UNIVERSITÀ
DI TRENTO

INDAGINI E PROVE NELLA SOCIETÀ DIGITALE

QUESTIONI ATTUALI E PROSPETTIVE FUTURE

a cura di
GABRIELLA DI PAOLO
LUCA PRESSACCO

2025

UNIVERSITÀ DI TRENTO
Facoltà di Giurisprudenza

QUADERNI DELLA FACOLTÀ DI GIURISPRUDENZA

95

2025

Al fine di garantire la qualità scientifica della Collana di cui fa parte, il presente volume è stato valutato e approvato da un *Referee* interno alla Facoltà a seguito di una procedura che ha garantito trasparenza di criteri valutativi, autonomia dei giudizi, anonimato reciproco del *Referee* nei confronti di Autori e Curatori.

PROPRIETÀ LETTERARIA RISERVATA

© Copyright 2025
by Università degli Studi di Trento
Via Calepina 14 - 38122 Trento

ISBN 978-88-5541-113-4
ISSN 2284-2810

Libro in Open Access scaricabile gratuitamente dall'archivio IRIS - Anagrafe della ricerca (https://iris.unitn.it/) con Creative Commons Attribuzione-Non commerciale-Non opere derivate 3.0 Italia License.
Maggiori informazioni circa la licenza all'URL:
http://creativecommons.org/licenses/by-nc-nd/3.0/it/legalcode

Il presente volume è pubblicato anche in versione cartacea,
con il contributo della Facoltà di Giurisprudenza
dell'Università di Trento,
per i tipi di Editoriale Scientifica - Napoli
con ISBN 979-12-235-0292-1.

Giugno 2025

INDAGINI E PROVE NELLA SOCIETÀ DIGITALE

QUESTIONI ATTUALI E PROSPETTIVE FUTURE

a cura di
GABRIELLA DI PAOLO
LUCA PRESSACCO

Università degli Studi di Trento 2025

INDICE

Pag.

Gabriella Di Paolo
Prefazione 1

Gli Autori 3

Gabriella Di Paolo
Comunicazioni digitali e prova penale. Note introduttive 5

Alberto Camon
I confini mobili delle intercettazioni 9

Federica Iovene
I dati esterni delle comunicazioni: tendenze evolutive 27

Giulio Illuminati
Circolazione probatoria interna e transfrontaliera. Note introduttive 45

Luigi Giordano
La circolazione degli esiti delle intercettazioni in altri procedimenti interni. I riflessi della sentenza delle sezioni unite "Cavallo" sulla giurisprudenza successiva 53

Rosanna Belfiore
L'acquisizione transfrontaliera di prove digitali 81

Marianna Biral
Intercettazioni e tutela di terzi estranei al procedimento 97

Pag.

Fabio Cassibba
Indagini tecnologicamente assistite e tecniche investigative speciali. Note introduttive 115

Elisa Lorenzetto
I sequestri di smartphone*, dispositivi informatici e memorie digitali* 119

Silvia Signorato
La geolocalizzazione: tecniche e garanzie 139

Pasquale Bronzo
Le operazioni sotto copertura nel web 173

Jacopo Della Torre
Indagini penali e criptovalute 203

Antonino Alì
Backdoor *nei sistemi crittografici tra esigenze di sicurezza e diritti umani* 253

Luca Pressacco
Gli elementi di prova generati o raccolti tramite intelligenza artificiale. Considerazioni metodologiche 273

PREFAZIONE

Gabriella Di Paolo

Il presente volume raccoglie le relazioni e gli interventi svolti nel corso dell'incontro di studio «Indagini e prove nella società digitale. Questioni attuali e prospettive future», tenutosi a Trento il 26 e 27 settembre 2024, nell'ambito delle iniziative legate al Dipartimento d'eccellenza 2023-2027.

Il Convegno – organizzato dalla Facoltà di Giurisprudenza dell'Università di Trento in collaborazione con la Scuola Superiore della Magistratura (struttura didattica territoriale del Distretto di Corte d'Appello di Trento), sotto il patrocinio della Camera penale di Trento "Michele Pompermaier" e dell'Associazione italiana studiosi della prova (A.I.S.P.) – rappresenta l'ultimo di una serie di incontri dedicati alla materia probatoria, organizzati nel corso degli anni presso l'Ateneo tridentino. L'iniziativa nasce dall'esigenza, fortemente avvertita sia in accademia che dagli operatori del diritto, di dedicare un momento di riflessione e approfondimento ai numerosi e complessi problemi posti dal crescente impiego di metodi di indagine a caratura tecnologica in "ambiente digitale".

In questa prospettiva, la prima parte del convegno è stata dedicata alle intercettazioni e all'acquisizione dei dati esterni delle "comunicazioni" in senso stretto, anche nell'ottica della circolazione dei relativi risultati tra i procedimenti penali nazionali e transfrontalieri. La seconda parte dell'iniziativa, invece, ha riguardato metodi investigativi (come i sequestri di dispositivi informatici e la geolocalizzazione) e tecniche d'indagine speciali (come le operazioni *undercover* nella rete e le indagini per fatti di reato connotati dall'uso di criptovalute per finalità illecite) che incidono su diritti fondamentali, per così dire, di "nuova generazione". Ne è emerso un quadro articolato e composito, il cui filo conduttore può essere ravvisato nella convinzione che sia improcrastinabile l'elaborazione di uno statuto dei nuovi mezzi di ricerca della

prova adeguato alle peculiarità dell'ambiente digitale e della c.d. *electronic evidence*.

