prospettiva, per l'appunto, di fronteggiare adeguatamente l'esigenza di individuare quale sia la tecnica più idonea per l'acquisizione e l'assunzione dei relativi *dati* a contenuto informativo[34].

In proposito, va detto che gli esperti di indagini digitali ritengono che il trattamento del dato informatico – nella prospettiva di renderlo valido ed utilizzabile ai fini processuali – si componga di quattro fasi: l'individuazione, l'acquisizione, l'analisi e la valutazione del reperto informatico, che devono avvenire osservando procedure idonee a ridurre il rischio di alterazione dei dati originali e, per effetto, a garantire la conservazione del relativo elemento probatorio [35].

In altri termini, "la modalità per preservare il dato informatico e garantirne l'autenticità è costituito dal rispetto della *chain of custody*, vale a dire il tracciare il procedimento di repertamento ed analisi mediante report, così da escludere alterazioni indebite delle tracce informatiche intervenute successivamente alla creazione, trasmissione o allocazione in altro supporto. In tal modo si consente ad accusa e difesa di esperire le relative indagini,

[33] In tema, ancora, v. Pittiruti, Digital evidence *e procedimento penale*, cit., 11, il quale afferma che «*a titolo d'esempio, un file comune, quale una immagine in formato jpg, comprende circa un milione di bit; la modifica di uno solo di essi può comportare un mutamento irreversibile, tanto che il file potrà apparire illeggibile o corrotto. Perché il dato sia alterato, è sufficiente che venga aperto una sola volta: quantomeno, infatti, sarà stato modificato il metadato relativo alla data di ultimo accesso, con il rischio che ne venga annullata la rilevanza probatoria*».

[34] «*Non esiste una metodologia condivisa per il trattamento delle prove digitali, ma vengono utilizzati un insieme di strumenti e talune procedure consolidatesi nella prassi con la sperimentazione. In un'indagine informatica, per le cognizioni tecniche implicate, è necessariamente coinvolta una molteplicità di figure professionali (ufficiali e agenti di polizia giudiziaria; ausiliari di polizia giudiziaria; consulenti tecnici, periti, esperti informatici). L'obiettivo principale di un'indagine in ambito digitale è la preservazione, l'identificazione e la documentazione delle attività che sono state compiute con un sistema informatico o telematico al fine di acquisire la prova della colpevolezza o dell'innocenza dell'indagato*» (Cuomo, *La prova digitale*, in *Prova scientifica e processo penale*, cit., 674).

[35] Per una disamina più approfondita delle singole fasi del trattamento del reperto informatico, v. Aterno, *Acquisizione e analisi della prova informatica*, in *La prova scientifica nel processo penale*, a cura di Tonini, cit., 63-64.

consulenze e valutazioni su un dato che risulta genuino e perfettamente cristallizzato"[36].
Ed è in tale ottica che si inquadra, seppur con colpevole ritardo, l'adozione della succitata l. 18 marzo 2008, n. 48, con la quale il legislatore -ratificando la Convenzione del Consiglio d'Europa sulla criminalità informatica, sottoscritta a Budapest il 23 novembre 2001- introdusse una disciplina specifica proprio in tema di acquisizione e conservazione degli elementi di prova digitali.

4. Il "ritardo" del legislatore e le spinte a matrice sovranazionale.

La l. 18 marzo 2008, n. 48 rappresenta, come già accennato in precedenza, la *risposta* che il legislatore ha fornito rispetto all'esigenza di avere regole specifiche che fossero, perlomeno in potenza, in grado di garantire la conservazione e la non alterabilità del dato informatico.
La rilevanza del testo normativo in discorso emerge anche considerando che nonostante lo sviluppo tecnologico necessitasse già da tempo di un intervento legislativo atto a disciplinare le modalità di acquisizione ed assunzione in giudizio delle prove digitali, il legislatore era rimasto sostanzialmente inerte[37].
Infatti, l'invito a legiferare sullo specifico tema è giunto dalla comunità internazionale con la sottoscrizione della Convenzione di Budapest del 2001, che contiene disposizioni in materia tanto di diritto penale sostanziale, con riguardo all'area dei reati informatici, quanto di diritto processuale, con l'introduzione di plurime prescrizioni relative all'acquisizione, raccolta e conservazione delle prove digitali.
Non è questa la sede per un'analisi approfondita in ordine a tutte le modifiche al codice di procedura penale intervenute con l'entrata in vigore della prefata l. 18 marzo 2008, n. 48. Tuttavia, vale, in ogni caso, segnalare che la principale novità che venne introdotta con la

[36] Giunchedi, *Le* malpractices *nella* digital forensics *Quali conseguenze sull'inutilizzabilità del dato informatico?*, in *Arch. pen.*, 2013, 3, 826.
[37] «[…] *l'evoluzione legislativa non ha seguito di pari passo quella tecnologica. La prima innovazione codicistica frutto dell'incontro tra macchina giudiziale e tecnologia informatica e telematica risale al 1993; segnatamente, il riferimento è alla creazione dell'art. 266-bis c.p.p., relativo all'intercettazione di comunicazioni informatiche o telematiche, all'interno del Libro III sulle prove. Tale modifica, però, è rimasta a lungo isolata: si è dovuto attendere ben quindici anni, allorché la L. n. 48/2008 ha provveduto ad un più generale, sia pur lacunoso, tentativo di sistemazione della materia mediante una serie di interpolazioni ad hoc*» (Pittiruti, Digital evidence *e procedimento penale*, cit., 5).

