Revista Ítalo-Española de Derecho Procesal
Vol. 2 | 2019 17 pp.
Madrid, 2018

© ISSN: 2605-5244

EQUITA' DEL PROCESSO PENALE E *AUTOMATED EVIDENCE* ALLA LUCE DELLA CONVENZIONE EUROPEA DEI DIRITTI DELL'UOMO*

Serena Quattrocolo
Professore ordinario di diritto processuale penale
nell'Università del Piemonte orientale

Riassunto: *Lo scritto affronta il tema della parità delle armi a fronte del sempre più frequente impiego di prove generate automaticamente anche nel processo penale. La straordinaria potenza computazionale –a costi ridottissimi– e la proliferazione incontrollata di dati attraverso tecnologie digitali di uso quotidiano generano un substrato conoscitivo ricchissimo ed utilissimo anche per il processo penale. Tuttavia, l'opacità degli algoritmi che regolano la creazione e la raccolta di questi dati rischia di rendere impossibile* in nuce *la difesa dell'imputato, che si trova per lo più nell'impossibilità di accedere, comprendere e validare il processo che ha portato alla produzione del dato. In questo contesto, l'attendibilità della prova generata automaticamente rischia di divenire incontestabile, in violazione della più essenziale concezione di parità delle armi, sancita dalla Convenzione europea dei Diritti dell'Uomo.*

Parole chiave: Processo penale; prova; algoritmo; validazione; squilibrio conoscitivo; attendibilità.

Abstract: *The paper focuses on the topic of the equality of arms, against the frequent use of algorithm-based evidence in criminal proceedings. Actually, the unprecedented and cheap computational power, coupled with the world-wide spread of digital devices, producing uncountable amounts of data, provide a useful base for evidence. However, the opacity of the algorithms generating those data may hinder* per se *the defendant's chance of defence, as she may not be able accessing codes, understanding and validating them. Thus, the trustworthiness of algorithm-based evidence seems to become absolute, without a chance to challenge it, in breach of the essential meaning of the equality of arms, set forth by the European Convention of Human Rights.*

Keywords: Criminal proceeding; evidence; algorithm; validation; knowledge impairment; trustworthiness.

* Il testo riprende, in parte, il capitolo che sarà pubblicato in R. Flor-L. Picotti, *Nuove tecnologie e lotta al (cyber)terrorismo ed al discorso d'odio nella prospettiva europea*, in corso di pubblicazione.

1. INTRODUZIONE

La recente entrata in vigore del GDPR e la trasposizione –avvenuta ormai in molti Stati membri– delle direttive 2016/680 e 2016/681 UE sottolineano con urgenza l'emersione di un tema non certo classico per il processual-penalista, ovvero la generazione e il trattamento automatizzati di dati, personali ma non solo, all'interno del procedimento penale[1]. E se per un verso è innegabile che già da tempo il dibattito dottrinale e giurisprudenziale (anche italiano) si è misurato con il difficile compito di coniugare evoluzione scientifica e "staticità" processuale, rendendo il tema dell'ingresso di nuove tecnologie e saperi scientifici nel procedimento probatorio un argomento ormai paradossalmente classico, per altro verso la stretta attualità impone due ordini di riflessioni, specificamente collegate con il profilo della *digital evidence 2*.

In primo luogo, all'interno di tale concetto, che non ha ancora raggiunto una vera dimensione normativa, ricadono strumenti di captazione e di raccolta di informazioni così invasivi da caratterizzarsi per un'insidiosità massima, ben più elevata di quella propria degli strumenti intercettivi tradizionali[3]. Emblematica, in tal senso, l'osservazione che si ritrova nello studio commissionato dal Libe Committee del Parlamento europeo[4]: «*although the use of hacking techniques will bring improvements in investigative effectiveness, the significant amount and sensitivity of data that can be accessed through these means acts as a stimulus for another key debate: ensuring the protection of the fundamental right to privacy*»[5]. Per questa ragione, il quadro del dibattito circa la loro compatibilità con i principi generali si è sempre concentrato sul profilo della sfera di riservatezza dei singoli, pur con tutto

---

[1] Per una prima analisi integrata della disciplina oggi vigente, v. L. Pulito, *Il trattamento dei dati personali in ambito penale e l'uso del* passenger name record *per contrastare il terrorismo e altri gravi reati*, in *Processo penale e giustizia* 2018, n. 6, p. 1138 ss.

[2] Difficile dar conto in termini esaustivi dell'ampia letteratura, anche solo nazionale, sviluppatasi sul tema dopo l'entrata in vigore della l. 48/2008. Tra gli altri, v.: M. Daniele, *La prova digitale nel processo penale*, in *Riv. Dir. Proc.* 2011, p. 283 ss.; L. Luparia-G. Ziccardi, *Investigazione penale e tecnologia informatica*, Giuffré, Milano, 2007, passim; M. Pittiruti, Digital evidence *e procedimento penale*, Giappichelli, Torino, 2017, passim; G. Vaciago, Digital evidence. *I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'imputato*, Giappichelli, Torino, 2012; G. Ziccardi, *Informatica giuridica. Privacy, sicurezza informatica,* computer forensic *e investigazioni digitali*, spec. vol. 1, Giappichelli, Torino, 2012, passim.

[3] In questo senso, M. Daniele, *La prova digitale*, cit., p. 288: «La loro capacità lesiva della *privacy* è addirittura superiore a quella delle intercettazioni». Ancor più critici, P. Tonini-C. Conti, *Il diritto delle prove penali*, Giuffré 2014, 482, mettono l'intrusione informatica in relazione con il controllo psichico.

[4] Studio commissionato dal Libe Committee del Parlamento europeo e realizzato dal Directorate-General for Internal Policies, *Legal Frameworks for hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices* (reperibile sul sito ufficiale del Parlamento Europeo).

[5] *Legal Frameworks*, cit., p. 21.

il complesso corollario della non lineare evoluzione in termini digitali dei concetti di corrispondenza e, soprattutto, di domicilio… Numerosi elementi, però, fanno ritenere che la riservatezza non sia l'unico diritto fondamentale messo a repentaglio dall'utilizzo nel processo penale di dati trattati e generati automaticamente[6].

Infatti, nell'ultimo decennio si è verificata un'accelerazione inedita nella produzione e nell'elaborazione quotidiana di dati digitali che, secondo una dato corrente, ammonterebbe a 2,5 quinitilioni (cioè 10 alla trentesima) di bytes al giorno, con un ritmo tale da rinnovare in due soli anni il 90% di tutti i dati disponibili nel mondo[7]. Tale smisurato flusso può immettere anche nel procedimento penale elementi conoscitivi di grande impatto, aprendo la strada a derive potenzialmente pericolose, sulle quali pare opportuno promuovere un dibattito autenticamente giuridico, per evitare che l'efficienza tecnologica diventi un criterio autosufficiente di attendibilità della prova[8].

