

Il processo penale alla prova delle nuove tecnologie e dell'intelligenza artificiale

a cura di

A. De Caro, V. Maffeo, G. Rossi, G. Tessitore



Giappichelli

Il processo penale alla prova delle nuove tecnologie e dell'intelligenza artificiale



Il processo penale alla prova delle nuove tecnologie e dell'intelligenza artificiale

a cura di

A. De Caro, V. Maffeo, G. Rossi, G. Tessitore



Giappichelli

© Copyright 2026 – G. GIAPPICHELLI EDITORE – TORINO

VIA PO, 21 - TEL. 011-81.53.111

<http://www.giappichelli.it>

ISBN/EAN 979-12-211-1389-1

ISBN/EAN 979-12-211-8150-0 (ebook-pdf)

ISBN/EAN 979-12-211-6661-3 (ebook-epub)

Convegno e pubblicazione finanziati nell'ambito del "PNRR Missione 4 - Componente C2 - Riforma Investimento 1.1 Fondo per il programma Nazionale di Ricerca e Progetti di Rilevante Interesse Nazionale (PRIN) - Progetto "Prova e Processo Informatico - PEPI" - Codice CUP E53D23006850006 - Soggetto attuatore; Università degli Studi di Napoli Federico II.



G. Giappichelli Editore



Questo libro è stato stampato su
carta certificata, riciclabile al 100%



Stampa: Stampatre s.r.l. - Torino

Le fotocopie per uso personale del lettore possono essere effettuate nei limiti del 15% di ciascun volume/fascicolo di periodico dietro pagamento alla SIAE del compenso previsto dall'art. 68, commi 4 e 5, della legge 22 aprile 1941, n. 633.

Le fotocopie effettuate per finalità di carattere professionale, economico o commerciale o comunque per uso diverso da quello personale possono essere effettuate a seguito di specifica autorizzazione rilasciata da CLEARedi, Centro Licenze e Autorizzazioni per le Riproduzioni Editoriali, Corso di Porta Romana 108, 20122 Milano, e-mail autorizzazioni@clearedi.org e sito web www.clearedi.org.

Indice

	<i>pag.</i>
Elenco autori	XI
Presentazione di <i>Vania Maffeo</i>	XIII
Introduzione di <i>Adolfo Scalfati</i>	1

Dialogo a due voci

Conoscere giudiziale, flussi di coscienza e paradigmi della complessità: itinerari, metodi, risorse, garanzie <i>Giuseppe Di Chiara</i>	7
Senza pregiudizi alla prova dell'IA nel processo penale <i>Antonio Ardituro</i>	21

Le modalità di controllo delle prove digitali

Le delicate traiettorie dell'informazione digitale nel processo penale <i>Agostino De Caro</i>	35
Controllo della prova digitale in contraddittorio <i>Michele Caianiello</i>	63

Prove digitali, diritti fondamentali e criteri di valutazione

Intelligenza artificiale e controllo contenutistico delle “forme” di produzione dei suoi <i>outputs</i> conoscitivi <i>Mariano Menna</i>	79
--	----

	<i>pag.</i>
Una criticità analoga <i>Roberto E. Kostoris</i>	91
Intelligenza artificiale, controllo umano significativo e ricostruzione del fatto <i>Giulio Ubertis</i>	105
Prove digitali e diritti fondamentali dell'individuo <i>Francesco Caprioli</i>	115
 Il futuro del processo penale tra tecnologie digitali e intelligenza artificiale (29 maggio)	
Messa alla prova e intelligenza artificiale: analisi, sfide e prospettive future <i>Concetta Bottino</i>	133
Informazioni e dati nella <i>digital forensics</i> : tra tutela dei diritti ed esigenze probatorie <i>Francesco D'Urso</i>	147
Intelligenza artificiale, algoritmi predittivi e cause di non punibilità <i>Alessandro Catania</i>	155
Criticità della c.d. giustizia predittiva: dall'esperienza statunitense alle posizioni europee <i>Giacomina Esposito</i>	165
L'IA come futuro agente sotto copertura nel mondo digitale? <i>Riccardo Gaeta</i>	175
La <i>digital evidence</i> e il suo accesso transfrontaliero. Tra diritti fondamentali ed effettività di tutela <i>Guido Rossi</i>	183
Quale futuro per le nuove forme di corrispondenza? <i>Alessandra Scalas</i>	195

pag.

Garanzie processuali a tutela della <i>privacy</i> <i>Michela Siracusa</i>	211
---	-----

Valutazione dell'impatto delle udienze da remoto sugli obiettivi dei principi del procedimento penale <i>Inga Žukovaitė</i>	225
---	-----

**Il futuro del processo penale tra tecnologie digitali
e intelligenza artificiale
(30 maggio)**

Ragionevole previsione di condanna e sistemi algoritmici: verso un possibile cambio di paradigma? <i>Anna Chiara Dellerba</i>	241
---	-----

Algoritmi di valutazione della prova dichiarativa: rischi e opportunità <i>Francesca Delvecchio</i>	253
--	-----

La tutela dei diritti di libertà alla prova della rivoluzione digitale nella giustizia penale <i>Piercarmine Lombardi</i>	265
---	-----

Informazione criptata all'estero e garanzie difensive <i>Nunzio Gallo</i>	281
--	-----

L'accertamento dei fatti nel giudizio penale, tra le lusinghe dell'intelligenza artificiale e gli approdi (ancora inesplorati) di saperi extra-giuridici <i>Aldo Franceschini</i>	289
--	-----

Polizia predittiva e misure cautelari personali: verso una <i>governance</i> etica dell'IA <i>Paola Ciccone, Camilla Felicita, Vanessa Lucchese, Antonio Vadalà</i>	303
---	-----

Sicurezza penale ed extra-penale nel <i>cyberspazio</i> <i>Ranieri Razzante</i>	313
--	-----

*pag.**Machine learning* e diritto penale:

dalla crisi del rapporto vicario di imputazione della responsabilità

al possibile superamento del paradigma *machina delinquere non potest*?*Serena Ucci*

317

Sistemi algoritmici e garanzie della ‘giusta decisione’:

l’IA tra i *naturalia* del processo penale?*Bianca Claudia Alongi*

331

Controllo della prova digitale in contraddittorio

Michele Caianiello

Sommario: 1. Rischi legati alla progressiva irrilevanza della prova dichiarativa. – 2. La prova dichiarativa in trasformazione. – 3. Contraddittorio sui dati. – 4. Contraddittorio e uso di IA. – 5. Conclusioni.