Nel licenziare le bozze del presente volume, desidero rivolgere un ringraziamento sincero a tutti coloro che hanno reso possibile lo svolgimento del Convegno all'interno degli Enti organizzatori, alle associazioni che vi hanno idealmente aderito concedendo il loro patrocinio nonché, e soprattutto, a tutti i relatori e interventori, per l'impegno profuso al fine di consentire una tempestiva pubblicazione degli atti. Ringrazio infine sentitamente la dott.ssa Marianna Biral e il dott. Luca Pressacco, che hanno impreziosito graficamente il presente volume con il loro attento e insostituibile lavoro di *editing*.

Trento, il 28 febbraio 2025
G.D.P.

GLI AUTORI

ANTONINO ALÌ, Professore Associato di Diritto internazionale – Università di Trento

ROSANNA BELFIORE, Professoressa Associata di Diritto processuale penale – Università di Catania

MARIANNA BIRAL, Ricercatrice di Diritto processuale penale – Università di Trento

PASQUALE BRONZO, Professore Associato di Diritto processuale penale – Università di Roma, *La Sapienza*

ALBERTO CAMON, Professore ordinario di Diritto processuale penale – *Alma Mater Studiorum*, Università di Bologna

FABIO SALVATORE CASSIBBA, Professore Ordinario di Diritto processuale penale – Università di Parma

JACOPO DELLA TORRE, Professore Associato di Diritto processuale penale – Università di Genova

GABRIELLA DI PAOLO, Professoressa Ordinaria di Diritto processuale penale – Università di Trento

LUIGI GIORDANO, Magistrato – Procura generale presso la Corte di Cassazione

GIULIO ILLUMINATI, già Professore Ordinario di Diritto processuale penale – *Alma Mater Studiorum*, Università di Bologna

FEDERICA IOVENE, Magistrato – Procura della Repubblica presso il Tribunale di Bolzano

ELISA LORENZETTO, Professoressa Associata di Diritto processuale penale – Università di Verona

LUCA PRESSACCO, Ricercatore di Diritto processuale penale – Università di Trento

SILVIA SIGNORATO, Professoressa Associata di Diritto processuale penale – Università di Padova

GLI ELEMENTI DI PROVA GENERATI O RACCOLTI TRAMITE INTELLIGENZA ARTIFICIALE

CONSIDERAZIONI METODOLOGICHE

Luca Pressacco

SOMMARIO: *1. Processo penale e intelligenza artificiale: intersezioni. 2. La c.d. "prova algoritmica". 3. Intelligenza artificiale e prova penale: opportunità e rischi. 4. Le decisioni fondate su trattamenti automatizzati. 5. Intelligenza artificiale e "ciclo probatorio".*

1. Processo penale e intelligenza artificiale: intersezioni

Le tecnologie di intelligenza artificiale possono contribuire in vario modo all'esercizio della funzione giurisdizionale. In una prospettiva puramente gestionale, i *software* basati sull'intelligenza artificiale potrebbero essere impiegati per agevolare l'amministrazione degli uffici giudiziari e la distribuzione dei carichi di lavoro al loro interno. Gli strumenti in questione potrebbero, inoltre, rivelarsi utili per coadiuvare il giudice e i suoi ausiliari nelle attività d'udienza, a partire dalla redazione del verbale, oppure per la gestione e la consultazione dei fascicoli processuali, nonché per la traduzione degli atti in essi compresi[1].

A titolo esemplificativo, è possibile immaginare sistemi esperti che semplifichino il lavoro svolto dai funzionari giudiziari, estraendo auto-

[1] Per un inquadramento teorico di questi profili, v. G. UBERTIS, *Processo penale telematico, intelligenza artificiale e Costituzione*, in *Cass. pen.*, 2024, p. 439 ss. L'autore osserva che «il processo penale telematico non può in linea di principio riguardare lo svolgimento della forma processuale tipica, che è costituita dal dibattimento; questo è caratterizzato tra l'altro dai principi di immediatezza e di oralità, poco consoni (per dirla eufemisticamente) a una relazione unicamente tecnologica tra i protagonisti dell'evento processuale, ed è al più possibile che i suoi atti siano documentati (ma non compiuti) informaticamente».

maticamente dalla notizia di reato e inserendo nel relativo registro tutti i dati funzionali alle doverose iscrizioni[2], oppure ordinando e indicizzando gli atti e i documenti presenti all'interno dei fascicoli processuali.