In ragione di queste considerazioni, la prospettiva che qui si propone tende a spostare il *focus* sul profilo della parità delle armi tra le parti a fronte dell'impiego processuale di dati conoscitivi che siano generati e trattati automaticamente, attraverso algoritmi, siano questi più o meno sofisticati, siano specificamente creati, o no, per essere impiegati all'interno del procedimento penale. Tale spunto appare particolarmente significativo con riguardo a tutte le fattispecie penali per le quali, spesso, la prova processuale è rappresentata dalla profilazione automatica di dati personali, non necessariamente sensibili[9], elaborata attraverso strumenti predittivi di stampo bayesiano, potenziati dall'impiego di forme, anche non particolarmente sofisticate, di *learning machines*.

2. IL CONTESTO NORMATIVO EUROPEO DI RIFERIMENTO

Prima di addentrarsi, seppur a grandi linee, in tale problematica, occorre premettere che l'attenzione sarà qui concentrata soltanto sui profili repressivi

---

[6] Grande impatto e seguito ha avuto l'opera di C. O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Random House: New York, 2016, *passim*.

[7] Il dato circola ormai da tempo (v. www.sciencedaily.com, 22.5.2013 e, quasi contemporaneamente, Å. Dragland, *Big Data. For Better or Worse*, in www.sciencenordic.com, 25.5.2013, sito di divulgazione scientifica), talvolta attribuito agli analisti IBM. La proporzione dell'aumento esponenziale nella produzione di dati pare essersi mantenuta costante nell'ultima trentina d'anni: approssimativamente, ogni due anni si producono dieci volte tanto di dati. Si tratta comunque di valori e valutazioni apparentemente non riportati in studi scientifici.

[8] V. già nel lontano 2006, E. Van Buskirk-V.T. Liu, *Digital Evidence: Challenging the Presumption of reliability*, in *Journal of Digital Forensic Practice*, 2006 (1), p. 20: «*Courts have seemingly unflappable faith in the ability of software to render reliable evidence*».

[9] Con riguardo al concetto di libera autodeterminazione informativa –anche rispetto a dati scarsamente caratterizzanti– elaborato dalla Corte costituzionale tedesca, v. R. Flor, *Dalla data retention al diritto all'oblio. dalle paure orwelliane alla recente giurisprudenza della corte di giustizia. quali effetti per il sistema di giustizia penale e quali prospettive de jure condendo?* in *Diritto dell'informazione e dell'informatica*, 2014, p. 780.

del reato e non anche preventivi. E' noto, infatti, come la regolamentazione delle attività investigative orientate a prevenire la commissione di un reato si collochi al di fuori del procedimento penale e, pertanto, nella maggior parte degli ordinamenti, sia laconicamente disciplinata. Si prenda ad esempio l'ordinamento italiano, nel quale l'art. 226 n.att.c.p.p. predispone oggi la regolamentazione delle intercettazioni di comunicazioni, anche telematiche, con finalità preventive anche dei reati di terrorismo, di cui all'art. 51 co. 3-*quater* c.p.p., se commessi con mezzi informatici e telematici. Tuttavia, nel panorama delle attività preventive, si tratta soltanto di uno degli strumenti a disposizione delle autorità che si occupano di *intelligence* all'interno di un quadro che rimane di difficile ricostruzione normativa[10].

E' proprio in tale àmbito che, quanto meno in molti ordinamenti di *common law*, si fa oggi il maggior impiego di algoritmi, elaborati con specifiche capacità predittive del reato e della recidivanza, da impiegarsi nella quotidiana attività di polizia (*patrolling*), nelle decisioni di *bail* e nel *sentencing*[11]. Nel contesto del procedimento penale di stampo anglosassone, lo sviluppo tecnologico ha agevolmente inoculato, al di fuori di un vero e proprio dibattito di matrice giuridica, algoritmi che si sostituiscono al giudizio umano nella prognosi di recidivanza, spostando l'attenzione dal tema centrale della presunzione di innocenza, a quello, non giuridico, della maggior accuratezza predittiva del software[12].

Il prepotente farsi strada di istanze securitarie –propiziato dalla disponibilità di penetranti mezzi di controllo sociale– e il frequente ricorso delle norme processuali a complesse prognosi di recidivanza e, più in generale, di pericolosità, sta producendo una progressiva sfumatura dei confini tra prevenzione e accertamento del reato[13]. Si tratta di un fenomeno che non ha ancora raggiunto, nel contesto europeo, l'adeguata attenzione critica dei

---

[10] Si veda lo studio *Legal Framework*, cit., p. 25 ss. con specifico riguardo al mercato dei c.d. zero-day exploits (che sfruttano, a vario scopo, le vulnerabilità di un sistema informatico prima che vengano a conoscenza del pubblico e dei produttori stessi: v. S.M. Bellovin, M. Blaze, S. Clark, S. Landau, *Lawful Hacking: Using existing vulnerabilities for wiretapping on the Internet*, in *NW. J. Tech. & Intell. Prop.*, 2014 vol. 12, 1, spec. p. 22 ss.), non regolamentato a livello nazionale e spesso impiegato dai governi nazionali per finalità di intelligence, in assenza di un quadro normativo chiaro e di un effettivo dibattito sul tema.

[11] Cfr. A. Liptak, *Sent to prison by a software Program's Secret Algorithm,* in The New York Times, 1° Maggio 2017, in nytime.com

[12] Si veda lo studio del Committee of Experts on Internet Intermediaries del Consiglio d'Europa, *Algorithms and Human Rights. Study on the Human Rights Dimension of Automated Data Processing Techniques and Possible Regulatory Implications,* Edizioni del Consiglio d'Europa, marzo 2018, p. 10 ss. La letteratura, spesso scientifica e non giuridica, in materia inizia ad essere considerevole. Ai limitati fini di questo breve accenno, lo studio segnalato offre una valida panoramica delle principali problematiche in gioco.

[13] La potestà punitiva statuale scivola lentamente nel controllo del rischio sociale, il diritto penale si trasforma in diritto di polizia: v. J. Vervaele, *Surveillance and Criminal Investigation: Blurring of Thresholds and Boundaries in the Criminal Justice System?*, in S. Gutwirth, R, Leenes, P. De Hert (a cura di), *Reloading Data Protection*, Springer, Heidelberg, 2014, p. 116 ss.; C. Cocq – F. Galli, *The catalysing effect of serious crime on the use of the surveillance technologies for prevention and investigation purposes,* in *N. J. Eu. Cr. L.*, 2013, p. 256.

giuristi, ma che necessita di una trattazione ampia e articolata, di cui i temi trattati in questa sede –ovvero la dimensione infraprocedimentale, probatoria, dell'impiego di dati raccolti e generati per mezzo di algoritmi– rappresentano il presupposto logico.

2.1. La tutela offerta alla riservatezza dall'art. 8 Cedu

Il primo e principale problema che si profila sul piano della compatibilità degli strumenti investigativi e probatori 'automatizzati', con i principi fondamentali dell'ordinamento multi-livello –costituito dall'integrazione tra ordine nazionale e circuiti di giustizia europea– è rappresentato proprio dall'estrema intrusività nella sfera individuale dei soggetti sospettati e sottoposti a procedimento penale. La realtà attuale della giustizia penale dimostra la bontà e la generalità dell'assunto che mette in rapporto direttamente proporzionale l'efficacia del mezzo investigativo e la sua intrusività nella vita privata[14]. La raccolta (attraverso la captazione occulta, ma non solo) di dati relativi alla sfera individuale dell'indagato garantisce sempre di più la ricostruzione di abitudini, di interessi, inclinazioni, stili di vita che possono rappresentare un corollario indiziario estremamente importante ai fini processuali. Ciò è reso progressivamente più agevole ed efficace da due fattori: appunto, l'uso quotidiano di supporti digitali che producono, senza costo, quintilioni di *bytes* e la disponibilità di una capacità computazionale rapida ed economica per processare quei dati[15].

