dirittifondamentali.it

Dirittifondamentali.it - Fascicolo 2/2026
Data di pubblicazione – 1° giugno 2026

Il processo penale come spazio di controllo del potere tecnologico

di
Sarah Grieco*

SOMMARIO: 1. Potere tecnologico, processo penale e stato costituzionale - 2. La sicurezza algoritmica come categoria giuridica - 3. *Legal AI*, interpretazione giuridica e giusto processo - 4. Il modello regolatorio dell'*AI Act*: approccio *risk-based* e principio antropocentrico - 5. Indagini preliminari, "finestre di giurisdizione" e controllo sull'uso investigativo dell'IA - 6. Prova algoritmica, art. 189 c.p.p. e contraddittorio "per" la prova - 7. Interpretazione giuridica e funzione decisoria - 8. La legge n. 132 del 2025: un primo passo, ancora incompleto – 9. La sfida della giurisdizione digitale: un nuovo modello di conoscenza.

1. Potere tecnologico, processo penale e stato costituzionale

Nel costituzionalismo contemporaneo, il potere non si legittima per la sua efficienza, ma per la sua sottoposizione al diritto, per la sua controllabilità e per la possibilità di essere giustificato, secondo procedure trasparenti e contestabili.

In questa prospettiva, la giurisdizione rappresenta il luogo in cui il potere è chiamato a rendere conto di sé, attraverso forme di verifica che ne assicurano la razionalità, la conoscibilità e la sindacabilità. Il processo, dunque, non rappresenta solo un meccanismo di accertamento, ma uno spazio di tutela, nel quale uno dei poteri più incisivi dello Stato sull'individuo, quello in grado di restringere le sue libertà personali, viene ricondotto entro i limiti della legalità[1].

La progressiva integrazione di sistemi algoritmici nell'esercizio delle funzioni pubbliche, in particolare nell'esercizio della giustizia, impone di interrogarsi, in via

*Avvocata, Assegnista di ricerca Scuola Superiore Meridionale, Napoli.

[1] In questa prospettiva teorica, il diritto opera come limite al potere e il processo come spazio di garanzia. Sul punto, in termini generali, v. L. FERRAJOLI, *Diritto e ragione. Teoria del garantismo penale*, Roma-Bari, 1989.

Contributo sottoposto a referaggio

preliminare, sulla tenuta dei principi fondamentali gli artt. 24, 101, 102 e 111 Cost. caposaldi imprescindibili dello Stato costituzionale di diritto, anche negli ecosistemi digitali[2].

La scelta compiuta dal legislatore europeo di classificare come "ad alto rischio" i sistemi di IA destinati a essere utilizzati nell'amministrazione della giustizia non ha un significato meramente tecnico, ma esprime una precisa opzione di valore. Come si avrà modo di approfondire nel proseguo, il *Considerando 61* dell'*AI Act* chiarisce che tale scelta è finalizzata «a far fronte ai rischi di potenziali distorsioni, errori e opacità», in ragione del loro impatto significativo sulla democrazia, sullo Stato di diritto, sulle libertà individuali e sul diritto a un ricorso effettivo e a un giudice imparziale.

Non siamo in presenza, dunque, di una classificazione neutrale: essa presuppone la consapevolezza che l'uso dell'algoritmo, in ambito giudiziario, non riguarda soltanto l'efficienza dell'amministrazione, ma investe direttamente la struttura delle garanzie costituzionali.

Non si tratta di disciplinare nuove tecnologie, ma di verificare se e in quale misura esse incidano sull'assetto delle garanzie che presidiano l'esercizio del potere e, in particolare, di quello punitivo.

L'ingresso dell'intelligenza artificiale nei processi decisionali pubblici introduce, infatti, una discontinuità rilevante: tende a spostare il baricentro della decisione da un modello fondato sull'argomentazione giuridica ad uno sempre più orientato all'elaborazione dei dati e alla previsione statistica, con il rischio di una progressiva attenuazione della dimensione giustificativa del potere. Come è stato efficacemente osservato, il pericolo non risiede tanto nella sostituzione dell'uomo con la macchina, quanto nella trasformazione del modo stesso di concepire la decisione pubblica, nella quale «l'operare finisce per prevalere sul pensare»[3].

---

[2] Cfr. P.P. PAULESU, *Intelligenza artificiale e processo penale. Una lettura attraverso i principi*, in P.P. PAULESU, M. DANIELE, S. SIGNORATO, M. BOLOGNARI, A. BOLDRIN (a cura di), *Studi in onore di Roberto E. Kostoris*, Giappichelli, 2022, 24 s.

[3] A. BALSAMO, *L'impatto dell'intelligenza artificiale nel settore della giustizia*, in *Sistema penale*, 22 maggio 2024.

È in questa prospettiva che la questione dell'intelligenza artificiale nel processo penale si colloca al crocevia tra tecnologia e costituzionalismo: interroga la capacità dell'ordinamento di preservare la centralità della persona, la pienezza del contraddittorio e la funzione garantista della giurisdizione di fronte a nuove forme di esercizio del potere.

2. La sicurezza algoritmica come categoria giuridica

Nella prospettiva sopra delineata, la *sicurezza algoritmica* diventa il nucleo centrale di tenuta stessa del sistema democratico.

Il concetto - che, attualmente, non trova una compiuta codificazione legislativa - non può essere ridotta al solo profilo della sicurezza informatica o dell'affidabilità tecnica dei sistemi. La sicurezza algoritmica va, piuttosto, intesa come categoria giuridica interpretativa, che emerge dall'intreccio tra il modello regolatorio delineato dall'*AI Act*[4], le garanzie costituzionali del "giusto processo" e la riflessione sulla trasformazione dell'interpretazione giuridica nell'epoca dell'intelligenza artificiale.

Se volessimo addentrarci in una definizione più compiuta, potremmo individuarla come l'insieme delle condizioni normative, procedurali e istituzionali necessarie affinché l'impiego di sistemi di intelligenza artificiale nel processo penale non comprometta i diritti fondamentali della persona, l'autonomia del giudizio, l'indipendenza della magistratura e, in ultima analisi, la tenuta democratica dell'ordinamento.

La sicurezza algoritmica si articola su tre dimensioni.

Una prima è di natura prettamente tecnica, che comprende la *cybersicurezza* del sistema, la sua accuratezza e robustezza, la trasparenza del funzionamento, la sorveglianza umana[5]. In tale ambito, a rilevare non è soltanto il suo ruolo di presidio contro intrusioni o alterazioni esterne, ma come "condizione di affidabilità" dell'uso processuale del sistema stesso. Un difetto di programmazione

[4] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024.

[5] Ivi, artt. 13, 14 e 15, nonché *Considerando 59* e *61.*

o di scarsità o non buona qualità del *dataset* utilizzato, conduce a false correlazioni o a *bias* cognitivi. Un algoritmo vulnerabile, manipolabile o strutturalmente opaco non pone soltanto un problema tecnico: mette in discussione la possibilità stessa che il suo *output* possa essere impiegato in un procedimento penale compatibile con le esigenze di verificabilità e contestabilità, proprie del giusto processo.