Analogamente, per quanto riguarda l'esercizio della funzione giurisdizionale, sarebbero molto utili *software* progettati per calcolare i termini di prescrizione o di durata delle misure cautelari personali, nonché applicativi idonei ad assistere il giudice nell'impostazione e nella compilazione automatica della parte c.d. enunciativa dei provvedimenti giurisdizionali[3], senza trascurare le banche dati orientate alla ricerca giurisprudenziale. Si tratta di scenari indubbiamente promettenti, visto che le tecnologie in esame forniscono prestazioni eccellenti – di gran lunga superiori a quelle umane – quando si tratta di sintetizzare testi, compilare documenti standardizzati e svolgere attività ripetitive, basate sull'applicazione vincolata di regole logiche, matematiche o informatiche[4].

---

[2] Si rammenta che il registro delle notizie di reato è costituito, a sua volta, da un applicativo informatico: il c.d. *Re.Ge Web*, acronimo di Registro generale delle notizie di reato, che – unitamente al c.d. *BDMC* (Banca dati delle misure cautelari) – compone il c.d. *SICP*, vale a dire il Sistema informativo della cognizione penale.

[3] La parte enunciativa della sentenza, usualmente contrapposta a quella espositiva (ossia la motivazione) e a quella dispositiva (consistente nell'ordine del giudice), è composta: dall'intestazione del provvedimento, dall'indicazione dell'autorità giurisdizionale che lo ha pronunciato, dalle generalità dell'imputato e delle altri private (nonché dalle altre informazioni complementari concernenti, per esempio, il difensore e il domicilio), dall'imputazione e dall'indicazione delle richieste o conclusioni rassegnate dalle parti (cfr. l'art. 546, co. 1, lett. *a-d* c.p.p.). A ciò, nella prassi, si aggiunge sovente il riassunto per sommi capi dello svolgimento processuale, non previsto dalle disposizioni legislative, ma considerato utile per l'organizzazione razionale della motivazione.

[4] Persino un commentatore fortemente scettico nei confronti della penetrazione dell'intelligenza artificiale nel contesto processuale – poiché considerata sintomatica di una «nuova tendenza alla gestione economico-aziendalistica degli affari penali», che condurrà fatalmente a un distopico rito artificiale – è disposto ad ammettere che «il gigantismo digitale delle informazioni processuali renderà ineludibile l'impiego di sistemi algoritmici sempre più evoluti per la gestione di una mole di dati che supera le capacità umane»; riconoscendo in conclusione che, da questo punto di vista, la trasformazione digitale «presenta anche aspetti di segno positivo, in quanto le tecnologie, a regime, dovrebbero effettivamente semplificare alcune attività processuali»: O. MAZZA, *Distopia del processo artificiale*, in *Archivio penale* (rivista web) 7 gennaio 2025 (ultimo accesso il 28 febbraio 2025), da cui sono tratte le citazioni che precedono in nota (*ivi*, p. 2).

Ad ogni modo, se l'intelligenza artificiale entrerà nella prassi giudiziaria quotidiana, in che termini e con quali tempistiche dipenderà, in larga misura, dalle scelte (politiche, economiche, gestionali) compiute dalle autorità preposte all'organizzazione e al funzionamento dei servizi relativi alla giustizia (art. 110 Cost.), vale a dire in particolare dal Ministero della Giustizia e dal Consiglio superiore della Magistratura. Tali scelte, infatti, determineranno la propensione della pubblica amministrazione a investire nello sviluppo delle tecnologie in esame, promuovendone l'utilizzo anche nel settore giudiziario, storicamente refrattario alle innovazioni organizzative e tecnologiche[5].

In questa sede, tuttavia, non intendo soffermarmi su questi aspetti, che riguardano le applicazioni dirette dell'intelligenza artificiale in funzione di supporto alle variegate attività compiute dai soggetti processuali e, più in generale, dagli operatori coinvolti nel sistema di giustizia penale. L'intento, piuttosto, è quello di riflettere su una dimensione ulteriore di interferenza tra le nuove tecnologie e la giurisdizione penale. Mi riferisco, in particolare, all'ingresso sulla scena processuale di elementi di prova *generati*, *elaborati* o *raccolti* tramite *software* di *artificial intelligence*.

Questa intersezione, sebbene meno appariscente, non dovrebbe destare particolare stupore, visto che in dottrina è stato evidenziato a più riprese il nesso che intercorre tra il sistema probatorio processuale e l'orizzonte epistemologico (inteso come l'insieme delle pratiche conoscitive e delle credenze a esso associate) tipico di una determinata società[6]. Se dunque l'epoca contemporanea è caratterizzata da un prodigioso avanzamento delle tecnologie di intelligenza artificiale, che tendono a permeare ogni ambito della vita individuale e collettiva, allora è

[5] Per alcune considerazioni sul rapporto fra transizione digitale ed esercizio della funzione giurisdizionale, volendo, cfr. L. PRESSACCO, *Trasformazione digitale e funzione giurisdizionale*, in G. DI PAOLO (a cura di), *Trasformazioni della giustizia. Norme, organizzazione, tecnologie*, Napoli, 2024, p. 73 ss. Per un inquadramento generale dell'argomento, v. B. GALGANI, *Forme e garanzie nel prisma dell'innovazione tecnologica. Alla ricerca di un processo penale "virtuoso"*, Milano, 2022, *passim*.