E' logico, quindi, che la frizione con i principi generali che tutelano la riservatezza degli individui abbia rappresentato il primo e principale profilo di analisi in letteratura. Nel contesto europeo, il paradigma di riferimento è quello dell'art. 8 Cedu, ispirato al concetto classico di privacy, riconducibile a luoghi e a contesti oggettivamente localizzati. La struttura della previsione si basa su un complesso sistema di bilanciamento tra valori che possono entrare tra loro in contrapposizione, incoraggiando un'elaborazione giurisprudenziale da parte della Corte di Strasburgo assai articolata, che non si può qui ricostruire compiutamente[16]. Per quel che specificamente interessa in questo contesto, occorre ricordare che, nello schema dell'art. 8 Cedu, il diritto alla vita familiare e privata può essere posto in bilanciamento con altri valori

[14] V. lo studio *Legal Framework*, p. 8, ove si riporta la posizione dell'Associazione Internazionale Comandanti di Polizia (International Association Chiefs of Police), i quali affermano di non essere più in grado di indagare sulle più varie attività illecite senza ricorrere a mezzi interecettivi e, in generale, intrusivi dei sistemi informatici e telematici.

[15] U. Pagallo-S. Quattrocolo, *Fair Trial and the Equality of Arms in an Algorithmic Society*, in M.L. Labate Mantovanini Padua Lima- J. Garcez Ghirardi (a cura di), *Global Law. Legal Answers for Concrete Challenges*, Juruà Editorial, Porto, 2018, p. 261 ss.

[16] E' stato peraltro sottolineato come l'approccio della Corte sia riscontrabile anche nella giurisprudenza di numerosi giudici costituzionali nazionali: P. Santolaya, *The right to a private and family life*, in X. Garcìa Loca-P. Santolaya, *Europe of rights: A Compendium on the European Convention of Human Rights*, Marinus Nijhoff, Leiden, 2012, p. 339.

di interesse come ad esempio, la sicurezza nazionale e la prevenzione del disordine e dei reati, nonché la repressione di questi ultimi, a due necessarie condizioni: la previsione per legge e la necessità in una società democratica. Anche la raccolta, l'elaborazione e la profilazione dei dati personali è confluita nella 'classica' cornice normativa dell'art. 8 Cedu, che la Corte ha spesso adattato pure a questa più moderna forma di intrusione nell'ambito della vita privata degli individui, tanto da potersi affermare che, negli ultimi anni, la giurisprudenza 'convenzionale' ha stabilito un substrato di principi e regole comuni per l'utilizzo per finalità di natura penale dei dati personali e della loro elaborazione[17]. Preliminarmente, dunque, occorre osservare che l'uso di tecnologie digitali per captare segretamente dati della vita privata degli individui non è di per sé partica contraria alla Convenzione. Ancora una volta, le condizioni di legittimità convenzionale sono rappresentate dalla necessità e dalla previsione per legge.

La necessità si traduce, nell'insegnamento della Corte, in un «*pressing social need*», condizione necessaria per la giustificazione dell'intrusione nell'area della privatezza individuale, la quale, tuttavia, esprime un valore relativo, poiché necessariamente misurato e misurabile soltanto in relazione all'obiettivo che si intende raggiungere attraverso l'intrusione medesima[18]. Ciò implica che se esistono altri strumenti per garantire lo stesso livello di interesse pubblico, l'autorità deve escludere l'invasione della vita privata, che assume quindi i caratteri del *last resort*, cui può condurre soltanto l'attenta applicazione del principio di adeguatezza.

Quanto al parametro della previsione per legge, la Corte ha superato la difficoltà di un approccio formale che possa ben sposarsi con le specificità di ciascun ordinamento enunciando le caratteristiche che la «previsione per legge» dell'intrusione nella sfera riservata deve possedere, ovvero l'accessibilità[19] e la prevedibilità[20]. Tali requisiti risultano rispettati, secondo la giurisprudenza di Strasburgo, quando ricorrano: un chiaro compendio delle ipotesi in cui i dati personali possono essere utilizzati; una descrizione trasparente delle finalità di tale impiego; la obiettiva delimitazione del potere discrezionale dell'autorità procedente.

Non si può, però, nascondere, in questa breve panoramica, che spesso la Corte finisce per far confluire i due illustrati parametri nella valutazione circa l'esistenza e l'effettività di rimedi giudiziali avverso le intrusioni in questio-

---

[17] Si veda lo studio, ricco e completo, di R. Sicurella – V. Scalia, *Data mining and profiling in the Area of Freedom, Security and Justice*, in *N. J. Eu. Cr. L.*, 2013, 409 ss. In particolare, p. 437.

[18] Sul punto, v. le interessanti riflessioni di F. Caprioli, *Brevi note sul Progetto Gratteri di riforma della disciplina delle intercettazioni*, in *Cass. pen.*, 2017, p. 3984.

[19] In C. eur. *Kokkinakis c. Grecia*, la Corte ha proprio censurato la formulazione della norma nazionale che rendeva impossibile comprendere il significato della previsione restrittiva della riservatezza.

[20] Tale profilo gioca un ruolo essenziale nei rapporti tra art. 8 e art. 6 Cedu (e art. 13), in relazione alle ipotesi in cui l'intrusione nella sfera personale abbia finalità di rilevanza processuale: v. P. De Hert, S. Gutwirth, *Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of Power*, in E. Claes, A. Duff, S. Gutwirth (eds.), *Privacy and the Criminal Law*, Intersentia, Antwerp, 2006, p. 85.

ne[21], finendo per trasformare soprattutto il vaglio di legalità in un controllo sulla sussistenza, sulla trasparenza[22] e sull'effettività dei rimedi giudiziali avverso possibili abusi dell'autorità che invadono la sfera di riservatezza dei singoli[23].

Il giudizio di adeguatezza appare assai complesso da declinare quando la compressione della libertà dei singoli risponde al (superiore?) interesse della giustizia. Per un verso, il potere punitivo rappresenta ancora –e soprattutto oggi– il caposaldo della sovranità statuale, di fronte alla quale le istanze di riservatezza dei singoli appaiono cedevoli; per altro verso, la violazione del diritto alla riservatezza potrebbe riverberarsi in un'ulteriore inosservanza del dettato convenzionale, quando l'impiego del dato viziato da contrarietà all'art.8 Cedu con finalità probatorie possa determinare anche una violazione del *fair trial*.