La seconda accezione è di tipo procedurale e riguarda le condizioni di ingresso e di utilizzo dell'algoritmo nel processo: occorre preservare la capacità di comprendere e contestare il funzionamento degli strumenti impiegati[6]. In questo senso, l'utilizzo di sistemi complessi e opachi rischia di accentuare le asimmetrie tra le parti, attribuendo un vantaggio strutturale a chi detiene il controllo del sistema o dispone delle competenze tecniche necessarie per interpretarne il funzionamento[7]. Il diritto di difesa non può dirsi pienamente effettivo laddove la parte non sia in grado di comprendere e contestare l'elemento probatorio algoritmico. È, pertanto, necessario assicurare il diritto alla spiegazione dei processi decisionali, la valutazione d'impatto sui diritti fondamentali, la conoscibilità del funzionamento del sistema (il cd. "problema della *black box*"[8]) e, soprattutto, il diritto della difesa a contestare

[6] M. RAGNEDDA, *The Third Digital Divide. A Weberian Approach to Digital Inequalities*, Routledge, London, 2017; Id., *Digital Capital*, Emerald Publishing, 2018. L'a. introduce il concetto di *digital capital*, inteso come capacità di trasformare uso digitale in vantaggio sociale, attraverso lo sviluppo della capacità di controllo effettivo della macchina.

[7] È sempre più diffuso il concetto di *digital divide,* fenomeno multilivello, non riducibile alla mera disponibilità di accesso alle tecnologie, ma esteso alle competenze, alle modalità d'uso e agli esiti dell'interazione digitale e alla conseguente capacità effettiva di accedere, comprendere e contestare i processi decisionali algoritmici. Cfr. J. VAN DIJK, *The Deepening Divide. Inequality in the Information Society*, Sage, London, 2005; HARGITTAI, *Second-Level Digital Divide: Differences in People's Online Skills*, in *First Monday*, 2002. In dottrina, è stata individuata come causa di disuguaglianza strutturale della società in rete, che incide sulla capacità dei soggetti di partecipare in modo effettivo ai processi decisionali. V., tra gli altri, J. VAN DIJK, *The Digital Divide*, Polity Press, Cambridge, 2020; P. DIMAGGIO, E. HARGITTAI, W. R. NEUMAN, J. P. ROBINSON, *Social Implications of the Internet*, in *Annual Review of Sociology*, 2001, p. 307 ss.; M. WARSCHAUER, *Technology and Social Inclusion. Rethinking the Digital Divide*, MIT Press, Cambridge (MA), 2003; M. CASTELLS, *The Rise of the Network Society*, Blackwell, Oxford, 1996 (ed. aggiornata 2010).

[8] F. PASQUALE, *The Black Box Society. The Secret Algorithms that Control Money and Information*, *Harvard University Press*, 2015; A.G. FERGUSON, *Illuminating Black Data Policing*, in *Ohio St. Journal of Crim. Law*, 2018, 503; G. CONTISSA, G. LASAGNI, G. SARTOR, Q*uando a decidere in materia penale sono (anche)gli algoritmi e la IA: alla ricerca di un rimedio effettivo*, in *Diritto di internet*, 2019, 619 ss. Gli autori sottolineano la natura di *black box* dei sistemi, inaccessibili al loro stesso programmatore.

effettivamente la prova algoritmica[9]. La sicurezza algoritmica si traduce nella necessità di impedire che l'algoritmo diventi una fonte occulta di decisione, o meglio, porre al riparo il processo dal rischio una "motivazione oracolare"[10], sottratta al contraddittorio (o soggetta ad un contraddittorio meramente "di facciata") o schermata da una opacità incompatibile con l'equità processuale.

La terza è una dimensione istituzionale che investe la distribuzione dei poteri e la *governance* del fenomeno tecnologico. Da un lato, la decisione finale deve restare "umana" (cd. riserva di umanità) in quanto la responsabilità rappresenta il presupposto della legittimazione democratica del potere pubblico. Dall'altro, si richiede il controllo giurisdizionale sull'impiego di sistemi vietati o ad alto rischio nelle indagini, nonché un assetto di governo della digitalizzazione che non comprometta l'indipendenza della magistratura

Intesa in questi termini, la sicurezza algoritmica consente di cogliere un dato essenziale: il problema dell'intelligenza artificiale nel processo penale non coincide con la sola questione dell'innovazione tecnologica, ma investe il modo in cui l'ordinamento costruisce le condizioni di legittimazione del potere. Atteso che l'algoritmo non argomenta e non giustifica, limitandosi a correlare dati e produrre *output* probabilistici, il rischio è quello di assistere ad una progressiva marginalizzazione della dimensione giustificativa della decisione, con un sostanziale spostamento del "baricentro" decisionale: da argomentazione giuridiche a disposizioni predittive, frutto di elaborazione di dati e previsioni statiche.

3. *Legal AI*, interpretazione giuridica e giusto processo

Nel settore della giustizia, la *Legal AI* può essere definita come l'insieme dei sistemi capaci di acquisire, ordinare e rielaborare enormi quantità di dati giudiziari e

[9] Ivi, artt. 27 e 86, nonché Considerando 170-171

[10] Termine utilizzato da A. GARAPON, J. LASSEGUE, *La giustizia digitale. Determinismo tecnologico e libertà*, ed.it. a cura di M. ROSARIA FERRARESE, Il Mulino, 2021, 172. Per gli autori l'impiego del termine "predittivo" avrebbe la funzione di attestare "un carattere magico, quasi divinatorio", che sarebbe recepita "come un oracolo".

giurisprudenziali, al fine di formulare previsioni, raccomandazioni o, nei modelli più avanzati, vere e proprie proposte decisionali.

Il suo impiego può assumere forme assai diverse: dal supporto alla ricerca dei precedenti all'analisi documentale, dall'organizzazione dei flussi di lavoro fino all'elaborazione di valutazioni "predittive"[11] su rischio, recidiva, attendibilità o probabilità di esito[12].

A questi strumenti si aggiunge, poi, la variegata galassia delle tecnologie "generative"[13] (rappresentate soprattutto da *ChatGPT*), così come di tecniche "miste", in grado di combinare entrambi gli strumenti. Strumenti generativi, o meglio, misti potrebbero essere utilizzati dai giudici per la redazione di dispositivi o motivazioni della sentenza, inserendo i dati della causa, le prove e le norme da applicare (cfr. *Par.7*)[14].

Così come sono pure ipotizzabili impieghi dell'IA volti a potenziare le risorse e le capacità conoscitive del difensore, tali da ridurre l'asimmetria che tradizionalmente caratterizza il rapporto tra accusa e difesa. Un ventaglio amplio, destinato ad allargarsi nel prossimo futuro, con il progredire della tecnologia.

Se il processo penale è il luogo in cui lo Stato esercita la sua potestà punitiva nei confronti del cittadino, l'opacità algoritmica che caratterizza i sistemi di IA ad alto rischio, genera asimmetrie informative e *deficit* di controllo democratico che minacciano il nucleo essenziale del giusto processo. Lo statuto epistemico del processo penale, infatti, è disciplinato da una rete di principi costituzionali e regole procedurali per i quali il rispetto della legalità del procedere e il metodo dialogico nell'acquisizione e valutazione delle prove prevalgono sull'obiettivo del mero risultato.