[6] Cfr., per tutti, F. CORDERO, *Il giudizio d'onore*, Milano, 1959, p. 68 ss.; M. TARUFFO, *La semplice verità. Il giudice e la costruzione dei fatti*, Roma, 2009, p. 4 ss.; G. UBERTIS, *Profili di epistemologia giudiziaria*, Milano, 2021, p. 4 ss.

agevole prevedere che anche il sistema probatorio subirà gli effetti di questa significativa transizione.

Ciò impone di svolgere alcune considerazioni introduttive sulla c.d. "prova algoritmica". Non si pretende, ovviamente, di esaurire una tematica che dischiude molteplici prospettive di indagine[7], bensì di svolgere alcune brevi considerazioni di carattere metodologico, in coerenza con gli obiettivi propri di un intervento programmato.

2. La c.d. "prova algoritmica"

Il primo quesito, che sorge spontaneo, inerisce all'inquadramento concettuale della c.d. "prova algoritmica". Si tratta di una nuova categoria dogmatica, meritevole di considerazione autonoma e foriera di una specifica disciplina giuridica? Ritengo che la risposta a questa domanda debba essere individuata, come per ogni questione categoriale, prestando attenzione alle ricadute operative della qualificazione in esame e saggiando la capacità esplicativa della stessa.

Da questo punto di vista, giova segnalare come le prospettive d'impiego dell'intelligenza artificiale nell'ambito del procedimento penale abbiano già sospinto il legislatore a introdurre talune definizioni autonome, delineando fattispecie assistite da specifiche garanzie procedurali.

Un esempio significativo, in questa direzione, è costituito dalla c.d. "profilazione", che l'art. 2 lett. *e* d.lgs. 18 maggio 2018 n. 51[8] definisce come

[7] In altra sede, per esempio, si è già indagato sul rapporto fra intelligenza artificiale e ragionamento probatorio, in prospettiva epistemologica: cfr., volendo, L. PRESSACCO, *Intelligenza artificiale e ragionamento probatorio nel processo penale*, in *BioLaw Journal*, 2022, 4, p. 503 ss. (ora anche in G. DI PAOLO, L. PRESSACCO (a cura di), *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, Napoli, 2022, p. 91 ss.).

[8] Recante: «Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla 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, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio».

> qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Consapevole della portata altamente invasiva dei trattamenti automatizzati orientati alla profilazione delle persone fisiche nella sfera della loro riservatezza, l'art. 8 del medesimo d.lgs. n. 51/2018 stabilisce che

> sono vietate le decisioni basate unicamente su un trattamento automatizzato, compresa la profilazione, che producono effetti negativi nei confronti dell'interessato, salvo che siano autorizzate dal diritto dell'Unione europea o da specifiche disposizioni di legge. Le disposizioni di legge devono prevedere garanzie adeguate per i diritti e le libertà dell'interessato. In ogni caso è garantito il diritto di ottenere l'intervento umano da parte del titolare del trattamento.

Si avrà modo di tornare in seguito su quest'ultima disposizione[9]. Per il momento, ciò che interessa mettere in luce è che il legislatore, consapevole dell'attitudine degli strumenti in questione a convertirsi in autentiche "tecnologie del controllo", idonee a conculcare le libertà individuali, ha avvertito l'esigenza di introdurre una regolazione specifica per talune sue particolari applicazioni.

Ciò non toglie, tuttavia, che la prova generata o raccolta tramite strumenti di intelligenza artificiale possa essere utilmente ricondotta entro il *genus* della prova scientifica e, in particolare, nel novero della c.d. prova digitale o informatica[10]. L'inquadramento dogmatico risulta proficuo poiché identifica gli snodi concettuali che non possono essere pretermessi nelle diverse fasi del procedimento probatorio, qualora vengano in rilievo elementi di prova siffatti.

---

[9] V. *infra*, par. 4.

[10] Nel medesimo senso, v. M. GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, p. 61 ss.

Così, quale che sia il canale prediletto per l'inserimento della prova algoritmica nel processo penale[11], la decisione sull'ammissione della prova non potrà mai prescindere dalla considerazione delle leggi scientifiche sottese al funzionamento dell'algoritmo, pena il rischio di introdurre nel contesto processuale informazioni irrilevanti (in quanto basate su fondamenta scientifiche non attendibili in linea di principio o non adeguate all'applicazione prevista).

Analogamente, nella fase di assunzione della prova, occorrerà tenere conto delle caratteristiche tipiche della *electronic evidence* come, per esempio, l'immaterialità, la congenita modificabilità e la promiscuità delle informazioni generate o raccolte tramite l'intelligenza artificiale.

Infine, la natura della "prova algoritmica" (eventualmente ammessa) emergerà nuovamente al momento della sua valutazione, quando si tratterà di individuarne l'effettiva persuasività, tenendo conto altresì del margine di errore insito nello strumento considerato.

3. Intelligenza artificiale e prova penale: opportunità e rischi

Allo stadio attuale, due sono i principali punti di intersezione tra la prova penale e l'intelligenza artificiale[12].