1. *Rischi legati alla progressiva irrilevanza della prova dichiarativa*

Uno dei problemi che affliggono la procedura penale nella nostra epoca sta nella riduzione progressiva degli spazi del contraddittorio¹. Questa erosione sembra dovuta a due fenomeni, diversi tra loro, e tuttavia convergenti verso il risultato di arrecare significativi *vulnera* alla dialettica orale nel contesto del processo. Il primo è il più tradizionale, e opera attraverso soluzioni ermeneutiche, non di rado criticabili, delle diverse disposizioni nel codice concernenti il recupero in dibattimento, quale prova, di atti a contenuto dichiarativo formati al di fuori dell'esame e controesame delle parti²: paradossalmente, questa manifestazione erosiva, sulla quale si sono sviluppate violente polemiche nell'arco di tempo che va dal varo del nuovo codice sino alla riforma costituzionale del c.d. "giusto processo", pare ormai la meno preoccupante. Naturalmente, non avendo essa cessato di infliggere danni al metodo orale e dialettico, è giusto che se ne parli e si stigmatizzino i problemi sistemati che possono originare da una attitudine interpretativa tesa ad espandere le deroghe alla oralità e al contraddittorio (tema nel quale possiamo inserire anche la *vexata quaestio* della immediatezza³). Ciò che tuttavia più colpisce, nel

¹ N. Capus, *Written Record of Statements and Fairness*, in J.D. Jackson, S. Summers (eds.), *Obstacles to Fairness in Criminal Proceedings*, London, 2018, p. 205 s.; J.H. Hodgson, *The Metamorphosis of Criminal Justice. A Comparative Account*, Oxford, 2020, p. 180; A. Roth, *The Lost Right to Jury trial in "All" Criminal Prosecutions*, in 72 *Duke Law Journal*, 2022, p. 599 s.

² Sul tema, per tutti, si rinvia al volume di D. Negri, R. Orlandi (a cura di), *Le erosioni silenziose del contraddittorio*, Torino, 2017 e ai contributi ivi contenuti.

³ Sul punto cfr. H. Belluta, *Mutamento del giudice e riassunzione delle prove*, in G.L. Gatta, M. Gialuz (a cura di), *Riforma Cartabia. Le modifiche al sistema penale*, vol. II, a cura di T. Bene, M. Bontempelli, L. Luparia Donati, *Nuove dinamiche del procedimento penale*, Torino, 2024, p. 293 s.

momento attuale, è senza dubbio il secondo fattore che pare in grado di minare alla radice il valore della oralità nel processo penale, legato al progressivo successo delle prove reali o documentali. Questi mezzi di prova, un tempo per lo più trascurati dalla dottrina, forniscono spesso oggi le informazioni più importanti per l'esito dei giudizi penali (e non solo). Ciò è dovuto, da un lato, alla ormai completa digitalizzazione di tanti aspetti della vita (e dunque della amministrazione degli affari, pubblici e privati), e, dall'altro, alla definizione generale che il codice prevede in materia di prova documentale: essa, infatti, è così ampia, da poter fungere da contenitore collettivo dei dati e metadati, dai quali, come noto, è possibile estrarre – e dunque produrre come evidenze nell'agone del processo – un profluvio di informazioni capaci di sostituire progressivamente il racconto umano.

Così non è infondato supporre che un insieme di dati, ipotizziamo di massive o comunque ingenti dimensioni, prodotti dall'uso di dispositivi digitali, possa finire per essere considerato – tutto sommato, con buone ragioni sul piano epistemico – più utile, maggiormente affidabile, più preciso e puntuale, rispetto al racconto che una persona può effettuare di una determinata vicenda. I dati, vale la pena rimarcare, risultano preziosi non solo al fine di ricostruire ciò che è avvenuto, così affiancando o sostituendo la narrazione effettuata da un individuo, ma anche per testare la credibilità di un racconto umano, in maniera più efficace del classico controesame: essi, infatti, posseggono quel carattere di oggettività, di "spontaneità" (si pensi ai dati automaticamente rilasciati dall'uso che quotidianamente facciamo di oggetti intelligenti – la c.d. *Internet of Things*⁴) meno esposto a rischi di sviamento dovuti alla capacità retorico-sofistica dei litiganti. Un dato non cade in una domanda tranello, non si fa confondere da una *leading question*, è immune a comportamenti nocivi o minatori dell'interrogante nel corso del giudizio: una volta rilasciato dalla macchina, e acquisito al processo, è lì, nella sua (im)materialità, difficilmente contestabile, se non a causa di errori umani nella sua raccolta e conservazione.

Se questo è vero, il processo penale quale fenomeno sociale sta andando incontro a mutamenti molto significativi, posto che la voce narrante umana ne ha retto le sorti, sul piano epistemologico, da diversi secoli: perdere la centralità del contraddittorio quale strumento per accertare i fatti significa, in primo luogo, relegare un principio costituzionale alla marginalizzazione: non un principio "qualunque", usando l'aggettivo indefinito in maniera retorica, bensì proprio quell'art. 111, comma 4, Cost. che, per la sua storia, svolge un carattere identitario in relazione al nostro sistema processuale. Di più, nella prospettiva che qui si propone, porta con sé il pericolo di una disumanizzazione del fenomeno processuale, dovuto alla perdita di rilevanza della prova dichiarativa, sostituita dal dato prodotto dalla macchina e dall'uso che ne facciamo. La metafora così efficace del *ghost in the shell* pare raffigurare bene il rischio odierno, nel quale l'umano – la sua essenza, il suo spirito

⁴ Cfr. S. Gless, *AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials*, in 51 *Georgetown Journal of International Law*, 2020, p. 197 s.

– è incapsulato nel guscio – nella *cyber*-armatura, ma anche nella prigione – del dispositivo digitale⁵.