Il processo è "giusto" non quando il suo esito è semplicemente esatto in senso tecnico o statistico, ma quando rispetta il nucleo delle garanzie costituzionali: la

[11] Sull'uso delle tecnologie predittive nel processo e, in particolare, nell'attività decisoria del giudice v. R. E. KOSTORIS, *Intelligenza artificiale, strumenti predittivi e processo penale*, in *DisCrimen*, 5 marzo 2024.

[12] Intesa come capacità di formulare previsioni statistiche sul futuro basate su dati del passato.

[13] Per "generativi" si intendono quelle tecnologie che, oltre ad analizzare i dati esistenti, sono capaci di produrne (generare, appunto) di nuovi, ivi inclusi i testi.

[14] R. E. KOSTORIS, *Intelligenza artificiale, strumenti predittivi e processo penale,* cit.,12.

dirittifondamentali.it

presunzione di innocenza, l'onere della prova a carico dell'accusa, il contraddittorio come metodo di verifica delle prove, la motivazione coerente e argomentata, il criterio dell'oltre ogni ragionevole dubbio, il controllo impugnatorio sulla legalità e sulla logicità della decisione.

Il modello "forte" di *decision-making* algoritmico, inteso come automazione completa del sistema decisionale[15], è estremamente attrattivo. Calcolabilità, uniformità e celerità rappresentano una sorta di *exit* rispetto alle numerose criticità da cui è attanagliato il nostro sistema giustizia: dalla costante crescita delle domanda di giustizia, e della conseguente mole di lavoro, al succedersi di riforme incoerenti e disorganiche per rispondere all'esigenza della politica; dall'*escalation* di strumenti di investigazione alla lentezza dei processi e dei loro riflessi su libertà e *privacy* delle persone; fino al dramma dell'esecuzione della pena nei sovraffollati istituti penitenziari che la contengono.

La promessa di una giustizia neutrale, efficiente e veloce porta, tuttavia, con sé un prezzo alquanto elevato: la rinunzia alla "riserva di umanità". È un modello dove si assiste ad una "frattura antropologica"[16], col venir meno del paradigma indiziario proprio della tradizione razionalista occidentale, favorendo conformismo, deresponsabilizzazione del decisore e sclerotizzazione del formante giurisprudenziale, oltre a ricadute importanti in termini di autonomia e indipendenza del giudice[17].

L'impossibilità di un controllo effettivo dei *big data*, della loro affidabilità e di contestazione efficace del funzionamento di sistemi informatici e algoritmi di estrema complessità, assegnano all'algoritmo un ruolo di fatto "normativo", rendendo concreto il pericolo che la soggezione del giudice soltanto alla legge e la

[15] G. CANZIO, *AI Act e processo penale: sfide e opportunità*, in *Sistema Penale*, 2024, 1.

[16] Per ampie considerazioni al riguardo cfr. A. GARAPON e J. LASSEGUE, *La giustizia digitale. Determinismo tecnologico e libertà*, cit., 79 e ss. Gli autori - assumendo come punto di partenza la necessità di integrare più sguardi, e in particolare quello del giurista e quello dell'epistemologo per comprendere le rivoluzioni introdotte dalle tecnologie - segnalano il rischio che la crescente fiducia nelle decisioni tecniche favorisca una progressiva sostituzione della mediazione giuridica con quella algoritmica, determinando una desimbolizzazione del diritto e del giudice.

[17] G. CANZIO, *Indagini e giudizio fra regolamento (UE) 2024/1689 (AI Act) e legge n. 132 del 2025*, in *Giustizia Insieme*, 13 gennaio 2026, 12.

distinzione tra funzione giurisprudenziale e legislativa possano ridursi ad un'astrazione.

Inoltre, l'utilizzo di strumenti predittivi come "orientamento giurisprudenziale consolidato", rischia una tendenza alla "burocratizzazione" dei giudici, con una sorta di loro sostanziale deresponsabilizzazione e annesso rischio di profilazione degli stessi (oltre che dei precedenti), che renderebbe sempre più arduo mutare i propri orientamenti, davanti ad una conoscenza e ad un'aspettativa di conformità da parte dei consociati.

Ciò non significa, tuttavia, che il dibattito debba essere condotto in termini ideologici o pregiudiziali. Un approccio maturo e laico richiede di evitare sia il timore astratto di una superintelligenza incontrollabile, sia la sopravvalutazione delle capacità umane.

Sotto questo profilo, una corretta impostazione del problema impone di superare la tradizionale contrapposizione tra decisione umana e decisione algoritmica. I limiti comunemente imputati all'IA — *bias*, opacità, difficoltà di esplicitazione del processo decisionale — non sono infatti del tutto estranei al giudizio umano, anch'esso esposto a distorsioni cognitive, selezioni implicite delle informazioni rilevanti e difficoltà di formalizzazione del percorso argomentativo[18].

4. Il modello regolatorio dell'*AI Act*: approccio *risk-based* e principio antropocentrico

La consapevolezza dei rischi connessi ai fenomeni di *bias automation* ha determinato, a livello europeo, l'adozione di un modello regolatorio volto ad assicurare che l'implementazione computazionale delle fonti informative nell'amministrazione della giustizia si coniughi con istanze di sorveglianza e responsabilità umane, secondo una logica collaborativa o ibrida (cd. *Hibrid AI)*, che consente all'uomo di mantenere il controllo della macchina in un'ottica di integrazione ed ausilio.

[18] O. DI GIOVINE, *Interpretazione umana e robotica (breve riflessione sul possibile ingresso dei Large Language Models nella giurisdizione)*, 2025.

In questo scenario si colloca il Regolamento Europeo sull'Intelligenza Artificiale n. 1689/2024[19] – meglio conosciuto come *AI Act*, primo tentativo organico di disciplinare l'intelligenza artificiale secondo un approccio fondato sul rischio.

Fin dall'art.1, il Regolamento chiarisce l'intenzione di promuovere la diffusione di un'IA «antropocentrica e affidabile», garantendo al contempo, mediante «regole armonizzate», un livello elevato di protezione della salute, della sicurezza, dei diritti fondamentali, della democrazia e dello Stato di diritto[20].

L'*AI Act* adotta un approccio *risk-based* («secondo la probabilità del verificarsi di un danno e la gravità del danno stesso»), fondato su una scala graduale di livelli, obblighi e limiti di applicazione: dal divieto di utilizzo, all'utilizzo condizionato per i sistemi ad alto rischio, sino ai livelli di rischio moderato o minimo. Per i sistemi ad alto rischio, come quello giustizia, il Regolamento richiede, in ogni caso, trasparenza del funzionamento (art.13), supervisione e sorveglianza umana (art. 14), accuratezza, robustezza, cybersicurezza, valutazione d'impatto sui diritti fondamentali (art. 27) e diritto alla spiegazione dei processi decisionali (art. 86)[21].

Per il settore penale, alcune disposizioni assumono rilievo centrale.

Il *Considerando 42* precisa che, in linea con la presunzione d'innocenza, la persona deve essere giudicata sulla base del suo comportamento effettivo e non di una mera previsione algoritmica fondata su profilazione, tratti di personalità o caratteristiche personali.

L'art. 5 vieta, tra l'altro, pratiche di *social scoring* (punteggio sociale in base a valutazioni o classificazione delle persone sulla base di comportamenti o caratteristiche personali) e forme di valutazione del rischio che una persona commetta un reato unicamente sulla base della profilazione; inoltre vieta, salvo deroghe tassative e sottoposte a rigorose condizioni, l'identificazione biometrica remota in tempo reale in spazi accessibili al pubblico.