Il primo è costituito dalla c.d. "automatedly generated evidence"[13]. Si tratta delle informazioni generate automaticamente, prevalentemente

[11] Cfr., sul punto, S. QUATTROCOLO, *L'ammissione della prova alla luce della rivoluzione digitale*, in E.M. CATALANO, P. FERRUA (a cura di), *Corderiana. Sulle orme di un maestro del rito penale*, Torino, 2023, p. 163 ss.; G. UBERTIS, *Perizia, prova scientifica e intelligenza artificiale nel processo penale*, in S. PATTI, R. POLI, *La consulenza tecnica d'ufficio. Funzione, oggetto, sindacabilità*, Torino, 2024, p. 181 ss. In termini generali, v. anche M. CAIANIELLO, *L'ammissione della prova scientifica nel processo penale italiano*, in G. CANZIO, L. LUPARIA DONATI (a cura di), *Prova scientifica e processo penale*, Milano, 2022, p. 189 ss.

[12] Cfr., al riguardo, K. LIGETI, *AI Evidence: Ensuring a Fair Trial in the Digital World*, in M. BERGSTRÖM, V. MITSILEGAS (eds.), *EU Law in the Digital Age*, Oxford-Dublin, 2025, p. 225 ss.

[13] Per una compiuta elaborazione della categoria della "prova generata automaticamente" v., da ultima, S. QUATTROCOLO, *Prova e intelligenza artificiale*, in C. CONTI, A. MARANDOLA (a cura di), *La prova scientifica*, Milano, 2023, p. 467 ss.

per motivi commerciali, da prodotti di consumo che utilizzano o applicano strumenti di intelligenza artificiale. Si pensi, a titolo puramente esemplificativo, alle informazioni incamerate dai sistemi di guida assistita presenti all'interno degli autoveicoli tecnologicamente avanzati, ai dati registrati dai dispositivi integrati in una rete domotica (nella quale possono rientrare anche sistemi di sorveglianza) oppure, ancora, alle informazioni registrate da alcune applicazioni per il monitoraggio dei parametri corporei presenti nei dispositivi elettronici mobili. Questi dati, ovviamente, costituiscono un vasto patrimonio informativo, potenzialmente rilevante anche nell'ambito di un procedimento penale.

Il secondo profilo da tenere in considerazione è costituito dai sistemi di analisi forense che integrano *software* di intelligenza artificiale per lo svolgimento dei relativi esami. Si pensi, in particolare, ai sistemi di riconoscimento facciale – e di analisi biometrica in generale[14] –, oppure ai *software* di analisi documentale, che consentono di filtrare ed esaminare una vastissima congerie di *file* digitali.

Entrambe le applicazioni considerate rappresentano una preziosa opportunità per il sistema di giustizia penale, ma sollevano anche numerosi interrogativi a causa dei rischi che si intravedono nella loro implementazione pratica.

Per quanto riguarda le informazioni generate automaticamente, occorre tenere sempre presente che i *software* da cui risultano prodotte sono stati progettati e realizzati per finalità differenti rispetto a quelle propriamente processuali. Ciò genera il rischio di un utilizzo improprio dei dati in esame e la produzione di gravi fraintendimenti cagionati dal c.d. *function creep*, che si verifica quando una certa tecnologia viene utilizzata al di fuori del dominio e degli scopi per cui è stata originariamente creata[15]. Si rende dunque necessaria una verifica accurata circa l'autenticità e l'attendibilità dell'informazione estratta dai singoli dispositivi per non incappare in errori che si rivelano fatali nella ricostruzione dei fatti in sede giudiziale[16].

---

[14] Su cui v. E. SACCHETTO, *La prova biometrica*, in C. CONTI, A. MARANDOLA (a cura di), *La prova scientifica*, cit., p. 243 ss.

[15] K. LIGETI, *AI Evidence: Ensuring a Fair Trial in the Digital World*, cit., p. 233.

[16] S. QUATTROCOLO, *Prova e intelligenza artificiale*, cit., p. 493.

Le difficoltà, com'è agevole intuire, sono legate alla necessità di verificare compiutamente il funzionamento del sistema di intelligenza artificiale che ha generato quell'informazione: ciò richiederebbe, infatti, di avere pieno accesso all'algoritmo proprietario, così come ai dati di addestramento del *software*.

Una tale situazione di completezza informativa sembra di difficile realizzazione, data l'esigenza di tutelare la riservatezza delle creazioni coperte da privativa industriale, senza che si possa rimproverare alle imprese produttrici la mancata cooperazione con l'autorità giudiziaria (dal momento che si troverebbero involontariamente coinvolte nella vicenda processuale). Di conseguenza, ove il legislatore non si premuri di introdurre un meccanismo specifico di *disclosure* controllata per affrontare le situazioni di questo genere, l'interprete si troverebbe di fronte a una rigida alternativa: l'esclusione in radice delle informazioni in questione dal contesto processuale (non essendo possibile verificarne autenticità, attendibilità e precisione) o la loro fideistica ammissione.