normativa in discorso coincise con l'inserimento nel codice di rito -attraverso la modifica di alcune disposizioni in tema di ispezioni, perquisizioni e sequestri- delle cc.dd. *best practices* in materia di prove informatiche, ossia "di quel comportamento, non necessariamente codificato o contenuto in manuali, che è ritenuto dalla comunità scientifica e dagli operatori tecnici come la modalità corretta per effettuare determinate operazioni informatiche su specifici dispositivi o supporti"[38].

Segnatamente, per quanto qui rileva, il legislatore, per un verso, ha prescritto agli *addetti ai lavori* il dovere di conservare inalterato il dato informatico originale, nonché di impedirne l'alterazione successiva: nello specifico, l'art. 244, 2° co., – così come modificato dalla l. 18 marzo 2008, n. 48- impone che i «rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica» possano essere disposti anche in relazione a sistemi informatici o telematici, purché vengano adottati «misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

Analogamente, il *nuovo* art. 247, co. 1-*bis*, c.p.p. impone l'osservanza della medesima prescrizione in occasione dell'esecuzione di perquisizioni di sistemi informatici o telematici, che siano disposte quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino al loro interno[39].

Stando così le cose, è evidente che il *target* sotteso allo specifico intervento normativo era quella di "preservare la scena criminis informatica sia nei casi sempre più frequenti di rinvenimento di sistemi informatici/telematici o smartphone accesi e collegati alla rete internet, sia nelle diverse ipotesi di rinvenimento di un personal computer spento"[40].

Per altro verso, la l. 18 marzo 2008, n. 48 ha imposto che in caso di sequestro disposto dall'autorità giudiziaria *ex* art. 254-*bis* c.p.p. o di accertamenti urgenti posti in essere su iniziativa della polizia giudiziaria, aventi ad oggetto ovviamente dati informatici, occorre

[38] Colaiocco, *La rilevanza delle* best practices *nell'acquisizione della* digital evidence *alla luce delle novelle sulla cooperazione giudiziaria*, in *Arch. pen. web*, 2019, 1, 2.

[39] La garanzia della conservazione e non alterazione del dato informatico originale è prescritta anche dagli artt. 352, comma 1-*bis* e 354, comma 2, c.p.p. in sede di perquisizioni ed accertamenti urgenti posti in essere su iniziativa della polizia giudiziaria.

[40] Aterno, *La convenzione di Budapest del 2001 e la l. n. 48/2008*, in *Cybercrime*, diretto da Cadoppi, Canestrari, Manna, Papa, cit., 1356, il quale precisa, sul punto, che «*è di facile comprensione infatti la differenza che intercorre tra l'ipotesi in cui si rinviene un sistema informatico spento oppure che quest'ultimo si trovi acceso e funzionante o che per le sue qualità e funzioni sia impossibile da sequestrare o da spegnere. È soprattutto i questa ipotesi che può parlarsi più correttamente di perquisizione informatica o di ispezione e di applicazione dell'art. 247 o 244 c.p.p.*. […] *Durante un'attività di perquisizione dmiciliare, in caso di ritrovamento di un personal computer spento, si deve procedere ad un comunissimo sequestro del sistema* […]».

procedere alla realizzazione, ove possibile, di un duplicato dell'elemento di prova digitale, «mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità»[41].

Pertanto, se il tentativo di adeguamento regolamentare compiuto dal legislatore è parso