---

[19] G.M. FLICK, *Intelligenza artificiale e processo: dalla riserva di legge ex ante a quella di giurisdizione ex post*, in *Sistema penale*, 4 dicembre 2025, 9.

[20] P.P. PAULESU, *Intelligenza artificiale e processo penale. Una lettura attraverso i principi*, in P.P.PAULESU, M. DANIELE, S. SIGNORATO, M. BOLOGNARI, A. BOLDRIN (a cura di), *Studi in onore di Roberto E. Kostoris*, Giappichelli, 2022, 24 e ss.

[21] G. GIGERENZER, *Perché l'intelligenza umana batte ancora gli algoritmi*, Cortina, 2023,119 ss.

dirittifondamentali.it

Sono, poi, classificati come ad alto rischio i sistemi destinati ad essere utilizzati dalle autorità di contrasto per valutare l'affidabilità degli elementi probatori, determinare il rischio di commissione del reato o di recidiva, effettuare la profilazione delle persone nel corso delle indagini o del perseguimento dei reati[22].

Il principio cardine è racchiuso nella "riserva di umanità" presente nel *Considerando 61*: gli strumenti di IA possono fornire sostegno al potere decisionale dei giudici, ma non sostituirlo; il processo decisionale finale deve rimanere un'attività a guida umana[23].

Tale principio, in realtà, era già stato fissato a livello eurounitario ad opera di strumenti di *soft law*, quali la Carta etica sull'uso dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi,[24] e di *hard law* come la Direttiva UE 2016/680 del 27 aprile 2016[25].

5. Indagini preliminari, "finestre di giurisdizione" e controllo sull'uso investigativo dell'IA

L'impatto dell'intelligenza artificiale risulta particolarmente rilevante nella fase delle indagini preliminari, oggi vero baricentro dell'accertamento penale e che, con molte probabilità, lo diverrà ancor di più proprio a seguito dell'introduzione degli strumenti predittivi, con la conseguente e progressiva marginalizzazione della formazione della prova in dibattimento.

[22] Regolamento (UE) 2024/1689, art. 1 e *Considerando 2, 8, 26 e 27.*

[23] Ivi, *Considerando 42.*

[24] Adottata il 3 dicembre 2018 dalla Commissione europea per l'efficienza della giustizia - Dipartimento per il programma di Governo, Focus, *Analisi del quadro normativo in materia di Intelligenza artificiale*, 23/04/2024, D.D.L. IA e Regolamento UE su IA, pp. 10 e Comunicato stampa, Consiglio dei ministri n.78, Palazzo Chigi, pag. 5, "attività giudiziaria", https://www.programmagoverno.gov.it/media/je0lo4i0/focus-ia.pdf.

[25] Recepita nell'ordinamento italiano dal d.lgs. 18 maggio 2018, n. 51, il cui art. 8 riprende i termini del divieto e dell'eccezione allo stesso. In questa ultima normativa sovranazionale, in realtà, si stabiliva un principio più circoscritto, ma anche più specifico e mirato, che fissava un divieto di decisioni automatizzate che producano effetti giuridici negativi o che incidano significativamente su una persona; lasciando, tuttavia, agli Stati membri la decisione, che deve prevedere garanzie adeguate alle libertà e ai diritti dell'interessato.

L'impego dell'IA durante le indagini può contribuire, in modo assai significativo, ad incrementare il "peso conoscitivo" degli atti investigativi[26].

L'uso di strumenti di IA come il riconoscimento facciale, l'analisi predittiva dei comportamenti sospetti, il monitoraggio automatizzato di comunicazioni, può compromettere l'efficacia delle garanzie difensive e favorire forme di controllo generalizzato e indiscriminato. Ciò è tanto più grave nei confronti di soggetti vulnerabili (migranti, persone senza fissa dimora etc.), statisticamente più esposti ad errori, controlli selettivi e falsi positivi[27].

In tale ambito, l'*AI Act* individua pratiche vietate e consente l'utilizzo di sistemi ad alto rischio solo nel rispetto di rigorose condizioni di necessità, proporzionalità, trasparenza e autorizzazione[28].

---

[26] R. E. KOSTORIS, *Intelligenza artificiale, strumenti predittivi e processo penale,* cit.,17

[27] M.PAPA, *Nuove tecnologie e "accesso alla giustizia" per le persone vulnerabili*, in A CADOPPI, S. CANESTRARI, C. CONTI, A. MANNA, M. PAPA (a cura di), *Tutela penale delle persone vulnerabili*, Milano, 2026, 1037.

[28] Sono vietate (art. 5, par. 1, lett. a-h) le pratiche di un sistema di IA: - che utilizza tecniche subliminali o manipolative o ingannevoli aventi l'effetto di distorcere materialmente il comportamento di una persona, anche sfruttandone la vulnerabilità; - che è mirato alla valutazione o classificazione delle persone sulla base del loro comportamento o di caratteristiche personali, inferendone un punteggio sociale pregiudizievole o sfavorevole (*social scoring*); - che effettua valutazioni o previsioni del rischio che una persona commetta un reato unicamente sulla base della profilazione della stessa (*profiling*), a meno che non sia utilizzato a sostegno della valutazione umana del coinvolgimento di una persona in un'attività criminosa, basata «su fatti oggettivi e verificabili direttamente connessi a un'attività criminosa»; - che crea o amplia banche dati di riconoscimento facciale mediante *scraping* di immagini facciali da *internet* o da filmati di telecamere; - che inferisce le emozioni di una persona nel luogo di lavoro, salvo che per motivi medici o di sicurezza; - che utilizza sistemi di categorizzazione biometrica che classificano le persone per trarne deduzioni in merito a razza, convinzioni politiche, sindacali, religiose, filosofiche, sessuali, a meno che il set di dati biometrici non sia acquisito legalmente come nel settore delle «attività di contrasto». È infine vietato (lett. h) l'uso di «sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico», finalizzati alla identificazione della persona senza il suo coinvolgimento attivo e a distanza, mediante il confronto dei suoi dati biometrici con quelli contenuti una banca dati. A meno che e nella misura in cui tale uso non sia strettamente necessario per la ricerca mirata di specifiche vittime di sottrazione, tratta o sfruttamento di esseri umani o di persone scomparse, per la prevenzione di una minaccia specifica sostanziale e imminente per la vita o l'incolumità fisica delle persone o di una minaccia reale e attuale o prevedibile di un attacco terroristico, per la localizzazione o identificazione di una persona sospettata di avere commesso un reato ai fini dell'indagine o dell'esercizio dell'azione penale o dell'esecuzione di una sanzione penale per i gravi crimini elencati *nell'Allegato II*, punibile con una pena privativa della libertà della durata massima di almeno quattro anni.

In assenza di una cornice normativa chiara, diventa pressante l'esigenza di un rafforzamento del controllo giurisdizionale già nella fase investigativa[29], secondo la scelta adottata dal "modello Cartabia"[30], di riconoscere una serie di rimedi ordinatori affidati al GIP o al GUP in taluni momenti topici delle indagini.

La regolamentazione sovranazionale, nella misura in cui introduce clausole aperte, deroghe e limitazioni per le pratiche vietate e per quelle ad alto rischio, impone il necessario adeguamento dell'ordinamento processuale interno[31].