Ovviamente, nessuna delle due soluzioni appare pienamente soddisfacente. Una via mediana sembra, tuttavia, percorribile adottando un approccio pragmatico. In effetti, potrebbe apparire eccessivo escludere dalla scena processuale determinate informazioni solo perché derivano da certe tecnologie, magari già ampiamente sperimentate e utilizzate nella vita quotidiana.

Per intenderci, una volta acquisito lo scontrino emesso dalla cassa automatica collocata all'interno di un supermercato, sembra difficile ipotizzare che il giudice disponga una minuziosa perizia per sviscerare tutti i meccanismi elettronici e informatici che ne regolano il funzionamento, a meno che non vi siano serie contestazioni in merito alle modalità di fatturazione o alla determinazione dell'orario di emissione della ricevuta (magari con la produzione delle tanto temute "allucinazioni").

Analogamente, non è detto che l'ammissione in giudizio di determinati elementi di prova debba essere subordinato alla disponibilità di informazioni specifiche e dettagliate sui sistemi di *artificial intelligence* che li hanno prodotti, ferma restando la necessità di mettere a disposizione di tutte le parti il *data-set* estratto dal dispositivo in questione.

Qualora, poi, l'attendibilità di questi dati fosse posta in discussione, il giudice avrebbe il dovere di valutare la necessità di disporre una peri-

zia o un esperimento giudiziario per verificare l'effettivo funzionamento del sistema, eventualmente attraverso un approccio di *reverse engineering*. Per converso, senza pieno accesso al *data-set* estratto dal dispositivo diviene impossibile garantire la parità delle armi e il diritto al "confronto" con la prova algoritmica, come ha posto in luce la dottrina più sensibile al tema[17]. Difatti, non sarebbe possibile verificare se le informazioni raccolte siano idonee, per quantità e qualità, a soddisfare le esigenze di accertamento dei fatti, né sarebbe possibile operare su di esse per ricostruire *ex post* la logica del sistema che le ha generate.

Problematiche solo in parte analoghe si riscontrano in relazione ai *Forensic Tools* che si avvalgono dell'intelligenza artificiale per lo svolgimento di esami ed analisi. Questi ultimi, infatti, sono progettati per le finalità tipiche del procedimento penale e dovrebbero garantire elevati standard di qualità. Inoltre, i *software* in questione sono spesso sviluppati direttamente dalle agenzie di *law enforcement* o, comunque, su impulso di un committente pubblico, motivo per cui le imprese produttrici non potrebbero dolersi di essere rimaste casualmente coinvolte nei procedimenti penali in cui quegli strumenti hanno trovato impiego[18].

Con l'introduzione del c.d. *Artificial Intelligence Act*[19], gli strumenti in questione hanno conosciuto una prima forma di regolazione. Difatti, tutti i sistemi volti alla valutazione di affidabilità di elementi probatori (nella fase delle indagini) e quelli volti alla ricerca e alla interpretazione

[17] E. BAMPASIKA, *AI-Based Means of Evidence and the Defendant's Right in the European Union*, in M. BERGSTRÖM, V. MITSILEGAS (eds.), *EU Law in the Digital Age*, cit., p. 247 ss.

[18] Cfr., *mutatis mutandis*, Cons. St., sent. sentenza 4 febbraio 2020 n. 881, § 10, ove si è affermato perentoriamente che «la caratterizzazione multidisciplinare dell'algoritmo (costruzione che certo non richiede solo competenze giuridiche, ma tecniche, informatiche, statistiche, amministrative) non esime dalla necessità che la 'formula tecnica', che di fatto rappresenta l'algoritmo, sia corredata da spiegazioni che la traducano nella "regola giuridica" a essa sottesa e che la rendano leggibile e comprensibile»; precisando, inoltre, che «non può assumere rilievo [in senso contrario] l'invocata riservatezza delle imprese produttrici dei meccanismi informatici utilizzati i quali, ponendo al servizio del potere autoritativo tali strumenti, all'evidenza ne accettano le relative conseguenze in termini di necessaria trasparenza».

[19] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale.

dei fatti rilevanti (in sede di giudizio) sono considerati come applicazioni ad alto rischio, ai sensi dell'allegato III del medesimo regolamento europeo, cui rinvia l'art. 6 § 2 Reg. (UE) 1689/2024. Ciò implica che essi debbano sottostare a tutte le cautele e agli obblighi di trasparenza, qualità e vigilanza disciplinati dal regolamento in esame di cui, tuttavia, sono ben noti inconvenienti ed eccezioni. In particolare, per quanto riguarda i *software* di analisi forense, è legittimo domandarsi se sia possibile "evadere" dalla stringente disciplina dettata per i sistemi ad alto rischio, facendo leva sulle clausole di salvaguardia contenute nell'art. 6 § 3 Reg. (UE) 1689/2024[20]. È chiaro, infatti, che, se queste disposizioni fossero interpretate in senso lato, gran parte dei dispositivi di analisi forense potrebbe essere escluso dal novero dei sistemi ad alto rischio, con un significativo abbassamento degli standard di trasparenza e di qualità previsti per questi ultimi[21].