2.2. Violazioni della riservatezza e processo equo: i frutti dell'albero avvelenato.

Il tema dei rapporti tra art. 6 Cedu e prova penale implica una riflessione e un approfondimento così densi da avere, ormai, proporzioni non monografiche ma enciclopediche. Com'è noto, nell'assenza di uno 'statuto generale' della prova penale[24], l'art. 6 § 3 Cedu detta alcuni principi che, nell'articolazione tra le lettere *b* e *d*, rappresentano uno standard minimo di garanzia che gli Stati devono prevede all'interno dei loro ordinamenti, con particolare riguardo alla prova testimoniale. In merito allo specifico profilo all'attenzione, la Corte è stata spesso 'invitata' a misurarsi con la più classica delle tematiche probatorie, ovvero quella dei "frutti dell'albero avvelenato", le prove che sono state ottenute attraverso la violazione di un parametro convenzionale, come ad esempio l'art. 3 o, appunto, l'art. 8 Cedu.

Dovendo sintetizzare estremamente la questione, si deve intanto osservare che la Corte ha sempre evitato di stabilire degli automatismi tra violazione 'preesistente' e iniquità processuale, riservandosi di valutare, caso per caso, la complessiva equità del procedimento penale in cui sia stato fatto uso della prova viziata. Nel *leading case Gäfgen c. Germania*, i Giudici di Strasburgo hanno confermato che l'ingresso nel patrimonio valutativo del giudice di una prova raccolta in spregio di altra previsione convenzionale non implica di per sé una violazione dell'art. 6 Cedu, quando essa non abbia influito sulla prova

---

[21] Si veda già C. eur., 6.9.1978, *Klas v. RFT*.

[22] In termini molto critici, P. De Hert, S. Gutwirth, *Privacy, Data Protection*, cit., 80: «*transparency seems to have replaced legitimacy as the core value of data protection*»

[23] Cfr. P. De Schutter, *La Convention européenne des droits de l'homme à l'*épreuve *de la lutte contre le terrorisme*, *Rev. Un. Dr. H.*, 2001, p. 142.

[24] Si veda già C. eur., 12.7.1988, *Schenk v. Switzerland*, § 46 e, da ultimo, C. eur., 22.5.2018, *Svetina v. Slovenia*, § 42.

dei fatti oggetto dell'imputazione[25]. La difficoltà di valutare il grado di incidenza che un dato conoscitivo ottenuto senza il rispetto dei parametri convenzionali possa aver esercitato sul procedimento decisorio è evidente, così come lampante è il rischio che tale parametro sia, di volta in volta, applicato in modo non coerente dalla Corte[26]…

Non solo. Con specifico riguardo proprio ad una doglianza mossa sotto il duplice profilo degli artt. 8 e 6 Cedu, nella decisione *Kahn v. UK* la Corte ha osservato che, stante la violazione del diritto alla vita privata e familiare –determinata da un'illegittima intercettazione di conversazione riservata– nessuna violazione dell'art. 6 Cedu poteva riscontrarsi nel caso di specie, data la possibilità, riconosciuta all'imputato di contestare sia l'ammissibilità, sia l'attendibilità del contenuto dell'intercettazione stessa, durante il dibattimento[27] (il riferimento all'attendibilità e, quindi, all'accuratezza del dato probatorio tornerà assai utile più oltre nel ragionamento: v. § 4).

Questa breve digressione serve a sottolineare che, ad oggi, lo scrutinio di legittimità convenzionale della prova ottenuta attraverso la raccolta di dati digitali sembra limitarsi al contesto della sfera individuale, cioè del solo diritto al rispetto della vita privata e familiare, con l'ulteriore rischio che non vi siano ricadute dirette sul piano processuale, poiché –applicando i criteri della Corte europea– la violazione dell'art. 8 potrebbe non determinare anche una violazione dell'equità processuale[28]…

Si esaurisce, quindi, in questa incerta triangolazione tra tutela della riservatezza, procedimento decisorio giudiziale e test di preponderanza, la protezione che la Convenzione europea dei diritti dell'uomo è in grado di offrire contro i rischi che si nascondono nell'impiego processuale di 'prove digitali'? Due sono i limiti evidenti di questo approccio. Per un verso, l'assenza di automatismo tra ingresso di prova viziata e iniquità processuale implica la

---

[25] C. eur., 1.6.2010, *Gäfgen v. Germany*, § 180: «*The impugned real evidence was not necessary, and was not used to prove him guilty or to determine his sentence. It can thus be said that there was a break in the causal chain leading from the prohibited methods of investigation to the applicant's conviction and sentence in respect of the impugned real evidence*».

[26] In termini critici rispetto all'ondivago atteggiamento mostrato dalla giurisprudenza di Strasburgo nell'applicazione del «*sole and decisive*» test, v. R. Goss, *Criminal Fair Trial Rights*, Hart Publishing, Oxford, 2014, p. 170.

[27] C. eur., 12.5.2000, *Khan v. the UK*, § 38: « *the applicant had ample opportunity to challenge both the authenticity and the use of the recording. He did not challenge its authenticity, but challenged its use at the voir dire and again before the Court of Appeal and the House of Lords*». La Corte fa ripetutamente richiamo ad un precedente parzialmente coincidente, ovvero il caso C. eur. (pl.), 12.7.1988, *Schenk v. Switzerland*, nel quale, tuttavia, sebbene le doglianze sollevate dal ricorrente riguardassero egualmente l'art. 8 e l'art. 6 Cedu, entrambe le denunciate violazioni venivano escluse dai giudici di Strasburgo. La doglianza sub art. 8, poiché irricevibile per mancato previo esaurimento delle vie di ricorso interno; quella sub art. 6 perché, appunto, il processo doveva ritenersi nel suo complesso equo, data la possibilità riconosciuta all'imputato di contestare l'autenticità e l'utilizzabilità della prova intercettiva illegittimamente acquisita.

[28] C. eur., *Svetina c. Slovenia*, cit., § 48: « *The Court notes in this connection that it has already found in several cases where investigative measures interfering with Article 8 rights were not "in accordance with the law" that the admission in evidence of information obtained thereby did not, in the circumstances of the cases, conflict with the requirements of fairness guaranteed by Article 6 § 1*».

necessità del 'doppio passaggio' sopra descritto[29], con i limiti connaturati agli illustrati parametri decisori impiegati dalla Corte di Strasburgo.

Per altro verso, certi vizi della '*digital evidence*' non riguardano soltanto i dati ottenuti attraverso l'intrusione occulta nella immateriale area di privatezza degli individui, ma caratterizzano tutti gli elementi conoscitivi che derivino dal procedimento automatizzato, nel quale la fonte della conoscenza che si introduce nel processo non è umana, ma è un algoritmo, o un modello, nel cui funzionamento l'apporto umano si riconosce soltanto in fase di design e non di produzione del dato conoscitivo.

Questa è la vera area grigia che occorre scandagliare, perché è proprio a questa modalità di formazione del dato probatorio che nessun ordinamento processuale è ancora preparato, poichè tradizionalmente ispirato all'intervento umano nel processo (o anche solo in parte del processo) che genera la prova.

3. OLTRE LA FRONTIERA DELLA PROTEZIONE DELLA RISERVATEZZA

In armonia con quanto indicato dall'art. 8 Cedu e da buona parte delle Costituzioni nazionali, gli ordinamenti dei Paesi del Consiglio d'Europa hanno, nel tempo, regolato per legge i mezzi di ricerca della prova atti a fornire una captazione segreta di comunicazioni e di informazioni, per lo più attraverso strumenti intercettivi. Come anticipato, la superfetazione di tali informazioni, sotto forma di dati digitali, e una potenza computazionale senza precedenti hanno dato luogo ad una situazione in cui l'impiego delle tecnologie digitali rappresenta un potenziamento (apparentemente)[30] irrinunciabile delle capacità investigative, sebbene il balzo in avanti tecnologico non sia stato colmato a livello normativo e sia rimasto, quindi, privo di specifica regolamentazione procedimentale.