In siffatta prospettiva, l'intervento del giudice nella fase investigativa è destinato a configurarsi non come elemento episodico, ma come presidio strutturale volto a contenere l'asimmetria tra accusa e difesa, assicurando che l'esercizio del potere investigativo resti entro i limiti tracciati dai principi del giusto processo. Il legislatore nazionale è chiamato a dislocare, con regole dettagliate, i poteri e le funzioni di accertamento tra polizia giudiziaria, pubblico ministero e giudice, riportando in equilibrio i rapporti tra tali soggetti anche mediante il ricorso a interventi ordinatori del giudice nella fase delle indagini, secondo la logica delle cosiddette "finestre di giurisdizione"[32].

Laddove l'attività di contrasto si concretizzi nell'utilizzo di strumenti di IA vietati o ad alto rischio[33], le operazioni di apprezzamento sulla stretta necessità e proporzione dell'uso, sulla valutazione d'impatto, sulla sussistenza dell'urgenza e

[29] Pur essendo dominata dal pubblico ministero, la fase delle indagini preliminari conosce significativi interventi del giudice, volti a controllare l'esercizio del potere investigativo e a garantire l'equilibrio tra le parti.V. M. GAITO, *Procedura penale*, Giappichelli, Torino, ult. ed.; P. TONINI, *Manuale di procedura penale*, Giuffrè, Milano, ult. ed.

[30] Il d.lgs. n. 150/2022 rafforza i meccanismi di controllo giudiziario, in particolare sotto il profilo della durata delle indagini e della verifica sull'esercizio dell'azione penale, al fine di garantire un più equilibrato bilanciamento tra esigenze investigative e tutela dei diritti fondamentali. Sulla riforma del processo penale attuata con d.lgs. 150/2022 e sul rafforzamento dei meccanismi di controllo giurisdizionale nella fase delle indagini, v. G. SPANGHER, *La riforma del processo penale e il ruolo del giudice*, in *Sistema penale*, 2022; F. VIGANÒ, *La riforma Cartabia del processo penale: prime riflessioni,* in *Sistema penale*, 2022.

[31] Ivi, *Allegato III*, punto 6.

[32] Ivi, *Considerando 61.* Sul tema delle "finestre di giurisdizione", in relazione al riequilibrio dei rapporti tra pubblico ministero e giudice nelle indagini, v. ancora G. CANZIO, *AI Act e processo penale: sfide e opportunità*, cit., 9.

[33] Si pensi alle pratiche di IA vietate di cui all'art. 5 del Regolamento e alla serie di deroghe ed eccezioni, che impegnano l'interprete in complesse operazioni di selezione delle regole applicabili nei singoli casi, quali, ad esempio, l'uso di sistemi di identificazione biometrica remota in tempo reale in spazi accessibili al pubblico a fini di attività di contrasto.

sulla gravità del pregiudizio da mancato utilizzo sembrano richiedere un controllo affidato a un giudice, non potendo essere rimesse integralmente al pubblico ministero, che pur resta parte[34] [35].

6. Prova algoritmica, art. 189 c.p.p. e contraddittorio "per" la prova

Le criticità diventano ancora più evidenti nella fase del giudizio, in funzione dell'introduzione e dell'ammissione della valutazione della *prova algoritmica*, cd. "*digital evidence*".[36]

Gli algoritmi, infatti, sono in grado di divenire preziosi alleati delle parti processuali, così come dello stesso giudice, per valutare, ad esempio, il grado di attendibilità dei testi oculari, fornendo più precise indicazioni su condizioni atmosferiche, visibilità, distanza del teste dal luogo di svolgimento dei fatti, o stabilire con maggiore precisione l'autenticità o la provenienza di un documento. Sempre ai fini probatori, oltre che investigativi, le tecnologie che presentano modalità "miste" (predittive/generative)[37] possono trovare applicazione nella ricostruzione facciale così come nella simulazione della scena del crimine.

Quando la prova stessa è prodotta o mediata da sistemi complessi o addestrati su *dataset* non immediatamente conoscibili, il tradizionale contraddittorio "sulla" prova appare insufficiente.

---

[34] G. CANZIO, *Indagini e giudizio fra regolamento (UE) 2024/1689 (AI Act) e legge n. 132 del 2025*, cit.

[35] Anche la giurisprudenza della Corte europea dei diritti dell'uomo sembra muoversi in questa direzione, sottolineando, ripetutamente, come, anche nelle fasi investigative, devono essere assicurate garanzie adeguate contro l'arbitrarietà, soprattutto quando vengono impiegate tecniche intrusive o strumenti tecnologicamente avanzati. Cfr. Corte EDU, *S. and Marper c. Regno Unito*, 4 dicembre 2008; Corte EDU, *Rowe and Davis c. Regno Unito*, 16 febbraio 2000; Corte EDU, *Edwards and Lewis c. Regno Unito*, 27 ottobre 2004.

[36] Queste prove assumeranno un aspetto rilevante nel prossimo futuro per le indagini poiché grazie all'evoluzione di queste tecnologie, in particolare di sistemi di IOT, *Internet of Things*, nonché di strumenti che sempre più sono presenti all'interno delle abitazioni, queste saranno in grado di fornire dettagli accurati e significativi; M. GIALUZ, *Prove fondate sull'intelligenza artificiale e diritti fondamentali*, in *Diritto di Difesa*, 15 gennaio 2025, 4.

[37] "Miste" in quanto ricostruiscono (quindi generano) il presente (come nel caso di ricostruzione facciale) o il passato (scena del crimine), prendendo a prestito dati del passato, ovvero mediante l'utilizzo di tecniche predittive. Sull'utilizzo dell'IA per il riconoscimento facciale v. J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?* In G. DI PAOLA, L. PRESSACCO (a cura di*), Intelligenza artificiale e processo penale Indagini, prove, giudizio*, Editoriale Scientifica, 2022, 12.

Occorre comprendere come organizzare correttamente l'accesso di questo peculiare tipo di prova nell'ambiente del processo penale, assicurando la sua legalità e utilizzabilità, oltre ad un legittimo spazio per l'esercizio del diritto di difesa, attraverso il confronto dialettico, la confutazione, la prova contraria, contro la deriva algoritmica della giurisdizione.

Più efficace sarebbe prevedere un filtro preliminare di ammissibilità, accompagnato da un contraddittorio anticipato "per" la prova, così da evitare l'ingresso nel dibattimento di informazioni non sorrette da una previa validazione di attendibilità o utilizzabilità.

In tale prospettiva, l'art. 189 c.p.p. offre una base normativa significativa. Il prodotto dell'intelligenza artificiale, nella misura in cui costituisce una prova digitale e scientifica non specificamente disciplinata dalla legge, rientra infatti nella disciplina delle prove atipiche, la cui ammissione richiede la dimostrazione positiva della loro idoneità ad assicurare l'accertamento dei fatti e la preventiva instaurazione del contraddittorio sulle modalità di assunzione[38].

Per il più rigoroso vaglio di attendibilità richiesto per le prove atipiche, occorre tenere conto anche dei criteri elaborati dalla giurisprudenza di legittimità in tema di prova scientifica, sulla scorta dei canoni *Daubert*[39].