2. La prova dichiarativa in trasformazione

Una trasformazione quale quella appena tratteggiata è certamente in atto. Essa non va sottostimata, e necessita di interventi normativi appositi (che, nel nostro Paese, tardano ad arrivare), nonché di un controllo costante, per quel che concerne i cambiamenti sociali che essa può produrre, anche nel campo della amministrazione del processo. La posta in gioco, infatti, è sempre quella di controllare i fenomeni e non di subirli o inseguirli, senza effettivamente comprenderne la essenza e la portata⁶. Tuttavia, i rischi paventati, almeno per ora, non vanno nemmeno enfatizzati. La prova digitale, per lo meno nel momento corrente, non sembra ancora in grado di sostituire quella dichiarativa. Essa, piuttosto, vi si affianca, e, cosa certamente da non trascurare, ne trasforma sensibilmente il contenuto, introducendo nuove forme di deposizione, a metà strada tra la testimonianza e la perizia o la consulenza tecnica. In questa chiave di lettura, il dichiarante chiamato a deporre in parte racconta brani della propria esperienza percettivo-fattuale, in particolare soffermandosi sulle azioni che ha intrapreso per raccogliere i dati digitali. Così, questi si sofferma su come li ha rinvenuti, come li ha raccolti, conservati e poi conferiti nel processo (elementi, questi ultimi, essenziali al fine di vagliare la genuinità degli stessi e la loro non alterazione); dall'altro, di quegli stessi dati, la stessa persona deponente elabora una interpretazione. In tal guisa, essa prova a formulare una spiegazione del perché, ad esempio, quel flusso starebbe a indicare un determinato avvenimento: ad esempio, perché mai si possa sostenere, alla luce dei dati acquisiti al processo, che l'imputato si è spostato da un luogo all'altro, in quale arco temporale ciò sarebbe avvenuto, come ciò sia compatibile con una ricostruzione fattuale rilevante ai fini della dimostrazione (o della confutazione) dei fatti di accusa. In questo quadro, anche il controesame sembra mutare colore, pur rimanendo centrale: esso serve, in primo luogo, a testare la qualità del lavoro di raccolta e conservazione del

⁵ Naturalmente, questo progressivo allontanamento dal racconto riferito nel processo dell'essere umano può trovare giustificazione nell'argomento per cui le prove digitali offrirebbero informazioni più affidabili. In questa prospettiva, l'accertamento della verità giustificerebbe dunque una parziale rinuncia al fattore umano, che nel testo si paventa. Non va tuttavia trascurata la questione legata alla accettazione sociale, tenendo conto del fatto che, ancora oggi, la giustizia penale è un prodotto umano, concepito e amministrato da umani e concernente il destino di (altri) esseri umani. Sembra dunque rilevante non relegare il dominio di questi ultimi nella gestione del sistema, se non si vuole incorrere nel rischio di un rigetto sociale causato da un affidamento sproporzionato alla macchina.

⁶ Adattando al contesto giuridico l'insegnamento dell'economista Peter Druker, secondo il quale «il pericolo più grande nei momenti di turbolenza non è la turbolenza in sé, ma è affrontarla con le logiche del passato».

dato, e, in secondo, a operare una contrapposizione dialettica sulla interpretazione delle informazioni che dai dati possono essere ricavate.

In sostanza, al momento la prova dichiarativa pare non correre un immediato pericolo di estinzione: sembra tuttavia che essa attraversi un percorso di mutazione, volto a contaminarne le forme, tra la testimonianza e la perizia. Rimane, ad ogni modo, ancora centrale il racconto dell'individuo, senza il quale la messe di dati prodotti dalle macchine da sola non è in grado di far rivivere i fatti che si vogliono accertare nel processo ⁷.

Questo slittamento del ruolo del testimone solleva, dunque, questioni non solo pratiche ma anche sistematiche. La "testiperizia" o "testiconsulenza" introduce un soggetto ibrido, difficilmente riconducibile ai canoni tradizionali del testimone puro, e ciò pone un problema di collocazione all'interno degli schemi processuali codificati. In particolare, quando il dichiarante, chiamato a riferire su dati digitali, finisce per interpretarli, ordinarli e trarne conclusioni, si verifica una sovrapposizione tra la funzione di narrazione e quella di valutazione: funzioni che, nel nostro modello, dovrebbero restare distinte. Tale fenomeno dà luogo a un'ambiguità che non va demonizzata, ma, piuttosto, guidata con una certa accortezza. Prima di affrettarsi a concludere che ci troviamo di fronte a un'anomalia da correggere (opzione, comunque, da non scartare a priori), è importante cogliere i caratteri essenziali di simile trasformazione, di modo, se possibile, da incanalarla entro regole chiare e funzionali. È infatti innegabile che la parola del "testimone digitale" (o del testimone che relazione sui dati rinvenuti o raccolti) porti con sé una ricchezza informativa nuova, una capacità di dare senso al dato attraverso il racconto, che merita attenzione e forse anche apprezzamento. Tuttavia, proprio per la sua natura composita, essa richiede che siano ben definiti i confini tra ciò che costituisce una deposizione sui fatti e ciò che, invece, si configura come una valutazione tecnica ⁸. In questa prospettiva, spetta al giudice – e, nei casi in cui il giudizio sia affidato a un organo collegiale, al presidente – il compito di adottare gli accorgimenti necessari per distinguere, già all'interno dell'esame, le diverse tipologie di domande ammissibili ⁹. È opportuno, cioè, che si separino chiaramente i quesiti dedicati all'accertamento fattuale (come e dove i dati sono stati rinvenuti, con quali modalità sono stati raccolti e conservati, su quali

⁷ Naturalmente, non si può escludere che questa sia solo una fase di passaggio, specie quando, attraverso programmi più sofisticati, i *computer* saranno in grado di elaborare rappresentazioni ricavate dalla analisi dei dati raccolti dagli inquirenti.

⁸ Operazione che non dovrebbe essere troppo complessa: anche oggi il perito o il consulente tecnico, quando riferiscono, ben possono, prima, raccontare fatti (come hanno proceduto a determinate attività prodromiche alla loro analisi), per poi effettuare le valutazioni delle quali sono stati richiesti in ragione del loro sapere specifico.