[41] A tal proposito, in dottrina vi è chi ha precisato che le suspecificate peculiarità delle prove digitali impongano di ritenere che il vincolo di indisponibilità disposto con il sequestro, ricada sul documento informatico contenuto all'interno di un dato supporto, e non sul supporto stesso: «*ne deriva che quando l'oggetto fisico (*hardware*) è restituito, ed è conservata sotto sequestro la copia clone, è quest'ultima ad essere il vero oggetto del sequestro*». Quanto detto determina che anche in caso di restituzione del supporto in origine sequestrato -e trattenimento da parte del pubblico ministero della copia forense del sistema informatico- vi è, in ogni caso, l'interesse dell'indagato ad impugnare lo specifico provvedimento cautelare (Tonini, *Manuale di procedura penale*, Milano, 2013, 392). Sennonché, sullo specifico punto non vi è concordanza di vedute in giurisprudenza. In proposito, da un lato v. Cass., Sez. un., 24 aprile 2008, Tchmil, in *Mass. Uff.*, 239397, che ha sancito che «*l'avvenuta restituzione del bene sequestrato rende inammissibili, per sopravvenuta carenza di interesse, la richiesta di riesame del sequestro probatorio e l'eventuale successivo ricorso per cassazione. Con la restituzione della documentazione sequestrata, anche se accompagnata dall'estrazione di copia della stessa, il provvedimento limitativo del diritto sulla cosa si è già esaurito e l'interessato non ha più alcuna ragione specifica per attivare o coltivare la procedura incidentale, funzionale esclusivamente a rimuovere le misure restrittive per le quali non sussistono i requisiti richiesti dalla legge*»; dall'altro lato, v., Cass., sez. un., 20 luglio 2017, Andreucci, in *Mass. Uff.*, 270497, che ha distinto tra dato informatico e supporto su cui esso era originariamente immagazzinato: infatti, «*sulla base delle disposizioni in precedenza esaminate e delle diverse esigenze investigative che rendono necessario il sequestro, la distinzione tra "copia-immagine" (o "clone") e semplice copia non sembra sufficiente per definire i termini della questione, dovendosi anche distinguere i casi in cui la apprensione riguardi, essenzialmente, il dato informatico in relazione al suo contenuto, in quanto rappresentativo di atti o fatti, dunque quale vero e proprio documento, la cui particolarità è data soltanto dalle modalità di acquisizione e conservazione. In definitiva, alla luce delle considerazioni sopra esposte, riguardo ai dati ed ai sistemi informatici possono verificarsi diverse situazioni, in precedenza individuate, rispetto alle quali il sequestro probatorio, secondo le diverse necessità, può colpire il singolo apparato, il dato informatico in sé, ovvero il medesimo dato quale mero "recipiente" di informazioni. Se, per quanto riguarda la prima ipotesi, è indubbio che l'interesse ad ottenere la restituzione va riferito all'intero apparato o sistema in quanto tale, perché specifico oggetto del sequestro, nella seconda, invece, la materiale apprensione riguarda il dato come cristallizzato nel "clone" identico all'originale e, perciò, da esso indistinguibile, perché riversato nella "copia immagine" solo per preservarne l'integrità e l'identità alle condizioni in cui si trovava al momento del prelievo e consentire successive verifiche o accertamenti tecnici. In tale caso l'interesse alla restituzione riguarda, appunto, il dato in sé e non anche il supporto che originariamente lo conteneva o quello sul quale è trasferito il "clone", sicché la mera restituzione del supporto non può considerarsi come esaustiva restituzione della cosa in sequestro; e ciò trova conferma anche nella ricordata definizione di "sequestro" offerta dalla convenzione di Budapest. Diverso è invece il caso in cui un atto o un documento si presenti sotto forma di dato informatico, non rilevando, in tali casi, il dato in sé, bensì quanto in esso rappresentato, come avviene per i documenti cartacei, ben potendosi distinguere, in tali casi, le copie dall'originale, che in questo caso sarà rappresentato dal documento elettronico originariamente formato ed univocamente identificabile. Se questa è, dunque, la distinzione che deve operarsi, è evidente che nei primi due casi ipotizzati non può trovare applicazione l'art. 258 c.p.p., che riguarda espressamente i documenti, mentre tale disposizione andrebbe considerata quando il dato informatico può essere ricondotto entro la nozione di atto o documento, nel qual caso andrebbero apprezzate le conclusioni cui è pervenuta la sentenza Tchmil.*». Ne consegue, pertanto, che negli altri casi, in cui viene in rilievo il documento informatico in sé « la restituzione non può considerarsi risolutiva, dal momento che la mera reintegrazione nella disponibilità della cosa non elimina il pregiudizio, conseguente al mantenimento del vincolo sugli specifici contenuti rispetto al contenitore, incidente su diritti certamente meritevoli di tutela, quali quello alla riservatezza o al segreto», tanto che permane comunque un interesse all'impugnazione del provvedimento ablativo per la verifica della sussistenza dei presupposti applicativi.

apprezzabile nella delineata prospettiva di individuare contromisure che fossero idonee a proteggere l'intrinseca fragilità del dato informatico, comunque la disciplina introdotta dalla l. 18 marzo 2008, n. 48 non si presenta esaustiva (anche e soprattutto) ove si consideri che si compone di plurime *leges impefectae*, prive della comminatoria di specifiche sanzioni processuali nel caso di mancato rispetto delle suspecificate procedure modali[42], che tendono a garantire la tutela della genuinità dei *dati* digitali[43].

5. I futuribili: l'intelligenza artificiale ed il *due process of law*.

La breve ricognizione sin qui compiuta impone perlomeno di segnalare che l'interazione fra l'innovazione tecnologica ed il sistema giustizia, in genere, e quello processuale penale[44], in particolare, costituisce oramai un *acquis* -non solo per chi ne studi i relativi fondamenti ed implicazioni, ma anche per chiunque operi nel settore[45].

In proposito, non è a discutersi che la *guidance* sia, al contempo, multilivello e multifattoriale, attenendo tanto ai rinnovati requisiti organizzativi dell'ordinamento e dello strumento processuale, quanto alle tendenze efficientiste da cui il sistema penale (e non solo) è permeato, quanto ancora alla metodica epistemologica propria della giurisdizione

[42] Lupària, *la ricerca della prova digitale tra esigenze cognitive e valori costituzionali*, in *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, cit., 158 ss.