Come dimostrato dallo studio realizzato per la commissione Libe, tutti i Paesi presi in considerazione hanno recentemente modificato (o stanno modificando) la propria disciplina in materia di ricerca della prova, per adeguarla alle specificità e, soprattutto, alla maggiore invasività degli strumenti digitali già ampiamente utilizzati per finalità di *hacking by law enforcement*.

E' stato più volte osservato che la difficoltà di predisporre una puntuale regolamentazione di tali strumenti dipende in primo luogo dall'obsolescenza dei concetti di domicilio e di corrispondenza, così come tradizionalmente

---

[29] «*The question which must be answered is whether the proceedings as a whole, including the way in which the evidence was obtained, were fair. This involves an examination of the "unlawfulness" in question and, where a violation of another Convention right is concerned, the nature of the violation found*» (così C. eur. Gr. Ch., 10.3.2009, *Bykov v. Russia* , § 89)

[30] Critico, sul punto, lo studio *Legal framework*, p. 9.

concepiti nei testi di legge vigenti[31]. Ad esempio, la condizione di compatibilità convenzionale enunciata dall'art. 8 Cedu –così come da molte Carte costituzionali– ovvero la riserva di legge, si sostanzia, per lo più, attraverso la individuazione di precise limitazioni, spaziali e temporali, alla possibilità per l'autorità inquirente di ingerirsi nella sfera di riservatezza privata. In assenza di chiare condizioni e limitazioni, l'ingerenza è arbitraria e contraria, quindi, alla Convenzione (e alla costituzione). Tuttavia, per un verso, l'uso generalizzato di strumenti digitali, come *smartphones*, *tablets*, *notebooks* ha ampliato esponenzialmente la quantità di informazioni che sono reperibili attraverso un semplice accesso occulto allo strumento, che vanno ben oltre alla corrispondenza e alle conversazioni orali, potendo consistere in *files* di testo, immagini stoccate nella memoria del supporto o prodotte in tempo reale dalla webcam integrata, in *files* audio ecc… Per altro verso, tali strumenti seguono l'utilizzatore in ogni luogo e in ogni contesto rendendo decisamente impossibile continuare ad applicare la tradizionale distinzione tra luoghi pubblici e luoghi privati, come il domicilio, nel quale la captazione occulta tendenzialmente poteva avvenire soltanto a condizioni ancora più stringenti di quelle generali.

La perdurante impossibilità di trasfondere il ricco e vivace dibattito che negli ultimi decenni ha riguardato il concetto di domicilio digitale[32] in un aggiornamento normativo rende per lo più difficoltoso, nei vari Stati, raggiungere una disciplina efficiente. Anche il requisito, spesso imposto, della riserva giudiziale (o proprio giurisdizionale), rischia di perdere significato di fronte alla costante mobilità del supporto che può fornire agli investigatori i dati rilevanti, il quale segue inevitabilmente la persona fisica: stante la denunciata, fuorviante confusione, fatta registrare spesso dal legislatore italiano, tra contenitore e contenuto dell'informazione digitale[33] –laddove il contenitore presenta ben più scarso "valore investigativo" del contenuto– l'individuazione nel provvedimento autorizzativo giurisdizionale dello specifico hardware da sottoporre a controllo rischia di svuotarsi del suo contenuto di tutela, per diventare una 'delega in bianco' all'intrusione in tutte le forme di comunicazione possibili attraverso l'apparecchio[34].

---

[31] E' pur vero che la più attenta dottrina ha sempre saputo astrarre la tutela offerta dalle previsioni normative dalla mera fisicità dei luoghi e dei contesti in esse indicati (F. Caprioli, *Colloqui riservati e prova penale*, Giappichelli, Torino, 2000, p. 56 s., con riferimento alle teorie di Amorth e Bricola), estendendola all'intera sfera di estrinsecazione della personalità dell'individuo… Tuttavia, la digitalizzazione produce dati e metadati che si estendono anche oltre tale sfera, la cui agevole captazione rende sempre più difficile distinguerne la rilevanza sul piano dei fatti rilevanti per l'accertamento penale e quelli irrilevanti, rispetto ai quali anche l'imputato ha diritto alla riservatezza v. G. Illuminati, *La tutela della segretezza delle comunicazioni tra vecchio e nuovo codice*, in L. Giuliani (a cura di), *Processo penale e valori costituzionali nell'insegnamento di Vittorio Grevi*, Cedam, Padova, 2013, p. 108.

[32] Non concorde sull'utilità di tale concetto, A. Capone, *Intercettazioni e costituzione, Problemi vecchi e nuovi*, in *Cass. Pen.*, 2017, p. 1266.

[33] In questo senso v., *ex multis*, E. Lorenzetto, *Utilizzabilità dei dati informatici incorporati su computer in sequestro: dal contenitore al contenuto passando per la copia*, in *Cass. pen.*, 2010, p. 1522

[34] V., sul punto, A. Capone, *Intercettazioni e costituzione*, cit., p. 1273.

Riassumendo, dunque, attraverso gli strumenti digitali di captazione occulta, un software (utilizzato dagli inquirenti) interagisce con altro software (quello del supporto digitale) per ricavare dei dati digitali che saranno usati per le indagini e per la prova dei fatti oggetto di imputazione[35]. Il risultato finale, ovvero il dato conoscitivo che potrà essere posto dal giudice alla base del suo ragionamento decisorio, è quindi il frutto di vari passaggi di elaborazione automatizzata.

Non solo. Anche senza impiego di strumenti di captazione occulta, da tutti i supporti digitali si possono estrarre informazioni di grande rilievo per il procedimento penale. Per un verso può trattarsi di metadati; per altro verso, con la crescente rilevanza dell'IoT, può trattarsi di dati elaborati automaticamente, senza alcun intervento umano nella loro rilevazione. Questi rappresentano, evidentemente, un patrimonio conoscitivo talvolta fondamentale per le indagini e per il procedimento penale: si pensi, ad esempio, ad un frigorifero "intelligente" che si accenda per mantenere stabile la temperatura dei cibi ogni volta che la temperatura della stanza aumenti, per la presenza fisica di persone. Il software che lo regola fornirà informazioni determinati agli investigatori che indaghino su un omicidio avvenuto proprio in quella stanza…

In entrambi questi scenari, il dato conoscitivo rilevante per il procedimento penale è generato in modo automatizzato, sulla base di un algoritmo che governa il software, sia questo specificamente preposto alla captazione occulta investigativa, sia invece destinato a finalità estranee al procedimento penale.

La questione che qui si pone come oggetto centrale della riflessione riguarda la verifica dell'accuratezza del dato, generato e/o raccolto esclusivamente attraverso un algoritmo. E' possibile contestarne l'attendibilità? Oppure la 'prova digitale', per la sua natura e per la sua genesi, è oggettivamente impermeabile al confronto dialettico tra le parti nel processo? A questa domanda si cercherà di rispondere qui di seguito, rimanendo nel quadro dei parametri convenzionali.