Sarebbe un esito davvero beffardo e poco auspicabile. In tal caso, difatti, per rispettare l'equità processuale e la parità delle armi, non resterebbe che affidarsi alle scarne – benché meritevoli di apprezzamento – indicazioni giurisprudenziali emerse fino a questo momento.

Muovendo dalle statuizioni più recenti, nelle pronunce sui c.d. criptofonini, la Corte di Cassazione ha espressamente riconosciuto che, in linea di principio, «la disponibilità dell'algoritmo di criptazione è funzionale al controllo dell'affidabilità del contenuto delle comunicazioni acquisite al procedimento»[22].

---

[20] Laddove si esclude che i sistemi di cui all'allegato III debbano essere considerati ad alto rischio quando siano destinati: a) a eseguire un *compito procedurale limitato*; b) a migliorare il risultato di un'attività umana precedentemente completata; c) a rilevare schemi decisionali o deviazioni da schemi decisionali precedenti e non siano finalizzati a sostituire o influenzare la valutazione umana precedentemente completata senza un'adeguata revisione umana; d) a eseguire un *compito preparatorio* per una valutazione pertinente ai fini dei casi d'uso elencati nell'allegato III.

[21] Cfr., sulle eccezioni in esame, T. RODRÌGUEZ DE LAS HERAS BALLEL, *High-Risk AI Systems in the European AI Act*, in O. POLLICINO et al. (a cura di), *La disciplina dell'intelligenza artificiale*, Milano, 2025, p. 241 ss.

[22] Cass., sez. un., sent. 29 febbraio 2024 n. 23755, Gjuzi Ermal, § 12.4, in *CED Cass.*, n. 286573 – 06 (ove, peraltro, la conseguenza logica di tale statuizione di massima è stata "sterilizzata", considerando che «il pericolo di alterazione dei dati non sussiste, salvo specifiche allegazioni di segno contrario, in quanto il contenuto di ciascun

La Corte di Strasburgo, dal canto suo, ha stabilito da tempo che – ove le autorità inquirenti abbiano effettuato il sequestro di una vasta mole di prove digitali, filtrate in seguito attraverso strumenti informatici di analisi documentale – tali *software* dovrebbero essere posti anche a disposizione della difesa, nella misura in cui si rivelino utili a garantire le facilitazioni necessarie per l'esercizio del diritto di difesa, ai sensi dell'art. 6 § 3 lett. *b* Cedu[23].

4. Le decisioni fondate su trattamenti automatizzati

Venendo, infine, al versante propriamente decisionale, giova soffermarsi rapidamente sul già menzionato art. 8 del d.lgs. n. 51/2018. Senza voler indugiare troppo su una disposizione che ha suscitato notevole attenzione in dottrina per il suo significato (anche simbolico) di garanzia, giova segnalare alcune questioni esegetiche problematiche, utili per individuare la portata delle garanzie legislative.

Anzitutto, sebbene talvolta venga intesa come un divieto assoluto di impiegare decisioni automatizzate nel contesto processuale, dal tenore letterale della disposizione si comprende agevolmente come, in realtà, l'interdizione sia soltanto relativa, essendo ancorata al rispetto della riserva di legge (europea o nazionale)[24].

Nei casi in cui la riserva di legge venga attuata e, di conseguenza, l'impiego di decisioni automatizzate sia stato debitamente autorizzato, il legislatore è chiamato a garantire i diritti e le libertà dei soggetti interessati tramite apposite garanzie procedurali. Fra queste ultime spicca, in particolare, il diritto a ottenere un controllo umano da parte del titola-

---

messaggio è inscindibilmente abbinato alla sua chiave di cifratura, per cui una chiave errata non ha alcuna possibilità di decriptarlo, anche solo parzialmente»).

[23] Corte eur. dir. uomo, sent. 4 giugno 2019, Sigurdur Einarsson e altri c. Islanda, § 90-91. Per gli opportuni approfondimenti al riguardo, cfr. L. BARTOLI, *Parità delle armi e* e-discovery *nel processo penale: quali indicazioni da Strasburgo?*, in R. BRIGHI (a cura di), *Nuove questioni di informatica forense*, Roma, 2022, p. 83 ss.

[24] In tal senso, v. L. LUPARIA, *Diritto probatorio e giudizi criminali ai tempi dell'intelligenza artificiale*, in R. GIORDANO, A. PANZAROLA, A. POLICE, S. PREZIOSI, M. PROTO (a cura di), *Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, Milano, 2022, p. 782.

re del trattamento, che deve essere assicurato in ogni caso dalla pertinente normativa[25].

In secondo luogo, sempre facendo riferimento al dato testuale, si evince con sufficiente chiarezza che il divieto in esame – nei termini in cui è stato ricostruito in precedenza – non riguarda soltanto l'adozione di decisioni giurisdizionali tramite programmi automatizzati (il c.d. giudice-robot), ma anche l'emissione di decisioni che siano basate in modo esclusivo o determinate sugli elementi generati da un trattamento automatizzato di dati. Se così non fosse, non si comprenderebbe lo specifico riferimento alla profilazione, che costituisce senza dubbio un trattamento automatizzato di dati, posto a supporto di un processo decisionale più ampio. Nel disegno normativo, dunque, l'emissione del provvedimento costituisce un'entità concettualmente distinta – e logicamente successiva – rispetto al trattamento di dati personali, su cui la decisione risulta fondata[26].