⁹ Torna utile l'insegnamento di R. Orlandi, *L'attività argomentativa delle parti nel dibattimento penale*, in P. Ferrua, F.M. Grifantini, G. Illuminati, R. Orlandi, *La prova nel dibattimento penale*, IV ed., Torino, 2007, p. 50, il quale vede nel potere direttivo del presidente e nella possibilità di chiamare in causa il collegio, ex art. 478 c.p.p., lo strumento adatto per rimediare in prima battuta agli abusi dialettici delle parti nel corso dell'esame e del controesame.

dispositivi sono stati trovati) da quelli volti a far emergere valutazioni e inferenze (quali informazioni gli investigatori hanno ritenuto di ricavare, come hanno deciso di sviluppare le indagini sulla base dell'interpretazione dei dati, quali conferme ritengono di aver ottenuto, e così via). Solo una conduzione vigile e strutturata dell'esame può consentire di mantenere intatta la trasparenza epistemologica della prova, evitando commistioni che ne indeboliscano il valore e compromettano l'equilibrio tra le parti.

La necessità di distinguere diverse fasi all'interno di una deposizione resa da un unico individuo non è solo un'esigenza teorica, ma ha ricadute concrete sulla gestione del contraddittorio. Se non è chiaro quando l'esame verta sui fatti o sulle valutazioni, l'interlocazione processuale ne risente: si fa più incerta la linea del controesame, più complessa la contestazione, più sfumata la distinzione tra ciò che è accaduto e ciò che se ne deduce. Occorre quindi che la cultura giuridica e la prassi processuale affrontino in modo consapevole questo cambiamento. Non si tratta tanto di opporre resistenza al mutamento, ma, se possibile, di governarlo: chiarendo, ad esempio, i criteri per distinguere la testimonianza tecnica dalla consulenza, o valutando l'opportunità di creare nuove figure processuali capaci di incanalare in modo trasparente questa nuova tipologia di dichiarazioni. Solo così sarà possibile mantenere fede al principio del giusto processo e alla sua struttura dialettica, salvaguardando al contempo l'apporto conoscitivo delle nuove fonti digitali e la dignità epistemologica della parola umana.

3. *Contraddittorio sui dati*

Alla luce di quanto osservato, si deve riconoscere che il nodo più problematico in ordine alla tutela del contraddittorio nel processo penale non si colloca tanto nella fase dibattimentale, con riguardo alla testimonianza *sui generis*, della quale si è detto; è invece nel momento iniziale, collocato nel corso delle indagini preliminari, che si addensano le maggiori criticità. In tale contesto, il pubblico ministero opera in condizioni di monopolio investigativo e in assenza di contraddittorio, avvalendosi dei poteri attribuitigli dalla legge per disporre perquisizioni informatiche e sequestri dei dispositivi in cui i dati sono contenuti. Queste operazioni possono condurre alla collezione di una vasta messe di informazioni, capaci di esporre la persona indagata, ma anche soggetti terzi, a un controllo pervasivo e penetrante capace di raggiungere ogni aspetto della vita privata. Proprio in questa fase – che si svolge in un contesto scarsamente regolato e ancora privo di un disegno sistemico – la raccolta dei dati digitali assume connotati che destano preoccupazione dal punto di vista delle garanzie. Le indagini su dati informatici non si limitano alla loro mera apprensione materiale, ma si sviluppano lungo una filiera complessa: dalla captazione grezza e generalizzata si passa, infatti, a un trattamento selettivo, operato mediante parole chiave, criteri di ricerca e filtri semantici che determinano quali dati saranno valorizzati nel successivo

sviluppo dell'accusa¹⁰. È in questa fase di selezione e interpretazione che la prova digitale inizia a prendere forma. Ed è qui che la logica del contraddittorio dovrebbe iniziare a esercitare un'efficacia anticipata, in quanto strumento imprescindibile per garantire la correttezza epistemica del procedimento¹¹.

Da tempo, la giurisprudenza europea ha richiamato l'attenzione su questo snodo. In particolare, la Corte europea dei diritti dell'uomo e la Corte di giustizia dell'Unione europea hanno ribadito che l'acquisizione e il trattamento dei dati, specie se massivi e suscettibili di interferire con diritti fondamentali, devono avvenire sotto il controllo di un giudice o di un'autorità indipendente (incluso questo predicato anche il requisito della "neutralità", concetto assimilabile alla terzietà, volendo trasporlo all'interno del nostro ordinamento). Questo controllo non può essere meramente formale, né limitato alla sola fase iniziale dell'apprensione: esso, al contrario, deve accompagnare l'intero percorso che porta il dato grezzo a trasformarsi in mezzo di prova. Al tempo stesso, la difesa deve poter accedere, in fase successiva, a forme di documentazioni (nella realtà del nostro sistema, si deve ipotizzare, a verbali) capaci di dare conto di tale percorso, così da poter permettere di verificare – e, se del caso, contestare – le modalità attraverso le quali gli elementi di prova sono stati selezionati, organizzati, interpretati.

Sotto questo profilo, la disciplina italiana si presenta ancora largamente inadeguata. Il pubblico ministero può disporre il sequestro dei dati informatici con un margine di libertà significativo, senza che siano previste forme di controllo sostanziale sul successivo trattamento degli stessi. A questo proposito, va messo in chiaro che, sì, il nostro ordinamento predispone di uno strumento efficace – il riesame – concernente la prima apprensione¹²: questa forma di impugnazione, sagomata sulla idea del gravame puro, indubbiamente permette a chi ne abbia subito le conseguenze di rimettere in discussione in radice l'an e il *quomodo* della apprensione originaria¹³ (si tratta di una forma di rimedio che certamente soddisfa i requisiti di effettività pretesi

¹⁰ Cfr. J.J. Oerlmans, S. Royer, *The future of data-driven investigations in light of the Sky ECC operation*, in *New Journal of European Criminal Law*, 2023, p. 447. Cfr. anche R. Brighi, M. Ferrazano, *Digital Forensics: Best Practices and Perspective*, in M. Caianiello, A. Camon (eds.), *Digital Forensic Evidence. Towards Common European Standards in Antifraud Administrative and Criminal Investigations*, Padova, 2021, p. 13 s.

¹¹ Sia consentito qui il rinvio a M. Caianiello, *Conclusive Remarks*, in M. Caianiello, A. Camon (eds.), *Digital Forensic Evidence. Towards Common European Standards*, cit., p. 254. Cfr., inoltre, G. Lasagni, *Admissibility of Evidence in Criminal Proceedings: Lessons (and Problems) from the "Data Retention Saga"*, in L. Bachmaier Winter, F. Salimi (eds.), *Admissibility of Evidence in EU Cross-Border Criminal Proceedings. Electronic Evidence, Efficiency and Fair Trial Rights*, Dublin-New York, 2024, p. 35.