3.1. Un problema di asimmetria conoscitiva.

L'assunto sul quale si basa l'interrogativo formulato qui sopra è l'impossibilità di falsificare il dato elaborato da un algoritmo se non è possibile accedere al codice sorgente che governa l'algoritmo stesso[36]. Tale assioma si declina con lo stesso grado di complessità in relazione sia ai dati digitali acquisiti attraverso specifico software intercettivo, sia derivati, come si è detto, da un software creato con finalità del tutto estranee al procedimento penale.

---

[35] V. dettagliatamente, M. Torre, Il captatore informatico: nuove tecnologie e rispetto delle regole processuali, Giuffré, Milano, 2017, *passim*.

[36] V. E. Van Buskirk-V.T. Liu, *Digital Evidence*, cit., 21

La rivelazione del codice sorgente implica un primo e particolare livello di difficoltà, legato, nella prima ipotesi, alla necessaria segretezza del software utilizzato dall'autorità inquirente per scopi di captazione occulta e, in generale, alla protezione della proprietà intellettuale che spesso copre tale codice[37]. Inoltre, poi, se il design dell'algoritmo non è improntato, *ab origine*, alla trasparenza[38], potrebbe essere impossibile verificare l'attendibilità dell'output per chiunque non sia il designer del codice sorgente stesso.

Questi aspetti saranno successivamente ripresi e ampliati, nell'ottica di immaginare se esistano soluzioni che possano essere utilizzate nel processo per ovviare all'evidente fenomeno di asimmetria conoscitiva che si verifica nelle situazioni descritte. Lo squilibrio conoscitivo è fenomeno che si riscontra nel processo penale sin da quando, per la soluzione di casi complessi, si è iniziato a fare ricorso a competenze tecniche, scientifiche o artistiche[39]. L'ingresso di saperi specialistici nel processo è difficilmente equilibrato, poiché una della parti - per lo più quella pubblica -ha accesso alla scienza e alle tecnologie migliori, disponendo di mezzi economici non limitati. Evidentemente, il fenomeno di *knowledge impairment* non è nuovo e ogni stagione del complicato rapporto tra scienza e processo penale ne ha riproposta una versione più o meno intensa (si pensi al debutto della profilazione del DNA nelle aule di giustizia, o al ricorso alla fMRI per l'accertamento di profili legati all'imputabilità). La prova algoritmica, tuttavia, introduce la forma più estrema di tale squilibrio, poiché il risultato probatorio può essere non criticabile laddove, appunto, l'inaccessibilità del codice sorgente o altre caratteristiche del *software* non consentano alla parte contro la quale la prova è introdotta nel processo di contestarne l'accuratezza e l'attendibilità. Ciò, evidentemente, trascende in maniera netta il profilo della riservatezza, sopra a grandi linee enunciato, per porre uno scottante problema di parità delle armi.

4. PARITÀ DELLE ARMI E CONFRONTO SULL'ATTENDIBILITÀ DELLA PROVA

E' infatti sotto il profilo della parità delle armi che la situazione segnalata si pone maggiormente in contrasto con il dettato convenzionale. E' ben noto che, pur nell'assenza di una esplicita enunciazione nel testo dell'art. 6 Cedu, il principio della parità delle armi è stato modellato dalla giurisprudenza della Corte come architrave, insieme al connesso canone del contraddittorio,

---

[37] V. ancora E. Van Buskirk-V.T. Liu, *Digital Evidence*, cit., 20.

[38] Sul paradigma della trasparenza si veda, ampiamente, M. Hildebrandt, *Profile Transparency by Design? Re-enabling double contingency*, in M. Hildebrandt – K. De Vries (a cura di), P*rivacy, Due Process and the Computational Turn*, Routledge, London, 2013, p. 239.

[39] Si veda la ricostruzione storica di A.J. Brimicombe – P. Mungroo, *Algortihms in the Dock: Should Machine Learning Be Used in British Courts?* Proceedings of the fourth Winchester Conference on Trust, Risk, Information and the Law, 3 maggio 2017.

dell'equità processuale nel suo complesso[40]. Notoriamente, *equality of arms* non implica una presunta, necessaria identità di facoltà o di posizioni che le parti essenziali del processo debbano sempre fruire, soprattutto laddove si tratti, appunto, di processo penale, il quale è caratterizzato –specialmente nelle sue fasi prodromiche– da un insuperabile squilibrio tra parte pubblica e difesa[41]. In questa connaturata differenza di ruoli istituzionali, il paradigma essenziale della parità delle armi è rappresentato dalla garanzia che a ciascuna delle parti deve essere garantita la possibilità di presentare i propri argomenti in condizioni che non la svantaggino rispetto alle altre[42]. Insomma, il principio esprime essenzialmente, nella sua portata generale, un giusto equilibrio tra le parti processuali[43]. Se indubbiamente tale affermazione può apparire per lo più declamatoria, essa va coniugata con più specifiche messe a punto della parità delle armi, come quella scolpita nel *leading case Brandstetter c. Austri*a, in cui la Corte ha ribadito che è necessario che ciascuna parte abbia effettiva conoscenza delle allegazioni e delle argomentazioni della controparte e che fruisca della concreta possibilità di contestarle e falsificarle. «*An indirect and purely hypothetical possibility for an accused to comment on prosecution argument*»[44] non soddisfa il parametro convenzionale.

Ancor più particolare, poi, è l'approccio che la Corte di Strasburgo adotta quando è chiamata ad accertare una violazione potenzialmente verificatasi nel procedimento probatorio, tradizionalmente devoluto alla disciplina nazionale, come non si manca mai di ricordare. Infatti, in questo contesto, è proprio la possibilità, per tutte le parti e, principalmente, per la difesa, di contestare l'accuratezza della prova a carico ad esprimere il senso proprio del suddetto giusto equilibrio tra le parti. È stato, infatti, ripetutamente sottolineato che «*it must be examined in particular whether the applicant was given the opportunity of challenging the authenticity of the evidence and of opposing its use. In addition, the quality of the evidence must be taken into consideration, including whether the circumstances in which it was obtained cast doubt on its reliability or accuracy*»[45]. L'assunto richiama quanto già sottolineato in

---

[40] Cfr. M. Chiavario, *Art. 6,* in S. Bartole, B. Conforti, G. Raimondi, *Commentario alla convenzione europea dei diritti dell'uomo e delle libertà fondamentali*, Cedam, Padova, 2002, p. 192. V., in particolare, C. eur., 28.8.1991, *Brandstetter v. Austria*, § 66; C. eur., 23.6.1993, *Ruis-Mateos v. Spain*, § 63.

[41] Cfr. Van Dijk – Van Hoof, T*heory and Practice of the European Convention on Human Rights*, 3rd ed., Martinus Nijoff, Leiden, 1998, p. 430 ss.

[42] In questo senso, C. eur., 7.6.2001, *Kress c. Francia*, § 72.

[43] J.F. Renucci, *Droit européen des Droits de l'Homme. Droits aux libertés fondamentaux garantis par la CEDH*, 5a ed., Lexestenso éditions, Paris, 2013, p. 378.