[43] Sul punto, tra le tante, v. Cass., sez. V, 3 marzo 2017, L.R.V.M., in *Cass. pen.*,2017, 12, 446, secondo cui «*la disciplina contenuta nell'art. 354, comma 2, c.p.p., che ha come unico ambito applicativo l'attività della polizia giudiziaria sul luogo e sulle tracce del reato, prevede l'obbligo di adottare modalità acquisitive idonee a garantire la conformità dei dati informatici acquisiti a quelli originali; ne deriva che la mancata adozione di tali modalità non comporta l'inutilizzabilità dei risultati probatori acquisiti, ma la necessità di valutare, in concreto, la sussistenza di eventuali alterazioni dei dati originali e la corrispondenza ad essi di quelli estratti*». In relazione a quanto affermato sul punto in dottrina, v. Colaiocco, *La rilevanza delle* best practices *nell'acquisizione della* digital evidence *alla luce delle novelle sulla cooperazione giudiziaria*, cit., 3 ss.; Conti, *La prova informatica e il mancato rispetto delle* best practice: *lineamenti sistematici sulle conseguenze processuali*, cit.,1329 ss.; Giunchedi, *Le* malpractices *nella* digital forensics *Quali conseguenze sull'inutilizzabilità del dato informatico?*, in *Arch. pen.*, 2013, 3, 821 ss..

[44] Sul punto, per gli interessanti spunti anche di natura metodologica, Nieva-Fenoll, *Intelligenza artificiale e processo*, trad. Comoglio, Torino, 2019, 11 ss.; di recente, anche per gli ulteriori riferimenti dottrinali, Riccio, *Ragionando su intelligenza artificiale e giusto processo*, in *www.archiviopenale.it*.

[45] In tema. v. Piana, *Giusto processo in trasformazione*, in *Giusto processo e intelligenza artificiale*, a cura di Castelli-Piana, Santarcangelo di Romagna, 2019, pp. 13 ss.

penale che si presenta, oramai da anni[46], come un *cantiere mobile* in perdurante cammino. Al riguardo, seppur con autolimitazione, si impongono, a tutta prima, almeno due questioni, legate alla diffusione applicativa al fenomeno processuale penale dell'intelligenza artificiale (d'ora innanzi, IA)[47], la cui intrinseca imperscrutabilità dà luogo a non poche fibrillazioni rispetto alla congrua protezione dei diritti giudiziari riconosciuti, in genere, alle parti del processo ed, in particolare, all'imputato[48] dalla Costituzione e dalle Carte sovranazionali dei diritti umani[49].

Sotto il primo aspetto, sono perlomeno due le aree in cui si sta consolidando l'uso dei *tools* di IA – il cui impiego, quale possibile ausilio giurisdizionale, rinverrebbe la propria base legale in alcune disposizioni legislative[50] – volendosi escludere scientemente la fase relativa alla prevenzione, nella quale si sta diffondendo progressivamente, per l'appunto, l'impiego di strumenti di *predictive policing*[51].

[46] Lupària, *Processo penale e scienza informatica: anatomia di una trasformazione epocale*, in *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, cit., 127 ss.;

[47] L'intelligenza artificiale «*è alla base di tutte le ricerche su Internet e di tutte le app; è in ogni richiesta fatta al GPS, in ogni videogame o film d'animazione, in ogni banca e compagnia di assicurazione, in ogni ospedale, in ogni drone e in ogni auto a guida autonoma, e in futuro – questa la previsione di una delle massime esperte della materia – "ce la ritroveremo dappertutto": e, ovviamente, anche in ambiti che hanno immediata rilevanza per il diritto penale*» (Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Dir. pen. e uomo*, 2019, 10, 2).

[48] Quattrocolo, *Equità del processo penale e* automated evidence *alla luce della Convenzione europea dei diritti dell'uomo*, in *Revista Italo-Española de Derecho Procesal*, 2019, 3 ss.

[49] Non è invalsa una definizione universalmente riconosciuta di intelligenza artificiale; di contro, si rilevano alcune specificità che connotano, per l'appunto, i sistemi di IA. In proposito, l'analisi di tali elementi classificatori ha spinto la Commissione europea a tentare un inquadramento, quantomeno dal punto di vista definitorio di essa. Segnatamente, l'IA «*indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi. I sistemi basati sull'IA possono consistere solo in software che agiscono nel mondo virtuale (per esempio assistenti vocali, software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale); oppure incorporare l'IA in dispositivi hardware (per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle cose)*». In tal senso, v. *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al comitato delle regioni. L'intelligenza artificiale per l'Europa*, in https://eur-lex.europa.eu, 2018, 1. Sulla relazione tra prova penale e IA, v. Lupària,, *Prova giudiziaria e ragionamento artificiale: alcune possibili chiavi di lettura*, in *Il concetto di prova alla luce dell'intelligenza artificiale*, a cura di J. Sallantin e J.-J. Szczeciniarz, Milano, 2005, XIV ss.; Parodi, Sellaroli, *Sistema penale e intelligenza artificiale: molte esperienze e qualche equivoco*, in *www.dirittopenalecontemporaneo.it*

[50] Al riguardo, tra gli altri, Riccio, *Ragionando su intelligenza artificiale e giusto processo*, cit., 1, secondo il quale, «*vuoi sul terreno del procedimento probatorio, vuoi nel campo della discrezionalità decisoria*», l'uso dell'IA e, quindi, il sistema "predittivo" «*troverebbe conferma*, in primis*, nell'art. 65 dell'Ordinamento giudiziario, che, nell'indicare le attribuzioni della Corte di cassazione afferma che questa "assicura l'esatta osservanza e l'uniforme interpretazione della legge, l'unità del diritto oggettivo nazionale, il rispetto dei limiti delle diverse giurisdizioni"*».