In sede penale, inoltre, alcuni strumenti predittivi sono destinati a fungere da indicatori di rischio, sia in sede prevenzione criminale che all'interno della singola vicenda giudiziaria.

Sotto il primo profilo, le *predictive policy* mirano a fornire affidabili indici di rischio di commissione di futuri reati in determinati luoghi e/o da parte di determinate

[38] G. CANZIO, *Indagini e giudizio fra regolamento (UE) 2024/1689 (AI Act) e legge n. 132 del 2025*, cit.,12.

[39] Secondo *Daubert v. Merrel Dow Pharmaceuticals*, Inc., 509 US 579 (1993), il giudice deve vagliare l'affidabilità di una teoria o un metodo e di una *expert witness's scientific testimony*, ai fini della loro ammissibilità come prova scientifica, per i seguenti profili: controllabilità mediante esperimenti; falsificabilità attraverso test di smentita con esito negativo; *peer review* della comunità scientifica di riferimento; conoscenza della percentuale di errore dei risultati; infine, generale accettazione da parte della comunità degli esperti. Criteri, questi, sostanzialmente condivisi e anzi arricchiti dalla giurisprudenza di legittimità. Cfr. Cass. pen., Sez. IV, sentenza del 17 settembre 2010, n. 43786, *Cozzini*; Sez. Un., sentenza dell'11 settembre 2002, n. 30328, *Franzese*. Cfr, anche Corte EDU, *S. and Marper c. Regno Unito*, 4 dicembre 2008.

persone. Nel processo l'Ai predittiva può tornare utile in tema di recidiva, nella disposizione, ad esempio, di una misura cautelare o in sede decisionale, per la commisurazione della pena.

Entrambe le applicazioni possono presentare il rischio di fuorvianti profilature degli individui, non lontane, secondo alcuni autori[40], dalla criminologia di Cesare Lombroso e foriere di possibili disuguaglianze e discriminazioni.

Sotto questo profilo, l'esperienza comparata offre un esempio emblematico nelle criticità emerse attorno al sistema statunitense *COMPAS*, utilizzato per la valutazione del rischio di recidiva. Basato su modelli statistici e tecniche di profilazione, il sistema attribuisce un punteggio di rischio sulla scorta di una pluralità di variabili, tra cui dati personali, precedenti penali e informazioni socio-economiche. Lo studio, condotto da *ProPublica* nel 2016, evidenziò significative distorsioni nei risultati prodotti dal *software*, evidenziando che gli imputati neri venivano più frequentemente classificati come ad alto rischio rispetto agli imputati bianchi, pur in assenza di una effettiva maggiore recidiva.[41] L'esperienza *COMPAS* mette in luce una duplice criticità: da un lato, il problema dei *bias* algoritmici derivanti dalla qualità dei dati di partenza utilizzati, che riflettono scelte e visioni del programmatore informatico; dall'altro, il problema della opacità del modello decisionale, che rende estremamente difficile per la difesa contestarne il funzionamento. Non a caso, già nel *leading case State v. Loomis*[42], la Corte Suprema del *Wisconsin* aveva chiarito che il *software COMPAS* non poteva costituire il

[40] G. ZACCARIA, *Postdiritto. Nuove fonti, nuove categorie*, Il Mulino, 2022, 63 ss. In particolare, a p.127, l'A. sottolinea come il «determinismo predittivo dell'algoritmo (consacra un aggravamento delle disuguaglianze, riproducendo su scale più vaste situazioni già in partenza di disuguaglianza", oltre a poter "determinare ingiustificabili discriminazioni indirette, ma non meno incisive, a danno degli individui che appartengono a tali gruppi, che possono essere stabilmente etichettati come *future criminals*». Analogamente, C. O'NEIL, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, New York, Crown, 2016.

[41] Nel Report si legge, significativamente, che il sistema era "*biased against black defendants*".

[42] *State v. Loomis*, 881 NW 2d 749 (Wis 2016). Sulla decisione v. K. FREEMAN, *Algorithmic injustice: how the Wisconsin Supreme Court failed to protect due process rights in State v. Loomis*, in *North Carolina Journal of Law and Technology*, n.5, 2016, 75 ss.

fondamento esclusivo della decisione, ma soltanto "*one of many factors*", da corroborare con ulteriori elementi informativi affidabili[43].

Il criterio della non esclusività del risultato algoritmico appare, dunque, funzionale a sterilizzare gli effetti perversi dei *confirmation bias* e a riaffermare che il giudice è tenuto ad integrare le stime probabilistiche offerte dall'algoritmo con le altre informazioni probatorie acquisite nel procedimento[44].

Nello stesso senso si colloca la giurisprudenza della Corte EDU, secondo cui l'utilizzo di prove o informazioni non accessibili alla difesa può compromettere il diritto al contraddittorio e all'equità del processo, salvo la presenza di adeguate garanzie compensative[45]. La Corte vieta altresì automatismi di valutazione della pericolosità sociale[46].

In conclusione, l'assunzione di prove digitali potrebbe portare al sistema giudiziario numerosi vantaggi, nonostante la loro costante evoluzione e difficoltà di inquadramento ai fini probatori, a condizione che vengano adottate tutte le precauzioni necessarie e che l'utilizzo di procedure informatizzate non costituisca motivo di elusione dei principi che conformano il nostro ordinamento.

7. Interpretazione giuridica e funzione decisoria

Le maggiori criticità nell'applicazione degli algoritmi al sistema giustizia risiedono nell'utilizzo degli stessi da parte dei giudici nella loro attività decisoria.

Numerosi sono i *tools* che l'intelligenza artificiale può mettere a disposizione dei giudici. Gli algoritmi possono rappresentare un affidabile supporto nell'accertamento dei fatti, nella valutazione del materiale probatorio e

[43] Art. 189 c.p.p.

[44] Si orientano per la stessa conclusione, muovendo invece da una più specifica considerazione ermeneutica relativa al testo dell'art. 11 par.1 Direttiva 2016/680/UE e dell'art. 8.1 d.lgs. 18 maggio 2018, n. 51, 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, 17; L. PRESSACCO, *Intelligenza artificiale e ragionamento probatorio nel processo penale*, in G. DI PAOLO, L. PRESSACCO (a cura di), *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, cit., 105 ss., che evidenzia, peraltro, la possibilità di utilizzare invece quei trattamenti *in utilibus.*

[45] Cass. pen., Sez. Un., sentenza dell'11 settembre 2002, n. 30328, *Franzese*; Sez. IV, sentenza del 17 settembre 2010, n. 43786, *Cozzini*; Sez. V, sentenza del 27 marzo 2015, n. 36080, *Knox*.

[46] Corte EDU, *M.M. vs Paesi Bassi*, 8 aprile 2024, ric. N 39339/98.

nell'individuazione di orientamenti giurisprudenziali rilevanti, contribuendo a ridurre errori cognitivi e ad ampliare le capacità conoscitive del decisore, nell'ottica di una "intelligenza aumentata" [47]. L'uso dell'IA può giungere alla stessa attività di *sentencing*, offrendo migliori parametri di controllo dei passaggi logico inferenziali del ragionamento giudiziario[48]. Gli strumenti predittivi possono anche essere impiegati in veste pienamente "decisoria", volti, cioè, a diagnosticare futuri orientamenti dei giudici in casi simili, favorendo, così, il ricorso a strumenti deflativi del contenzioso e orientare la scelta di soluzioni alternative al giudizio[49].