¹² Strumento, come noto, aperto anche ai terzi che abbiano diritto alla "restituzione" delle cose sequestrate, qui da intendere, sulla scia delle Sezioni Unite 20 luglio 2017, n. 40963, riferite alla esclusiva disponibilità dei dati.

¹³ Cfr. F. Tacconi, *Art. 324 c.p.p.*, in G. Illuminati, L. Giuliani, *Commentario breve al codice di procedura penale*, Padova, 2020, p. 1561. V., prima ancora, R. Adorno, *Il riesame delle misure cautelari reali*, Milano, p. 418 s.

dalle Carte europee come pochi altri, nel panorama continentale)¹⁴. Manca, invece, un presidio per quel che concerne la lavorazione successiva, vale a dire l'opera progressiva di trattamento che deve condurre alla selezione delle prove, relativamente alle quali la legge non predispone prescrizioni in grado di assicurare una piena *disclosure* del percorso compiuto dagli inquirenti. Ne deriva un potenziale squilibrio, in cui la parte pubblica detiene un vantaggio informativo ed epistemico significativo, che rischia di compromettere la parità delle armi e l'equilibrio dialettico del processo.

In tale scenario, la proposta di introdurre l'art. 254-ter c.p.p. si colloca come tentativo, pur ancora imperfetto, di allineamento con i principi europei¹⁵. Essa prevede, anzitutto, che il sequestro di dispositivi digitali sia subordinato a un'autorizzazione del giudice per le indagini preliminari, con ciò recependo la richiesta, di elaborazione giurisprudenziale europea, relativa alla necessità di assicurare un previo controllo esterno da parte di un'autorità imparziale (requisito che, vale la pena ribadirlo, implica anche nella accezione sovranazionale quello della neutralità-terzietà): controllo e autorizzazione che divengono duplici, seguendo l'insegnamento della Corte costituzionale (sent. n. 170 del 2023), nel caso in cui, una volta appreso il dispositivo, il pubblico ministero abbia necessità di acquisire «dati inerenti a comunicazioni, conversazioni o corrispondenza informatica».

Ma l'elemento più interessante della proposta consiste nella centralità riconosciuta al principio di proporzionalità¹⁶. La misura deve essere giustificata in rapporto agli scopi perseguiti, e, significativamente, può essere disposta solo se funzionale alla prosecuzione delle indagini. È dunque esclusa – almeno in linea teorica – la possibilità di disporre sequestri esplorativi, finalizzati a scoprire se vi sia qualcosa che meriti di essere indagato. In tal modo, si mette al bando l'uso dell'investigazione digitale come strumento di *fishing expedition*, che altera il corretto ordine logico del procedimento probatorio anche in sede di indagine, aggirando il vincolo della pertinenza-rilevanza, che deve essere rispettato anche in questa fase¹⁷.

Merita inoltre di essere sottolineata la previsione secondo cui il sequestro può essere revocato quando, anche per fatti sopravvenuti, vengano meno i presupposti

¹⁴ Naturalmente, altri paesi hanno forme di controllo comparabili con la nostra. Cfr. S. Gless, T. Whal, *The Handling of Digital Evidence in Germany*, in M. Caianiello, A. Camon (eds.), *Digital Forensic Evidence*, cit., p. 75. V. anche K. Ligeti, G. Robinson, *The Handling of Digital Evidence in Luxembourg*, *ivi*, p. 140.

¹⁵ Cfr. A. Chelo, *Tanto tuonò che piovve: il nuovo sequestro di dispositivi informatici*, in *Riv. pen. dir. e proc.*, *Riv. trim.*, 2024, p. 29 s.

¹⁶ Principio che gioca in questa disposizione un ruolo cruciale, considerato che l'art. 254-ter c.p.p. sembrerebbe permettere l'accesso non solo ai dati contenuti nel dispositivo sequestrato, ma anche a quelli accessibili da remoto proprio grazie al dispositivo appreso. In tale maniera, il perimetro dei dati potenzialmente acquisibili attraverso questa forma di sequestro si allarga in maniera considerevole (oltretutto, permettendo di bypassare le previsioni normative che regolano la acquisizione di dati da un *service provider*, come l'art. 254-bis c.p.p. o l'art. 132 cod. *privacy*).

¹⁷ M. Nobili, *Art. 187 c.p.p.*, in M. Chiavario (a cura di), *Commento al nuovo codice di procedura penale*, vol. II, Torino, 1990, p. 390; D. Negri, *Fumus commissi delicti. La prova per le fattispecie cauleari*, Torino, 2004, p. 46 s.

che ne avevano giustificato l'adozione. La previsione può essere apprezzata, forse, non tanto per il contenuto della prescrizione, tutto sommato già presente nel sistema attraverso l'art. 262, comma 1, c.p.p., quanto per la perentorietà dei termini nei quali essa si esprime: termini che lasciano intendere come i dati vadano trattenuti per il minor tempo possibile, tanto da dover essere "restituiti" (da intendere come cancellati, nella lezione delle Sezioni unite¹⁸) non appena appaia venir meno il vincolo della rilevanza. Si ribadisce così, in termini sensibilmente più stringenti, il carattere dinamico della misura, la quale deve continuare a rispondere a un'esigenza attuale e concreta di indagine, pena la sua illegittimità sopravvenuta. L'idea della restituzione immediata, volendo, può anche essere interpretata come punto di emersione della proporzionalità – sotto il profilo della idoneità e, soprattutto, stretta necessità – da cui discende un obbligo di operare rapidamente la restituzione di ciò che è irrilevante, pena la compressione ingiustificata di un diritto costituzionale inviolabile, rientrando nei parametri degli artt. 14 e 15 della nostra Carta fondamentale.

Più importante ancora appare poi il tentativo di introdurre un modulo di contraddittorio anticipato, mediante la previsione di una procedura assimilabile, per struttura e garanzie, a quella degli accertamenti tecnici irripetibili. La duplicazione dei dispositivi sequestrati avviene alla presenza delle parti, che possono nominare consulenti tecnici abilitati a partecipare alle operazioni. In tal modo, si cerca di evitare che la creazione della copia forense – momento decisivo nella costruzione della prova digitale – avvenga in un contesto totalmente unilaterale.