[51] In tal senso, v. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre del risk assestment tool tra Stati Uniti ed Europa*, in www.penalecontemporaneo.it. A tale specifico riguardo, Galgani, *Considerazioni sui "precedenti" dell'imputato e del giudice al cospetto dell'IA nel processo penale*,

In proposito, si ha riguardo sia all'ambito investigativo e probatorio, delle *automated o digital evidence* che – per lo più in chiave prospettica- agli strumenti basati sull'IA, di cui si fa uso nella cosiddetta giustizia latamente "predittiva"[52]: il riferimento, in prospettiva esemplificativa, è all'analisi di un numero rilevante di pronunce giudiziali effettuato tramite tecnologie di IA – che consentirebbe di formulare previsioni potenzialmente affidabili circa l'esito di alcune specifiche tipologie di controversie- così come alla diffusione dei c.d. *risk assessments tools* (*id est*, gli strumenti computazionali, fondati sull'IA, che calcolano il rischio che il prevenuto si sottragga al processo o commetta dei reati)[53].

Sennonché, a fronte della diffusione di strumenti di giustizia digitale e predittiva, la questione che si impone consiste nel chiedersi se le garanzie del giusto processo possano essere, oltre che salvaguardate, addirittura rafforzate a fronte di una *governance* della giustizia digitale che sottoponga i nuovi strumenti a controlli, meccanismi di *check and balance* e di *accountability* ovvero se, di contro, l'applicazione di tali dispositivi collida irrimediabilmente con il diritto all'accesso alle razionalità *decidendi* di cui ognuno è titolare, così come con l'effettività delle guarentigie difensive latamente intese[54].

In proposito, va sottolineato, in via ricognitiva, che, nell'ambito del Consiglio di Europa, la Commissione europea per l'efficienza della giustizia (CEPEJ) -nel dicembre del 2018- ha adottato la Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi

---

in *Sist. Pen.*, 2020, 4, 81 ss.; Riccio, *Ragionando su intelligenza artificiale e giusto processo*, cit., 7, fa rilevare che «*non tutti i* tools di predective policing *risultano indifferenti al processo penale*» ove si considerino i «*software di riconoscimento facciale, oramai ad un passo dal nuovo (qui nel senso di attuale, contemporaneo) processo penale*», avendo specifico riguardo a *Sicurezza4P*, primo sperimento algoritmico creato dalla Questura di Napoli. A tale ultimo riguardo, v. Lombardo, *Sicurezza 4P*, Napoli, 2010.

[52] Viola, voce *Giustizia predittiva, in Enc, giur.*, www.treccani.it, *Diritto on line*, 2018.

[53] In proposito, v. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre del risk assestment tool tra Stati Uniti ed Europa*, in www.penalecontemporaneo.it, il quale, inoltre, specifica che «*Si tratta di veri e propri algoritmi* "that use socioeconomic status, family background, neighborhood crime, employment status, and other factors to reach a supposed prediction of an individual's criminal risk, either on a scale from "low" to "high" or with specific percentages". *Questi strumenti analizzano un numero molto elevato di dati relativi al passato e individuano delle ricorrenze (ossia dei pattern), caratterizzate da una base statistica molto più solida di quelle che stanno al fondo dei giudizi umani*». In tema, tra gli altri, v. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, cit., 4 ss., secondo il quale l'IA potrebbe essere impiegata nelle seguenti attività: «*1. le attività di* law enforcement*, in particolare le attività di c.d. polizia predittiva; 2. i c.d.* automated decision systems*, che potrebbero in futuro conoscere un impiego anche all'interno dei procedimenti penali, sostituendo, in tutto o in parte, la decisione del giudice-uomo; 3. i c.d. algoritmi predittivi, impiegati per valutare la pericolosità criminale di un soggetto, vale a dire la probabilità che costui commetta in futuro un (nuovo) reato; 4. infine, le possibili ipotesi di coinvolgimento - come strumento, come autore, o come vittima - di un sistema di IA nella commissione di un reato*»

[54] Nieva-Fenoll, *Intelligenza artificiale e processo*, cit., 118 ss.

giudiziari e negli ambiti connessi[55].

Nello specifico, la Carta contiene "disposizioni senza dubbio eterogenee, nelle quali si rinvengono norme di diritto positivo, forme di *soft law* e mere raccomandazioni di esperti, ma che tuttavia costituiscono un primo corpus con funzioni di orientamento e regolazione sia delle policIies pubbliche che dell'attività degli stakehoIlders coinvolti e si agglutinano attorno ad un nucleo di principi già sufficientemente delineati nella prospettiva di tutela dei diritti fondamentali, per quanto le soluzioni proposte non sempre siano in grado di sciogliere tutti i nodi complessi di una realtà dall'impatto oggettivamente non ancora del tutto prevedibile"[56].