Permane, certamente, una differenza strutturale tra il funzionamento dei sistemi di intelligenza artificiale e il ragionamento giuridico: i primi operano attraverso correlazioni statistiche tra dati laddove il secondo si fonda su connessioni logiche e nessi causali[50].

Gli algoritmi sono concepiti per lavorare senza regole predefinite, anche in presenza di dati vaghi, indeterminati, discrezionali, facendo ricorso a sistemi di autoapprendimento (cd. *machine learning*) in cui lo strumento, appunto, apprende, implementando le sue prestazioni, dalla sua stessa attività di processione dei dati, aggiungendo nuove correlazioni rispetto a quelle inserite originariamente dal programma[51]. Tuttavia, i *Large Language Model*, sebbene particolarmente efficaci nell'elaborazione linguistica e nell'individuazione di regolarità statistiche, non governano, almeno allo stato, la semantica pura e, pertanto, sono incapaci di

[47] N. LETTIERI, *Contro la previsione. Tre argomenti per una critica del calcolo predittivo e del suo uso in ambito giuridico*, in *Ars Interpretanti*, 2021, 92.

[48] L. LUPARIA DONATI, *Notazioni controintuitive su intelligenza artificiale e libero convincimento*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Centro nazionale di prevenzione e difesa sociale - Convegni di studio «Enrico de Nicola». Problemi attuali di diritto e procedura penale, Milano, 2021, 117 ss.

[49] Tale impiego potrebbe favorire il ricorso a strumenti di *diversion* e ad altre forme di definizione anticipata del procedimento, come già avviene in alcuni ordinamenti attraverso l'utilizzo della giustizia predittiva quale supporto alla soluzione stragiudiziale delle controversie. Per un approfondimento: A. SIMONCINI, *La dimensione costituzionale della giustizia predittiva. Riflessioni su intelligenza artificiale e processo* in *Rivista di diritto processuale*, 2024, 389 e ss.

[50] J. ANGWIN, J. LARSON, S. MATTU, L. KIRCHNER, *Machine Bias*, in *ProPublica*, 2016.

[51] M. KUBAT, *An introducing to machine learning*, Spriger Cham, 2017.

dirittifondamentali.it

penetrare il senso isolato delle parole[52]. Inoltre, non dispongono di una reale comprensione del contesto fattuale e non sono in grado di sostituire l'attività interpretativa che caratterizza l'esercizio della giurisdizione. Difettano, pertanto, in capacità raziocinante, creatività e generazione originale, fondamentali quando i contesti sono incerti e mutevoli[53].

Al di là degli innegabili risultati di "stabilità" dell'ordinamento giurisprudenziale, il pericolo principale risiede, allora, nella prospettiva di un progressivo consolidarsi di forme di "conformismo giudiziario" basate sulla "tirannia del precedente", tale da rappresentare un limite all'evoluzione del diritto, oltre a condurre ad una sostanziale deresponsabilizzazione del giudice (e, aggiungerei, del difensore).

Un impiego generalizzato ed un affidamento acritico nell'IA, da parte dei giudici in ogni grado di giudizio, finirebbe, così, per degradare la funzione nomofilattica della giurisprudenza alla standardizzazione algoritmica del precedente.

Il rischio è quello di una giurisprudenza che perde la propria vitalità, facendo vivere le norme nel tempo e adeguandone l'interpretazione ai mutamenti della società.

In questa prospettiva, particolare attenzione merita l'utilizzo dell'IA nella redazione dei provvedimenti giudiziari. Se appare opportuno escludere ogni forma di automazione del dispositivo, stante il rischio di una sostanziale delega della decisione alla macchina, maggiori margini sembrano sussistere con riguardo all'impiego di strumenti generativi come supporto alla motivazione, purché il giudice mantenga il pieno controllo del percorso argomentativo e assuma integralmente la responsabilità della decisione[54].

---

[52]F. ROSSI, *Il confine del futuro. Possiamo fidarci dell'intelligenza artificiale?* Feltrinelli, 2019, 67; S. QUATTROCOLO, *Artificial intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Springer, 2020, 120.

[53] R. BALIOTTA, *Giustizia, errore, intelligenza artificiale*, in *Sistema penale*, 2/2023 sottolinea il ruolo del sentimento nella valutazione dei fatti della vita, in ausilio alla ragione e all'intuizione.

[54] R. E. KOSTORIS, *Intelligenza artificiale, strumenti predittivi e processo penale*, cit., 12. L'A. definisce come «rischio assai concreto che di fatto i termini logici di quella sequenza vengano invertiti e che il giudice finisca per demandare la stessa decisione alla macchina.». L'A. suggerisce: «Per non indurlo in questa tentazione è dunque opportuno escludere in partenza

Sebbene il codice attribuisca espressamente al giudice, e non ad altri, il dovere di dar conto dei motivi della sua decisione, è anche vero che quest'attività potrebbe non definirsi *tout court* vietata, almeno nella misura in cui viene considerata alla stregua di un contributo offerto al giudice[55], che spetta a lui eventualmente recepire, assumendosene la piena paternità[56].

In linea di principio, dunque, potrebbe non destare particolare preoccupazione il fatto che un singolo giudice si possa giovare di un ausilio degli algoritmi nella redazione della motivazione[57].

La soluzione allora depone - oltre ad un impiego integrato uomo-macchina, che impedisca di attribuire ai precedenti una funzione "paranormativa" - sulla qualità degli *input* inseriti per "addestrare" l'algoritmo interpellato dal giudice[58]. Sentenze, massime, dottrina, banche dati dovranno essere complete[59], aggiornate e non discriminatorie, neutralizzando al massimo i fenomeni di cd. allucinazione informatica. Un "modello di sentenza" utilizzabile potrebbe quello della CorteEDU, strumento utile nella costruzione del patrimonio comune, consentendo una identificazione immediata, da parte dell'IA, dei fatti rilevanti[60].

Così come, sempre attingendo dall'esperienza della giurisprudenza sovranazionale, di indubbia utilità potrebbe essere la redazione di guide sui diritti,

---

l'ammissibilità di una redazione automatizzata del dispositivo, la quale, oltretutto, in sé e per sé non varrebbe ad alleggerire in modo significativo il lavoro giudiziario".

[55] A ben guardare, la stessa istituzione dell'ufficio per il processo testimonia come il legislatore abbia già valorizzato forme di supporto all'attività del giudice, affidate a soggetti incaricati di coadiuvarlo anche nella predisposizione di bozze di sentenza.

[56] In omaggio al principio di trasparenza e di lealtà digitale, dovrebbe essere statuito, parimenti a quanto avviene per gli avvocati, il diritto ad essere informati dell'eventuale utilizzo di strumenti tecnologici nella decisione, con il conseguente dovere di informativa da parte del giudice.

[57] Di segno contrario la giurisprudenza. V., ad esempio, TAR Lazio, sentenza del 3 marzo 2025, n. 4546. I giudici amministrativi, nonostante la dichiarata apertura in positivo verso l'impiego di piattaforme di intelligenza artificiale, si sono pronunciati contrari all'utilizzo della piattaforma "ChatGPT" limitatamente alle interrogazioni effettuate su di essa, poiché «prive di qualunque fondamento logico e giuridico».