Se questo tentativo è meritorio, la proposta presenta tuttavia significativi limiti. Non vi è, ad esempio, una previsione espressa che subordini all'autorizzazione del giudice l'utilizzo delle parole chiave o dei criteri di ricerca con cui i dati vengono esplorati e analizzati. Eppure, è proprio in questa attività che si condensa la capacità selettiva e interpretativa dell'investigazione, e che, dunque, si gioca gran parte della sua affidabilità e correttezza.

Inoltre, le garanzie previste per l'accertamento tecnico sono escluse – o possono essere escluse – nei casi di maggiore gravità, seguendo una logica emergenziale che, paradossalmente, sacrifica le garanzie proprio dove il loro presidio dovrebbe essere più saldo¹⁹. Infine, manca la possibilità per la persona sottoposta ad indagini di invocare il meccanismo atto a innescare l'incidente probatorio: quest'ultima scelta può apparire comprensibile, nella ottica di bilanciamento nella quale il legislatore si è probabilmente posto, tra tutela delle prerogative della difesa e assicurazione della efficienza dell'indagine. È possibile, in questa prospettiva, che abbia giocato un ruolo il timore di richieste in senso lato a carattere dilatorio, oppure anche solo la necessità di non gravare oltre misura gli uffici dei g.i.p., sui quali già pesa il

¹⁸ Cfr. Cass., Sez. un., 20 luglio 2017, n. 40963, cit.

¹⁹ Infatti, quando si procede per reati di una certa gravità o siano in pericolo la vita, la incolumità di una persona o la sicurezza dello Stato, l'intera procedura partecipata di duplicazione può essere derogata, stando al comma 10.

controllo autorizzativo preteso dal comma 1 del nuovo art. 254-ter c.p.p. Non v'è dubbio che la strada di un coinvolgimento del giudice per le indagini preliminari, nel *mare magnum* della apprensione dei dati – anticipata con la riforma dell'art. 132 cod. *privacy* – per quanto necessaria, alla luce della giurisprudenza europea, rischi di mettere sotto significativa pressione l'ufficio giudicante designato al presidio del rispetto dei diritti individuali nel corso delle indagini. Tuttavia, l'esclusione in radice di questa figura non persuade, posto che si potrebbero ipotizzare criteri di ammissibilità della eccezione di incidente probatorio tali da permettere di ammettere soltanto le richieste effettivamente necessarie: quelle in cui, in sostanza, un presidio del perito nominato dal giudice appaia effettivamente la scelta più appropriata, in vista della salvaguardia successiva della ammissione dei dati come prova in dibattimento.

Va comunque detto che, al di là delle luci e delle ombre che riguardano la proposta in discussione sull'art. 254-ter c.p.p., se mai esso verrà approvato, permane un disordine sistemico più ampio, in relazione alla legislazione concernente le indagini informatiche. Il quadro normativo italiano risulta frammentato, stratificato nel tempo, e spesso non coordinato. Solo per fare una breve ricapitolazione, un giurista deve oggi confrontarsi con l'art. 132 cod. *privacy*, che regola l'accesso ai dati conservati presso i gestori dei servizi; ad esso si aggiunge poi l'art. 254-bis c.p.p. – mai formalmente abrogato – che continua a consentire al pubblico ministero di acquisire dati informatici con proprio decreto, in contrasto con i principi affermati a livello europeo. La giurisprudenza, inoltre, ammette ancora l'uso del captatore informatico (*trojan*) in assenza di una disciplina organica, affidandosi a interpretazioni giurisprudenziali che suppliscono al silenzio del legislatore: captatore che, quando usato per scopi diversi dalle intercettazioni, non incontra i limiti previsti dalla legge 266, comma 2-bis, 267, comma 1 e 2-bis e 268, comma 3-bis c.p.p. (semmai, per quel che riguarda le perquisizioni informatiche in *real-time*, bastando il solo decreto motivato del pubblico ministero). In materia di sorveglianza in tempo reale sui dati e le informazioni bancarie, infine, si deve fare riferimento al regime delle intercettazioni, richiamato dall'art. 20 del d.lgs. n. 108/2017 di attuazione della direttiva sull'ordine europeo di indagine, regime che, per le ragioni già espresse in altra sede, deve valere, sul piano ermeneutico, anche per analoghe operazioni meramente interne²⁰. Infine, non va trascurato che, per quel che concerne il pedinamento elettronico, esso è considerato dalla giurisprudenza libero e non assoggettato ad alcun controllo da parte della autorità giudiziaria²¹. Questa situazione di frammentazione normativa, determinata per lo più da interventi settoriali e reattivi, vale a dire cagionati dalla necessità di mettere una toppa a un sistema largamente incompleto in una prospettiva d'emergenza, non consente di governare in modo coerente il fenomeno delle indagini digitali. Occorrerebbe, al contrario, una

²⁰ Cfr. M. Caianiello, *L'attuazione della direttiva sull'ordine europeo di indagine penale e le sue ricadute nel campo del diritto probatorio*, in *Cass. pen.*, 2018, pp. 2205-2207.

²¹ Cfr. F. Iovene, *Pedinamento satellitare e diritti fondamentali della persona*, in *Cass. pen.*, 2012, p. 3556.

riforma di respiro sistematico, capace di costruire un quadro di principi generali applicabili a ogni forma di acquisizione, trattamento e conservazione dei dati in ambito procedimentale penale. Solo a partire da una simile architettura normativa sarà possibile elaborare regole tecniche e procedurali specifiche per ciascuna delle attività investigative “*data-driven*”. In assenza di questo passaggio fondativo, il rischio è quello di inseguire la realtà tecnologica con strumenti giuridici insufficienti, condannando la giustizia penale a una perenne condizione di rincorsa.