Segnatamente, si ha riguardo a cinque principi generali, di natura, al contempo, sostanziale e metodologica, da applicarsi al trattamento automatizzato delle decisioni e dei dati giudiziari: *1)*-l'uso degli strumenti di IA in ambito processuale deve avvenire garantendo il diritto di accesso al giudice ed a un processo equo e, quindi, assicurando la parità di armi ed il rispetto del contraddittorio (*principle of respect for fundamental rights*); *2)*-è sancito il canone di non discriminazione: infatti, i soggetti pubblici e privati, stante la capacità dei metodi di elaborazione di rivelare le discriminazioni esistenti, devono garantire che i *tools* di IA non riproducano o aggravino tali discriminazioni, conducendo ad analisi deterministiche (*principle of non-discrimination*); *3)*-è raccomandato l'uso esclusivo, per assicurare la qualità e la sicurezza, di dati -in particolare, decisioni giudiziarie- acquisiti da fonti certificate attraverso un processo tracciabile; inoltre, è doveroso che i modelli e gli algoritmi realizzati siamo eseguiti e memorizzati in ambienti sicuri, a garantire dell'integrità del sistema (*principle of quality and security*); *4)*-è imposta la trasparenza, l'imparzialità e la correttezza dei modelli e degli algoritmi; in proposito, l'accessibilità al processo algoritmico deve prevalere sui diritti di privativa connessi alla tutela della proprietà intellettuale; inoltre, va assicurata l'assenza di pregiudizi e l'integrità intellettuale (*principle of transparency, impartiality and fairness*).; *5)*-è sottolineata la centralità dell'utente, la cui libertà di scelta deve essere preservata, tanto da essere escluso un approccio prescrittivo dell'impiego dell'IA ed assicurato agli utilizzatori di agire come

[55] European Commission for the efficiency of Justice, *European ethical charter on the use of Artificial Intelligence in judicial systems and their environment*, 3-4 dicembre 2018, 4-5. In tema, v. Quattrocolo, *Intelligenza artificiale e giustizia: nella cornice della Carte etica europea gli spunti per un urgente discussione tra scienze penali e informatiche*, in www.legislazionepenale.it

[56] Ziroldi, *Intelligenza artificiale e processo penale tra norme, prassi e prospettive*, in *www.questionegiustizia.it*.

soggetti informati, avendo inoltre il pieno controllo delle loro scelte (*principle under user control*). In particolare, il giudice deve poter controllare in qualsiasi momento le decisioni giudiziarie e i dati che sono stati utilizzati per produrre un risultato e continuare ad avere la possibilità di discostarsi dalle soluzioni proposte dall'IA, tenendo conto delle specificità del caso in questione; del pari, ogni utente deve essere informato, in un linguaggio chiaro e comprensibile, della natura vincolante o non vincolante delle soluzioni proposte dagli strumenti di IA, delle diverse opzioni disponibili e del loro diritto all'assistenza di un avvocato ed al ricorso a un tribunale[57].

Quanto sin qui detto fa da *pendant* con la constatazione che in ambito U.E., la Commissione -per assicurare lo sviluppo di un'intelligenza artificiale affidabile- nel dicembre 2018 ha pubblicato le *Draft Ethics Guidelines for Trustworthy AI*,[58] che sono state elaborate da un gruppo di esperti ad alto livello sull'IA (*AI HLEG*) e aperte alla consultazione pubblica e che, tra l'altro, hanno dichiaro imprescindibile un approccio antropocentrico all'IA, garantendo alle persone sempre il potere di supervisione sulle macchine[59].

---

[57] Va detto che nella Prima appendice alla succitata Carta etica si leggono, tra le altre, condivisibili riflessioni ragionate in ordine alla criticità coeve al ricorso alle statistiche ed all'intelligenza artificiale nei procedimenti penali. Segnatamente: «*sebbene non sia appositamente progettato per essere discriminatorio, il ricorso alle statistiche e all'intelligenza artificiale nei procedimenti penali ha dimostrato che sussiste il rischio di incoraggiare la recrudescenza di dottrine deterministiche a scapito delle dottrine di individualizzazione della pena che sono state ampiamente acquisite a partire dal 1945 nella maggior parte dei sistemi giudiziari europei*» e che «*alla luce di quanto esposto precedentemente, appare essenziale, quando gli algoritmi sono utilizzati nel contesto di un processo penale, garantire il pieno rispetto del principio della parità delle armi e della presunzione di innocenza di cui all'articolo 6 della CEDU. La parte interessata dovrebbe avere accesso all'algoritmo ed essere in grado di contestarne la validità scientifica, il peso attribuito ai vari elementi e le eventuali conclusioni erronee cui è pervenuto ogniqualvolta un giudice suggerisce che potrebbe utilizzarlo prima di adottare la sua decisione. Tutte le persone hanno diritto a non essere sottoposte a una decisione che incide significativamente sulla loro persona, adottata unicamente sulla base di un trattamento automatico di dati, senza che si tenga preliminarmente conto del loro punto di vista*» (Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi, in *https://rm.coe.int*, 37-38). Invece, nella Seconda appendice, si auspica che l'impiego dei *risk assestment tools* -considerati i deprecabili effetti discriminatori e deterministici che essi hanno avuto negli Stati Uniti e nel Regno Unito (in particolare, si compie un riferimento testuale agli «*esperimenti…(COMPAS negli Stati Uniti e HART nel Regno Unito)*» che «*sono stati criticati da alcune ONG (si vedano i lavori di ProPublica negli Stati Uniti e di Big Brother Watch nel Regno Unito)*»- avvenga «*con le più estreme riserve*» Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi, in *https://rm.coe.int*, 44).