Infine, giova precisare che il divieto sancito dalla norma in esame colpisce soltanto i trattamenti automatizzati che producono *effetti pregiudizievoli* nei confronti degli interessati. Rimane, dunque, insoluto il quesito ermeneutico su quali sarebbero le conseguenze giuridiche nell'ipotesi in cui un trattamento automatizzato producesse, al contrario, effetti potenzialmente favorevoli per i soggetti interessati. È evidente

[25] Per una critica a tale impostazione legislativa, v. S. SIGNORATO, *Il diritto a decisioni penali non basate esclusivamente su trattamenti automatizzati: un nuovo diritto derivante dal rispetto della dignità umana*, in *Riv. dir. process.*, 2021, pp. 107 ss., ove si sostiene che la decisione algoritmica sia radicalmente incompatibile con il diritto al rispetto della dignità umana e che «tale violazione non potrebbe ritenersi sanata dal successivo (oltretutto eventuale) intervento umano» (*ivi*, p. 108). Di conseguenza, l'autrice dubita «della legittimità dell'art. 11 dir. 2016/680/UE e dell'art. 8 d.lgs. 18 maggio 2018 n. 51 nella parte in cui essi prevedono che la decisione robotica possa essere autorizzata dal diritto dell'Unione o degli Stati membri» (*ivi*, p. 109).

[26] Muovendo da queste considerazioni, si giunge ad affermare che la disposizione in commento non si limita a vietare l'emissione (*rectius*: la deliberazione) di provvedimenti giurisdizionali tramite strumenti di IA, ma prescrive anche una regola negativa di valutazione della prova, analoga a quella prevista dall'art. 192, co. 2 c.p.p. In questa direzione, v. M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Diritto penale contemporaneo - Archivio web*, 29 maggio 2019, p. 17 (ultimo accesso il 28 febbraio 2025).

che, qualora si ritenesse necessario verificare la concreta incidenza delle informazioni generate o elaborate mediante un trattamento automatizzato, l'interdizione prevista dall'art. 8 d.lgs. n. 51/2018 dovrebbe essere concepita alla stregua di un vero e proprio criterio di valutazione della prova[27].

5. Intelligenza artificiale e "ciclo probatorio"

Un'ultima considerazione in merito al contesto in cui è destinato a svilupparsi il dibattito sugli elementi di prova generati o raccolti tramite strumenti di intelligenza artificiale.

In dottrina è stato evidenziato come, a dispetto delle regole che disciplinano l'ammissione della prova in giudizio in ciascun ordinamento, ogni "nuovo" strumento di prova, frutto dell'evoluzione della scienza o della tecnica, attraversa un "ciclo probatorio"[28] nel quale sono riconoscibili – approssimativamente – i seguenti stadi (senza che tra essi siano sempre individuabili rigide separazioni o che il passaggio da uno stadio all'altro sia irreversibile):

a) Too new to be reliable
b) New but subject to testing
c) Generally reliable but occasionally improperly applied
d) Blindly Trusted.

Ciò costituisce ulteriore riprova del legame profondo che intercorre tra il sistema probatorio processuale e l'orizzonte epistemologico di riferimento in una determinata epoca storica. Se, come appare probabi-

[27] Sembra riproporsi, sotto nuove sembianze, l'antica diatriba dottrinale sull'efficacia delle prove illegittimamente acquisite, le quali sarebbero inutilizzabili *contra reum*, mentre – secondo parte della dottrina – potrebbero essere oggetto di valutazione in favore dell'imputato (cfr., al riguardo, F. CORDERO, *Prove illecite* (1961), in ID., *Tre studi sulle prove penali*, Milano, 1963, p. 171, il cui pensiero è stato ripreso, recentemente, da F. CAPRIOLI, *Verità e giustificazione nel processo penale*, in G. FORTI, G. VARRASO, M. CAPUTO (a cura di), *«Verità» del precetto e della sanzione alla prova del processo*, Napoli, 2014, pp. 204-205, ricordando che «l'accertamento dell'innocenza è una posta troppo importante, per essere sacrificata agli idoli della procedura»).

[28] V. S. GLESS, *AI in the Courtroom: a Comparative Analysis of Machine Evidence in Criminal Trials*, in 51 *Georgetown Journal of International Law* (2020), no. 2, p. 195 ss.

le, anche gli elementi di prova generati o raccolti tramite l'intelligenza artificiale sono destinati ad affrontare queste evoluzioni ed involuzioni, è opportuno cominciare ad attrezzarsi culturalmente e giuridicamente, affinché l'interprete – sia esso pubblico ministero, avvocato o giudice – sia davvero artefice consapevole delle proprie decisioni e non rimanga esposto alle intemperie, in balia dalla corrente.