Alla luce di queste evidenze, sembra ormai giunto il momento di riscrivere in maniera organica l'intera disciplina relativa all'apprensione dei dati nel processo penale. Non si tratta più di intervenire con correttivi parziali o aggiornamenti puntuali, ma di compiere un vero e proprio salto di sistema, orientato a costruire un impianto normativo coerente con la complessità delle tecnologie attuali e con le garanzie pretese dal diritto europeo. In questa prospettiva, vi sono almeno due snodi fondamentali che dovrebbero costituire i pilastri della riforma. In primo luogo, occorre prevedere in via generalizzata l'intervento del giudice quale garante imparziale della legalità dell'apprensione dei dati, superando definitivamente il modello che si accontenta del mero decreto del pubblico ministero. Il controllo giurisdizionale, per essere effettivo, deve intervenire non solo nella fase iniziale del sequestro, ma accompagnare le principali fasi di trattamento e selezione del materiale informatico, secondo una logica di vigilanza continua e sostanziale. In tal modo, si darebbe finalmente piena attuazione ai principi espressi dalla giurisprudenza della Corte di giustizia dell'Unione europea, che esige la presenza di un'autorità terza e indipendente in grado di valutare, caso per caso, la proporzionalità e la necessità dell'ingerenza. In secondo luogo, risulta ormai anacronistica la distinzione tra dati esterni (c.d. metadati) e contenuto delle comunicazioni, sulla quale si è a lungo fondata la differenziazione del regime delle garanzie²².

L'evoluzione tecnologica e la natura massiva della raccolta dei dati hanno ormai reso evidente che la potenzialità informativa di un insieme strutturato di dati esterni può eguagliare – se non addirittura superare – quella delle tradizionali intercettazioni. Tracciati di accesso, geolocalizzazioni, *log* di connessione, cronologie d'uso: tutti questi elementi, se osservati in combinazione, consentono una ricostruzione dettagliata e dinamica della vita dell'individuo, tale da rendere insostenibile, sul piano costituzionale ed eurounitario, un trattamento differenziato in termini di garanzie. Una riforma complessiva della materia non può dunque eludere la necessità di adeguare le categorie giuridiche alla realtà tecnologica. Solo riconoscendo la pari (o, talora, persino superiore) invasività del dato esterno rispetto al contenuto si potrà costruire un sistema di garanzie realmente proporzionato all'interesse in gioco, capace di bilanciare le esigenze investigative con i diritti fondamentali della persona²³. È in

²² Cfr. G. Lasagni, *Dalla riforma dei tabulati a nuovi modelli di integrazione fra diritti di difesa e tutela della privacy*, in *Legisl. pen.*, 2022, p. 8.

²³ Va anche considerato che con l'avvento e il progressivo espandersi delle tecniche di criptazione l'impossibilità di accedere ai contenuti farà sì che i metadati acquisiranno sempre più importanza.

questo rovesciamento di prospettiva – che impone di ripensare le fonti, le soglie di controllo e i regimi autorizzativi – che si misura oggi la sfida più rilevante per il diritto processuale penale nell'era digitale.

4. Contraddittorio e uso di IA

Nel contesto dell'evoluzione digitale del processo penale, merita una riflessione specifica anche l'uso, attuale o prospettico, di sistemi di intelligenza artificiale. L'impiego dell'IA in ambito giudiziario – sia in fase investigativa, sia in sede valutativa o predittiva – pone sfide inedite in termini di tutela del contraddittorio, dal momento che le indicazioni elaborate da tali sistemi rischiano di essere recepite come oggettive, neutre o scientificamente indiscutibili²⁴. L'affidamento alla cosiddetta scatola nera algoritmica, cioè a un apparato di calcolo il cui funzionamento interno è spesso opaco o non esplicitabile, può produrre una sostanziale deresponsabilizzazione dell'organo che ne assume i risultati, oltre a precludere un effettivo scrutinio da parte della difesa. In questo quadro, pare opportuno spostare il baricentro del problema: più che insistere sulla *disclosure* del codice sorgente – esigenza comprensibile, ma talvolta tecnicamente irrealizzabile o, comunque, poco significativa ai fini della comprensione del funzionamento concreto dell'IA²⁵ – sarebbe preferibile riformulare le garanzie del contraddittorio in una chiave diversa. In questa prospettiva, ciò che conta potrebbe essere non tanto sapere “come funziona” l'algoritmo, o come esattamente è stato disegnato, quanto poter discutere e mettere alla prova i risultati che esso produce. A tal fine, come è stato efficacemente osservato, si potrebbe pensare a un nuovo paradigma di verifica, fondato su un contraddittorio tra sistemi di IA comparabili²⁶. Se un sistema di intelligenza artificiale ha prodotto un determinato *output* (ad esempio, una correlazione tra dati, una ricostruzione temporale o una classificazione di contenuti), le parti dovrebbero poter essere autorizzate ad introdurre, nel processo, i risultati ottenuti da altri sistemi – configurati con parametri simili, ma indipendenti – così da confrontare, confermare o eventualmente confutare le conclusioni tratte sulla base del primo. Non sarebbe in questa maniera tanto la trasparenza dell'algoritmo in sé a garantire la correttezza dell'analisi, bensì la possibilità di sottoporre i suoi esiti a una verifica dialettica, tecnicamente controllabile e metodologicamente riproducibile, in

²⁴ S. Quattrocchio, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Switzerland, 2020, p. 67. Cfr., volendo, M. Caianiello, *Dangerous Liaisons. Potentialities and risks deriving from the interaction between Artificial Intelligence and preventive justice*, in 29 *European Journal of Crime, Criminal law and Criminal Justice*, 2021, p. 3 s.

²⁵ Cfr. G. Sartor, *L'intelligenza artificiale e il diritto*, Torino, 2017, p. 59.

²⁶ G. Contissa, G. Lasagni, *When it is (also) Algorithms and AI that decide on Criminal Matters: In Search of an Effective Remedy*, in 28(3) *European Journal of Crime, Criminal Law and Criminal Justice*, 2020, p. 280 s.

senso lato ispirata alla idea della “prova contraria”: dove questa ultima sarebbe rappresentata dal secondo *test*, ammesso su richiesta della controparte in verifica della prova per IA prodotta dalla parte istante.

Naturalmente, ciò non significa che lo scrutinio sulla credibilità del sistema di IA, alla luce del modo in cui è stato concepito (incluso, se del caso, il codice sorgente), dei dati sui quali si è allenato, del contesto sociale nel quale è stato concepito e realizzato, non possano mai avere significato. Al contrario, un simile dibattito certamente in numerosi casi continuerà ad essere cruciale, per non dire doveroso²⁷. Ciò che si intende valorizzare, tuttavia, in questa sede, è un approccio diverso, capace di affiancarsi al precedente, che potremmo definire di “contraddittorio algoritmico per analogia”: esso avrebbe il pregio di preservare il principio della formazione della prova nel contraddittorio delle parti (art. 111, comma 4, Cost.), adattandolo, tuttavia, attraverso la soluzione proposta, a un contesto in cui la fonte dell’informazione non è più la dichiarazione umana, ma costituisce la risultanza elaborata da un sistema computazionale. In questo senso, la discussione dialettica tra le parti, che certamente deve continuare ad avere luogo²⁸, potrebbe giovare anche di forme di raffronto tra diversi sistemi di IA, in grado confermare o smentire l’ipotesi indicata dal modello usato in origine da una delle parti per sostenere le proprie tesi.