[58] Sul tema "*Intelligenza artificiale, ecco le nuove linee guida dell'Europa*", in *www.nova.ilsole24ore.it*, 8 aprile 2019. Sul punto, Bolognini, "*Codice etico UE sull'intelligenza artificiale: forte la tecnica, debole la politica",* in *www.focus.it*, il quale sottolinea che il codice non contiene norme cogenti, ma risulta aperto all'adesione volontaria da parte di governi, ricercatori e imprese. Pertanto, linee guida condivisibili sul piano tecnico, ma dotate di scarsa valenza su quello economico-politico.

[59] Le specifiche Linee Guida possono leggersi in *https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai*. Esse muovono dalla consapevolezza che l'IA può generare rilevanti vantaggi per gli individui e per la società, ma dà luogo anche a determinati rischi che vanno gestiti in maniera adeguata, assecondando un'ottica di massima riduzione di essi. In tale contesto, come accennato, è stata

Inoltre, a livello di diritto derivato, alcune garanzie fondamentali riguardo all'uso di *tools* di *risk assessment* si rinvengono nel *data protection reform package*, che si compone del regolamento 2016/679/UE (GDPR) e della direttiva 2016/680/UE[60].

Segnatamente, la direttiva 2016/680/UE è la fonte di riferimento per scrutinare quali potrebbero essere gli ambiti applicativi dei *risk assessment tools* nel procedimento penale: infatti, essa si atteggia a *lex specialis* rispetto al regolamento, ponendo norme minime relative alla "protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica"[61].

Pertanto, la norma fondamentale è l'art. 11 della medesima direttiva -rubricato «Processo decisionale automatizzato relativo alle persone fisiche» – che pone il divieto di decisioni che siano basate unicamente su trattamenti automatizzati, sancendo che «gli Stati membri dispongono che una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici negativi o incida significativamente sull'interessato sia vietata salvo che sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che preveda garanzie adeguate per i diritti e le libertà dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento».

Sennonché, la disposizione *de qua* -il cui contenuto è analogo a quello dell'art. 22 del regolamento 2016/679/UE (GDPR) – ha una *formulazione ambigua* che ruota intorno all'interpretazione dell'espressione «decisione basata unicamente su un trattamento automatizzato».

In proposito, la direttiva vieta le decisioni nelle quali non vi sia alcun coinvolgimento umano nel processo decisionale, qualora producano effetti giuridici che riguardano l'interessato o che incidano in modo analogo significativamente sulla sua persona; pertanto,

---

affermata la necessità di un approccio antropocentrico all'IA, assicurando alle persone sempre il potere di supervisione sulle macchine. Infatti, si legge che: «*AI is human-centric: AI should be developed, deployed and used with an "ethical purpose" (...), grounded in and reflective of fundamental rights, societal values and the ethical principles of Beneficence (do good), Non-Maleficence (do no harm), Autonomy of humans, Justice, and Explicability*».

[60] Il regolamento 2016/679/UE (GDPR) e la direttiva 2016/680/UE hanno sostituito, rispettivamente, la direttiva 95/46/CE, ritenuta il pilastro in materia di protezione dei dati personali, e la decisione quadro 2008/977/GAI.

[61] Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre del risk assestment tool tra Stati Uniti ed Europa*, cit., 16.

essa richiede di regola un intervento dell'uomo, con la specificazione che, "per aversi un coinvolgimento umano, il titolare del trattamento deve garantire che qualsiasi controllo alla decisione sia significativo e non costituisca un semplice gesto simbolico"[62].

Breve. Al fine di scongiurare la violazione delle disposizioni sopraindicate (artt. 11 direttiva 2016/680/UE ed art. 22 regolamento 2016/679/UE) il trattamento automatizzato può assolvere, in esclusiva, ad una funzione ausiliatrice dell'uomo, a cui spetta, invece, la decisione[63].