[44] C. eur., *Brandstetter v. Austria*, cit., § 68.

[45] Così, C. eur., *Bykov v. Russia*, cit., § 90, da ultimo ripresa in C. eur., *Svetina c. Slovenia*, cit., § 44, nella quale la questione denunciata dal ricorrente riguardava proprio l'impiego di prove raccolte sulla base di un iniziale, illegittimo (perché non espressamente autorizzato dal locale "giudice istruttore") accesso al telefono della vittima. Posta ancora una volta di fronte al problema dell'applicabilità della teoria dei frutti dell'albero avvelenato, la Corte ha rilevato che le giurisdizioni interne hanno fatto applicazione della contraria dottrina della "*inevitable discovery*"; tuttavia, poiché la questione della ammissibilità o meno delle susseguenti prove –che, appunto, secondo la Suprema Corte slovena sarebbero state scoperte comunque, a prescindere dall'illegittimo accesso– riguarda in definitiva l'interpretazione di norme interne, la Corte europea si limita ad osservare che le risultanze dell'accesso illegittimo non

precedenza rispetto alle decisioni *Khan v. the UK* e *Schenk v. Switzerland* che rappresentano la "cerniera" tra queste considerazioni formulate, in generale, rispetto al vasto panorama delle prove penali e gli specifici aspetti che caratterizzano le prove ottenute attraverso mezzi occulti.

Date queste coordinate generali, dunque, i problemi posti dalle prove raccolte e generate in via del tutto automatizzata sono evidenti. L'impossibilità –variamente declinata– di accedere al codice sorgente o di poter effettivamente comprendere il funzionamento dell'algoritmo che le ha generate determina un rischio implicito per la parità delle armi, così come intesa dalla richiamata giurisprudenza europea. Ecco il tassello di complessità che questo scenario aggiunge al quadro già analizzato e risolto dalla Corte europea in *Khan v. the U.K.*, lasciando ipotizzare possibili conclusioni diverse. Se l'essenza dell'equità processuale risiede nella parità delle armi, che si sostanzia (anche) nel diritto della difesa di contestare l'ammissibilità e l'accuratezza della prova, l'impossibilità di verificare *a posteriori* l'*output* di un algoritmo può costituire *in nuce* una violazione dell'art. 6§1 Cedu (a prescindere dall'esistenza di una violazione, a monte, del diritto alla vita privata e familiare).

Questa affermazione, tuttavia, non può rappresentare il punto finale, ma solo quello iniziale, del ragionamento: nella giurisprudenza della Corte europea dei diritti dell'uomo è infatti cristallizzato il canone "olistico" dell'equità del procedimento nel suo complesso. Occorre dunque verificare se esistano degli strumenti, tecnici e processuali, che consentano alla difesa di esercitare concretamente (e con cognizione di causa, quindi fondatamente, almeno in potenza) il proprio inviolabile diritto a criticare l'accuratezza della prova a carico.

4.1. Possibili rimedi

La prima e più immediata risposta al quesito che precede è la trasparenza. Si è già in parte accennato al fatto che, nell'ambito della trattazione automatizzata dei dati, la trasparenza pare essere divenuta l'unico e determinante parametro di legittimità del trattamento, sostituendosi subdolamente al canone della legalità[46]. Se il software è concepito secondo parametri di trasparenza, la possibilità di validazione o di falsificazione dei suoi outputs è più elevata e a questo assunto sembrano ispirati il GDPR, appena entrato in vigore e per certi versi anche la direttiva UE 2016/680, in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali (art. 20), recentemente trasposta anche in Italia con il d.lgs. 18.5.2018 n. 51[47].

---

sono state poste alla base della decisione sulla colpevolezza dell'imputato, fondata, invece, su prove validamente raccolte, secondo la disciplina nazionale.

[46] V. *supra* nt. 21.

[47] Pubblicato in G.U. 24 maggio 2018 ed entrato in vigore il 6 giugno 2018.

Tuttavia, la trasparenza non è un concetto autosufficiente, ma si articola in relazione al risultato che si desidera ottenere. Essa, ad esempio, si può raggiungere ottenendo l'accesso al *source code*, agli *inputs* e agli *outputs* del software[48]. Tuttavia, tale accesso può non essere utile perché soltanto gli esperti informatici sono in grado di trarne degli elementi significativi perché comprensibili. E' stato osservato, quindi, che in tal caso non può dirsi comunque garantita la trasparenza[49].

Inoltre, nemmeno l'*open source code* –che parrebbe a prima vista la principale garanzia di trasparenza– può garantire la possibilità di un'effettiva validazione a posteriori dei risultati prodotti dall'algoritmo, se questo non è stato concepito con criteri più che di trasparenza[50] –appunto– di responsabilità (*accountability*, intesa come possibilità, capacità di dar conto di come i risultati sono stati prodotti, partendo da determinati inputs)[51]. Per un verso, come già sottolineato, nell'ambito della ricerca e della raccolta della prova difficilmente è possibile utilizzare software open source, proprio perché l'efficacia degli specifici mezzi intercettivi occulti sta nella segretezza, innanzitutto, del loro operare, ma anche delle loro modalità di funzionamento. Per altro verso, poi, quando il software faccia uso di forme anche molto semplici di intelligenza artificiale, la validazione *ex post* del risultato può diventare impossibile anche per chi lo abbia messo a punto, stante il meccanismo di auto-apprendimento che lo alimenta.

Come poter contestare, allora, l'accuratezza di un dato, generato automaticamente e utilizzato nel processo penale come prova? Esistono e possono essere messi a punto dei software di crittografia, definiti "*zero-knowledge proof*" o, più correntemente *black boxes* attraverso i quali è possibile dimostrare quali sono i criteri che governano la *policy* dell'algoritmo, senza dover svelare la *policy* stessa[52]. Questo strumento può essere molto utile alla difesa per contestare l'accuratezza e, quindi, l'attendibilità della prova a carico, senza presupporre necessariamente il disvelamento dell'algoritmo che governa il *software* da cui la prova è stata generata. Insomma, uno strumento utile a verificare la correttezza dell'output che è stato generato automaticamente.

---

[48] J.A. Kroll, J. Huey, S. Barrocas, E.W. Felten, J.R. Reidenberg, D.G. Robinson, H. Yu, *Accountable Algorithms*, in *University of Pennsylvania Law Review*, 2017 (Vol. 165, Issue 3), p. 675.

[49] A. Koene, H. Webb, M. Patel, *First UnBias Stakeholders workshop*, 2017, in https://unbias.wp.horizon.ac.uk

[50] E. Van Buskirk-V.T. Liu, *Digital Evidence*, cit., 24, i quali non ritengono del tutto superabile un 'nocciolo duro' di tutela intelletuale.

[51] Cfr. A. Kroll, J. Huey, S. Barrocas, E.W. Felten, J.R. Reidenberg, D.G. Robinson, H. Yu, *Accountable Algorithms*, cit., p. 662 ss.

[52] Offrono un utile esempio A. Kroll, J. Huey, S. Barrocas, E.W. Felten, J.R. Reidenberg, D.G. Robinson, H. Yu, *Accountable Algorithms*, cit., p. 668: si pensi al caso di due commensali molto ricchi, i quali stabiliscono che il più ricco dei due dovrà pagare il conto del pranzo, senza essere tuttavia disposti a rivelare l'ammontare del proprio patrimonio. L'impiego di un *software zero-knowledge proof* consentirà di scoprire chi dei due è il più ricco –e debba pagare il pranzo– senza rendere noto l'ammontare delle rispettive ricchezze.