²⁷ K. Ligeti, *Ensuring Fair Trial in the Digital World*, in M. Bergström, V. Mitsilegas (eds.), *EU Law in the Digital Age*, Dublin/New York, 2025, p. 239. Va altresì tenuto presente che il nuovo Regolamento sull’IA (il c.d. *AI Act* – Reg. EU 2024/1689) introduce, a partire dall’art 8, una serie di obblighi per i fornitori di servizi ad alto rischio (quali quelli per l’analisi e la valutazione delle prove) che dovrebbero, in primo luogo, imporre una *disclosure* su come questi sistemi sono stati concepiti, e, in secondo, consentire una comparazione dei due sistemi da parte del giudice, nell’ipotesi in cui le parti propongano un contraddittorio sugli *output* di sistemi di IA alternativi, nel senso che si è appena richiamato.

²⁸ Nuovi modi di esercitare il diritto al controesame sono esemplificati da A. Roth, *Machine Testimony*, in 126 *The Yale Law Journal*, 2017, p. 1972 (in particolare v. p. 2050). Citando il passaggio testualmente: «Il diritto a contrastare la credibilità in modo significativo di una fonte non umana potrebbe richiedere molto di più, o di meno, di un esame in aula. Il controesame specifico del programmatore responsabile della progettazione di un pacchetto software potrebbe non essere necessario per sondare il potenziale della macchina in termini di falsità per progettazione, inarticolazione o errore analitico dovuto a una cattiva progettazione o a un errore. Invece, il programmatore potrebbe testimoniare dal vivo davanti a un qualche tipo di commissione scientifica, e ritornare alla commissione ogni volta che il software viene modificato o aggiornato. Una commissione di questo tipo potrebbe raccomandare le strutture contraddittorie esistenti, ma una proposta simile di “tribunali consultivi” per valutare le testimonianze di esperti in conflitto è stata avanzata da Learned Hand oltre un secolo fa [...] D’altra parte, una azione efficace di verifica della credibilità di una macchina in un determinato caso potrebbe richiedere l’accesso al codice sorgente o, in alternativa, risposte scritte a domande che sono formulate da esseri umani ma che interrogano la macchina come se fosse in un controesame, come ad esempio “quali statistiche di frequenza della popolazione stai usando per calcolare il tuo rapporto di verosimiglianza?” o “quale soglia usi per decidere cosa chiamare un marcatore genetico rispetto al ‘rumore’?”. Un “*impeachment*” significativo potrebbe anche includere, ove possibile, la presenza di un esperto della difesa al momento del *test* per scoraggiare ed eliminare gli errori di *input* specifici del caso» (trad. nostra, avvalendosi di DeepL e verificandone a posteriori il risultato).

5. Conclusioni

Pur in un conteso in veloce mutamento, a causa delle trasformazioni prodotte dall'avvento delle tecnologie digitali e delle investigazioni *data-driven*, il principio del contraddittorio non può ancora dirsi oggi in pericolo di sopravvivenza. Piuttosto, esso sta conoscendo un processo di metamorfosi, che impone una riflessione attenta sulle sue nuove modalità di concretizzazione. Il contraddittorio, insomma, non è (ancora) scomparso: sta, più semplicemente, cambiando forma. Sul piano dibattimentale, esso continua a svolgere una funzione fondamentale, anche in presenza di prove digitali. La prova dichiarativa, in particolare, ha assunto una configurazione composita, che fonde elementi tipici della testimonianza classica con tratti propri della prova per esperti. Ne nasce una figura ibrida – a metà tra il testimone, il consulente tecnico e il perito – che impone una gestione sapiente dell'esame e del controesame, così da garantire l'effettivo esercizio del diritto alla prova.

È tuttavia nelle indagini preliminari che si gioca la sfida più delicata. Qui, la possibilità di garantire forme adeguate di contraddittorio richiede un duplice sforzo. Da un lato, occorre coinvolgere la difesa già nel momento dell'apprensione dei dati, secondo modelli partecipativi anticipati, come quelli, magari migliorati rispetto alla versione attuale, proposti nell'art. 254-ter c.p.p. in corso di discussione. Dall'altro, è essenziale assicurare un pieno accesso alle modalità di trattamento dei dati: ciò significa, ad esempio, comunicare alle parti le parole chiave utilizzate, i criteri di selezione applicati, le tecniche di ordinamento e filtraggio adottate dagli inquirenti. In assenza di tali informazioni, il contraddittorio rischia di diventare uno strumento ineffettivo, perché usato senza le preve informazioni necessarie.

Infine, con riferimento ai sistemi di intelligenza artificiale, la tutela del contraddittorio può – e, talora, deve – realizzarsi attraverso la possibilità di confronto tra sistemi analoghi: una forma di verifica che consenta di mettere in discussione i risultati generati da un sistema IA confrontandoli con quelli prodotti da altri strumenti simili. In tal modo, l'intelligenza artificiale non si configura come fonte indiscutibile, ma come prodotto epistemico aperto alla dialettica processuale (dialettica che può servirsi anche di sistemi di IA alternativi, in funzione di *test* di quello introdotto dalla parte interessata).

In conclusione, il processo penale è chiamato a misurarsi con un mutamento profondo degli scenari conoscitivi. L'elemento umano nella formazione della prova non appare, al momento, in pericolo di vita. Ma rischia di diventarlo, se il legislatore e gli interpreti non sapranno cogliere – e governare – le sfide poste dalla trasformazione tecnologica in atto. Occorre, dunque, accettare il cambiamento senza demonizzarlo, ma al tempo stesso senza arretrare rispetto ai principi costituzionali che presidiano il giusto processo. Il contraddittorio può sopravvivere all'era digitale. Ma solo se sarà in grado di evolvere con essa.