Ad ogni modo, se, di regola, non ci si deve accontentare della riconosciuta centralità dell'intervento umano ma occorre anche che l'elemento cognitivo generato dall'intelligenza artificiale sia confermato da altre fonti e se, come segnalato in precedenza, sia in sede Consiglio d'Europa, che a livello di U.E., sono state poste una serie di regole che salvaguardano il ruolo dell'intelligenza umana nei processi decisionali, tra l'altro, vietando l'uso di *tools* che facciano uso di dati sensibili e siano suscettibili di condurre a discriminazioni, allora è chiaro che la garanzia fondamentale sta nella riconosciuta centralità del giudice a mente dell' 11 della direttiva 2016/680/UE e dell'art. 8, d.lgs. 18 maggio 2018, n. 51, che ha dato attuazione in Italia alla specifica direttiva, ribadendo, per ciò che nello specifico interessa, il divieto di decisioni basate unicamente su un trattamento automatizzato, «compresa la profilazione», qualora producano effetti negativi nei confronti

[62] Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre del risk assestment tool tra Stati Uniti ed Europa*, cit., 17, il quale rileva che «*Questo è il contenuto, per così dire, minimo della disposizione. Per la verità, sembra preferibile una lettura un po' più esigente, secondo la quale, al fine di garantire un intervento effettivo dell'uomo, la stessa decisione non potrebbe basarsi esclusivamente sull'*output *di un meccanismo automatizzato. Insomma, accanto all'obbligo di un intervento umano andrebbe ritenuta sussistente quella che, nel lessico processualpenalistico, chiameremmo regola di valutazione, in forza della quale l'*output *prodotto dall'IA va considerato come un mero indizio, che va sempre corroborato con altri elementi di prova. Questa lettura sembra peraltro confermata dall'eccezione alla regola, contemplata dalla stessa disposizione: si ammette, infatti, che la regola possa essere derogata, a condizione che vi sia una previsione di tutele sufficienti per i diritti personali e che vi sia, quanto meno, un intervento umano*».

[63] Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre del risk assestment tool tra Stati Uniti ed Europa*, cit., 17, il quale sottolinea che «*la stessa interpretazione pare essere alla base del documento della House of Commons proprio sul tema "*Algorithms in decision-making*", con particolare riferimento alla portata della norma analoga dell'art. 22 GDPR: proprio facendo leva su tale interpretazione è stato ritenuto legittimo l'utilizzo del software HART in Inghilterra*». Sul punto, va segnalato che il sistema denominato *Harm Assessment Risk Tool* (HART), è stato utilizzato dal corpo di polizia di Durham a partire dal 2017 in chiave di *diversion* e, quindi, al fine di valutare quando una persona possa essere sottoposta a un *rehabilitation programme*, chiamato *Checkpoint*, il quale costituisce un'alternativa all'esercizio dell'azione penale. In proposito, Oswald-Grace-Urwin-Barnes, *Algorithmic risk assessment policing models: lessons from the Durham HART model and "Experimental" proportionality*, in *Information and Communications Technology Law*, 2018, 227. Ad ogni modo, sul rilievo del controllo umano rispetto alla "macchina" ed al procedimento di calcolo algoritmico, v. anche Parodi, Sellaroli, *Sistema penale e intelligenza artificiale: molte esperienze e qualche equivoco*, cit., 11.

dell'interessato» e che le «disposizioni di legge devono prevedere garanzie adeguate per i diritti e le libertà dell'interessato»[64].

Per tirare le fila del discorso: diritto e giustizia vivono una fase di radicale trasformazione con ineludibili implicazioni a più livelli; la relativa narrazione è in via di graduale consolidamento; il più è ancora da scrivere anche se già si colgono i prodromi di un cambiamento che si *scorge* radicale; in tale contesto, la strada da percorrere non deve essere minata da resistenze preconcette o da aperture acritiche; essa deve essere attraversata da una visione interdisciplinare, che si dimostrerà affidabile solo se garantirà adeguatamente il percorso segnato dalle garanzie definite a livello costituzionale ed europeo. Bisognerà, quindi, pensare estremo, ma agire accorto.

Abstract: Il progresso tecnologico ha *implementato* l'insieme degli strumenti conoscitivi utilizzabili nel procedimento penale, sia nel corso delle indagini preliminari, che nella fase dibattimentale. Tuttavia, la vischiosità della relazione corrente -tra il sapere scientifico ed il tradizionale metodo epistemologico invalso nel processo penale- impone di esaminare alcune questioni problematiche che derivano, anzitutto, dall'imprescindibile verifica di c.d. affidabilità ricostruttiva delle nuove tecnologie. In tale contesto, non può prescindersi da uno sguardo sui c.d. futuribili tenendo conto delle potenzialità connesse con l'uso dell'intelligenza artificiale all'interno del sistema processuale penale.

Abstract: Technological progress has increased the cognitive tools that can be used in criminal proceedings, both during preliminary investigations and in the trial phase. However, the sticky nature of the current relationship -between scientific knowledge and the traditional epistemological method used in criminal proceedings- requires us to examine some of the problematic issues that arise from the essential verification of c.d. reconstructive reliability of new technologies. In this context, it cannot disregard a look at the future c.d. taking into account the potential associated with the use of artificial intelligence within the criminal trial system..

[64] Anche la specifica disposizione è rubricata, per l'appunto, «*Processo decisionale automatizzato relativo alle persone fisiche*»

Parole chiave: Processo penale – giusto processo – prova – prova informatica – intelligenza artificiale – investigazioni digitali.

Key words: Criminal trial – due process – evidence – computer forensics – artificial intelligence – digital investigation.