Un altro possibile strumento per ottenere la verifica dell'attendibilità della prova è un'eventuale certificazione indipendente dell'affidabilità del software che l'ha generata. Ciò implica il ricorso alla nomina di un perito che, sulla base dei quesiti formulati dal giudice sia messo in grado di validare o meno ex post i risultati la cui attendibilità è in contestazione. Il riferimento, almeno nel contesto nordamericano, è sempre quello del Daubert test, le cui quattro articolazioni trovano perfetta applicazione anche con riferimento al frensic softwere[53].

In primo luogo, il perito nominato dal giudice, proprio con l'incarico di svolgere una validazione indipendente, rappresenta uno strumento "mediato" di critica della prova da parte della difesa, che potrebbe non avere fiducia nell'esperto individuato dal giudice. Tale inconveniente potrebbe essere limitato attraverso la nomina di un consulente tecnico di parte, come ad esempio prevede la disciplina italiana, che consente alle parti di nominare un proprio esperto in occasione dell'incarico peritale *ex* art. 220 c.p.p. Tale, ipotesi, tuttavia, richiede alcune riflessioni. Certamente essa garantirebbe alla difesa una più diretta ed efficace contestazione del dato probatorio, ma innescherebbe –sempre prendendo ad esempio la normativa italiana– un potenziale inconveniente sotto il profilo, ove sussistente, della necessaria segretezza dei codici sorgente. Allo stato attuale, infatti, i consulenti di parte dovrebbero essere immessi nella conoscenza degli stessi elementi forniti al perito, per consentire loro di svolgere il proprio incarico; tuttavia non pare sussistere, sul piano processuale, un divieto di divulgazione, da parte del professionista nominato dalla difesa, degli elementi appresi durante tale ufficio (ma al limite una facoltà di opporre eventualmente il segreto professionale). Trattandosi, infatti, di attività probatoria dibattimentale, non paiono sussistere limiti formali processuali all'eventuale divulgazione di quanto appreso[54]. Inoltre, com'è stato già segnalato da commentatori vicini a realtà processuali diverse da quella italiana, l'introduzione dell'*expert witness* per l'accertamento dell'accuratezza del dato probatorio generato automaticamente significherebbe riprodurre anche in questo contesto la complessa e confusa "battaglia tra esperti" che sempre più frequentemente anima i dibattimenti, e che può portare alla «paralisi delle corti»[55], inducendo il giudice a ergersi arbitro di una disputa su profili a lui del tutto estranei[56].

---

[53] E. Van Buskirk-V.T. Liu, *Digital Evidence*, cit., 23.

[54] E' certamente in atto una progressiva assimilazione della figura dei consulenti, quantomeno del p.m., a quella del testimone, avviata dalle pronunce della Corte costituzionale 163/2014 e, soprattutto, dall'ordinanza delle Sezioni Unite della Corte di cassazione (Cass., Sez. un., ord. 27 giugno 2013, n. 43384, in www.penalecontemporaneo.it), che sollevava, appunto, la questione di legittimità costituzionale decisa con la predetta sentenza, in relazione, appunto, ai doveri del consulente tecnico del pubblico ministero.

[55] In questo senso, M. Cross, *Algortihms and Schroedinger's Justice*, in *The Law Society Gazette*, 8.5.2017; ma v. già, E. Van Buskirk-V.T. Liu, *Digital Evidence*, cit., 25, con riguardo ad un noto caso deciso in Florida, con riguardo all'attendibilità dell'etilometro utilizzato per le rilevazioni alcolemiche in un caso di guida in stato di ebbrezza.

[56] Vengono alla mente le conclusioni di O. Dominioni, *La prova penale scientifica*, Giuffré, Milano, 2005, p. 69: «non è consentito che nella funzione probatoria si usino apparati conoscitivi insuscettibili

5. LA PARITÀ DELLE ARMI MESSA IN DISCUSSIONE.

Il quadro dei rimedi al rischio insito nell'impiego nel processo penale di prove generate automaticamente non è del tutto confortante. Ciascuna delle soluzioni indicate implica delle limitazioni e degli 'effetti collaterali' di non poco conto. Tuttavia, in assenza di qualsiasi accorgimento, la violazione del principio della parità delle armi –intesa nel suo nucleo essenziale– pare difficilmente evitabile.

In questo senso, il tema di questa riflessione amplifica, portandolo alla massima potenza, il problema, già anticipato, dell'asimmetria conoscitiva che caratterizza tutte le nuove prove scientifiche. Non per questo, però, la riflessione proposta è sterile, in quanto la 'prova algoritmica' esalta e mette in luce il rischio che, in una società in cui tutto ciò che è oggetto di conoscenza e di comunicazione è un dato –è cioè costituito da o è racchiuso in una 'espressione digitale'– i soggetti del processo vengano deprivati del loro ruolo nel procedimento probatorio (dalla raccolta, ma anche dalla valutazione, dalla discussione e dalla valutazione). Il dato, ottenuto o elaborato digitalmente rischia di divenire di per sé attendibile perché la verificazione del processo che lo ha generato è troppo complessa o sfugge, almeno in parte, per via del ricorso a forme più o meno sofisticate di intelligenza artificiale, ad un controllo *ex post*. In tale quadro, l'accusa ha accesso, per evidenti ragioni, alla migliore tecnologia, i cui risultati vengono trasferiti nel processo penale come prove. La difesa, per le ragioni sopra esposte, non ha la possibilità di mettere convincentemente in dubbio l'attendibilità di tale prova, poiché non ha gli elementi necessari alla falsificazione. Il giudice, per parte sua –soprattutto in quegli ordinamenti più nettamente ispirati al principio dispositivo della prova– può non avere motivo di dubitare di tale prova, in assenza di elementi concreti addotti dalla difesa, 'adagiandosi' sul convincimento che il dato digitale sia scevro da rischi di inaccuratezza[57].

Come spesso accade quando si cerca di ragionare sull'evoluzione del processo di integrazione tra realtà attuale e progresso digitale –soprattutto, intelligenza artificiale– il quadro appare distopico. Ciò che conforta, nell'analisi fin qui svolta, è che il sistema convenzionale –nella sua interazione con la Carta dei diritti fondamentali dell'Unione europea e con le costituzioni nazionali– già contiene gli strumenti per neutralizzare la stortura connaturata all'impiego nel processo penale di prove generate automaticamente. La parità delle armi, elaborata dalla giurisprudenza di Strasburgo attorno a situazioni concrete assai differenti rispetto a quelle qui in esame, può e deve rappresentare il baluardo contro il rischio, che l'efficienza tecnologica diventi un criterio autosufficiente di attendibilità della prova.

---

di controllo ad opera del giudice e delle parti».

[57] V., icasticamente, E. Van Buskirk-V.T. Liu, *Digital Evidence*, cit., 20: «*rather than wrestle with, or even acknowledge, this conundrum, most courts simply presume that all code is reliable without sufficient analysis*».