[58] R.E. KOSTORIS, *Intelligenza artificiale, strumenti predittivi e processo penale,* cit., 12.

[59] O. DI GIOVINE, *Interpretazione umana e robotica*, cit

[60] O. DI GIOVINE, *Interpretazione umana e robotica*, cit.,

in grado di fornire una ricostruzione aggiornata e accessibile dell'attuale diritto vivente attraverso l'esposizione della giurisprudenza in determinati settori. [61]

Discorso differente, invece, dovrebbe essere condotto per i casi più complessi per i quali il ricorso a motivazione automatizzate dovrebbe considerarsi vietato a causa delle opacità degli algoritmi, che potrebbe rappresentare, a differenza da quelli caratterizzati da una certa opacità, di più difficile impugnazione per la difesa.

Se, tuttavia, anche i giudici dei gradi successivi, a cui viene affidato il controllo sulla decisione del giudice di *primae curiae* dovessero, a loro volta, far uso dell'IA, si finirebbe per generare un verso un preoccupante scenario di "algoritmi che controllano algoritmi"[62], con una sostanziale aggiramento dell'obbligo di motivazione di cui al sesto comma dell'art.111C.

8. La legge n. 132 del 2025: un primo passo, ancora incompleto

Sul piano interno, la legge n. 132 del 2025 rappresenta il primo intervento organico del legislatore italiano, volto a disciplinare l'impiego dell'intelligenza artificiale nelle professioni giuridiche e nell'attività giudiziaria, in attuazione del quadro europeo delineato dall'*AI Act*.

Per quanto riguarda le professioni intellettuali, l'art. 13 limita l'utilizzo dell'IA per attività strumentali e di supporto, quali la ricerca giurisprudenziale o la gestione documentale, con un contributo umano prevalente, sia sotto il profilo qualitativo che quantitativo[63]oltre ad un obbligo di trasparenza nei confronti del cliente.[64]

---

[61] Cfr. modelli operativi adottati nel Tribunale di Palermo con provvedimento del 30 dicembre 2022, consultabile in www.tribunale-palermo.giustizia.it/cmsresources/cms/documents/Prot.17761.pdf. Così come Procura di Tivoli sui reati in tema di femminicidio: *Linee guida sull'applicazione del delitto di cui all'art. 572 c.p. e su questioni procedimentali /processuali relative ai reati di violenza di genere, domestica e contro le donne. Esposizione ragionata della più recente giurisprudenza della Corte di Cassazione,* Procura presso il Tribunale di Tivoli, Protocollo nr. 2189.U del 16.09.2025, in *Giurisprudenza penale*, 22 settembre 2025.

[62] R. E. KOSTORIS, *Intelligenza artificiale, strumenti predittivi e processo penale,* cit., 14.

[63]Sul rischio di standardizzazione del precedente A. BALSAMO, *L'impatto dell'intelligenza artificiale nel settore della giustizia*, cit.

[64] Meritano, in tal senso, menzione le *Linee Guida* CNF sui requisiti essenziali per l'affidamento del sevizio all'IA del 10 settembre 2025: utilizzo per le analisi documentali e l'estrazione di informazioni e, obbligo di fornitori localizzati UE, con divieti transnazionali, rispetto della segretezza e del GDPR.

Nell'attività giudiziaria, l'art. 15 afferma, in modo esplicito, che restano riservate al magistrato tutte le decisioni fondamentali: interpretazione della legge, valutazione dei fatti e delle prove, adozione dei provvedimenti.; con esclusione esplicita dell'utilizzo della "giustizia predittiva" nelle decisioni che incidono direttamente sull'esito del giudizio, al fine di evitare che l'algoritmo possa orientare o condizionare la funzione giurisdizionale.

L'intelligenza artificiale è, invece, ammessa per attività accessorie e di supporto, coerentemente con il modello europeo. Essa può essere impiegata per l'organizzazione dei servizi giudiziari, la gestione documentale, l'analisi statistica dei dati, la ricerca e sistematizzazione della giurisprudenza, l'anonimizzazione delle decisioni, nonché in progetti sperimentali finalizzati a migliorare l'efficienza del sistema senza incidere sul nucleo decisionale.

Un uso molto utile potrebbe, ad esempio, riguardare il calcolo dei termini di prescrizione i di quelli massimi delle misure cautelari personali, che tenga conto delle diverse normative applicabili, in grado di incidere anche sulla programmazione delle udienze

La legge introduce, inoltre, meccanismi di sperimentazione controllata e promuove la formazione digitale di magistrati e personale amministrativo[65].

Sebbene il legislatore interno abbia compiuto un primo passo significativo, la disciplina presenta rilevanti profili di criticità.

In primo luogo, l'eccessiva centralizzazione nel Ministero della giustizia del potere autorizzatorio e di governo del processo di digitalizzazione solleva interrogativi in ordine alla tutela dell'indipendenza della magistratura[66]. Inoltre, il mancato coinvolgimento del Consiglio Superiore della Magistratura nella *governance* complessiva del fenomeno appare particolarmente problematico, atteso il possibile impatto delle scelte tecnologiche sull'esercizio concreto della funzione giurisdizionale.

[65] Legge 25 settembre 2025, n. 132, artt. 1, 13, 15 e 24.
[66] Ibidem, art. 13.

Più in generale a preoccupare è la genericità dei principi e dei criteri direttivi della delega contenuta nell'art. 24, rispetto all'obiettivo di una effettiva armonizzazione del sistema processuale penale interno. Nulla viene detto, ad esempio, circa i poteri, i divieti, le condizioni, i limiti e le procedure dirette ad acquisire, utilizzare e valutare la prova digitale, generata in via deduttiva dai sistemi di IA.

Alla macchina verrà chiesto di analizzare verbali di testimonianza, atti e documenti; individuare norme vigenti rilevanti per la causa; reperire precedenti decisioni su casi identici o analoghi; scrivere bozze di testo di provvedimenti. Occorrono, inoltre, nuove regole per il contradditorio e per l'esercizio del diritto di difesa, per gli accertamenti tecnici.

9. La sfida della giurisdizione digitale: un nuovo modello di conoscenza

L'impiego dell'intelligenza artificiale nel processo penale non può essere ricondotto ad una questione meramente tecnologica o organizzativa, ma deve essere inquadrato nel più ampio problema delle condizioni di esercizio e di legittimazione del potere nelle democrazie costituzionali contemporanee.

La riflessione sulla prova algoritmica e sull'impiego dei modelli linguistici conferma che il nodo centrale non risiede nella maggiore o minore accuratezza degli strumenti tecnologici, ma nella possibilità di sottoporli a un controllo effettivo nell'ambito del contraddittorio. Laddove tale controllo risulti limitato o precluso, si determina una tensione con i principi fondamentali del processo penale, che trovano nel confronto dialettico tra le parti e nella motivazione della decisione i loro presidi essenziali.

La narrazione di una cooperazione dialogica uomo-macchina nella prospettiva di un'intelligenza aumentata, così come indicato dal legislatore interno oltre che sovranazionale, appare una prospettiva a dir poco ottimistica. L'auspicato controllo umano, come già avvenuto nella storia, tende fisiologicamente ad affievolirsi con il progressivo affinamento dei modelli, sino a sfociare in un affidamento acritico nel materiale da essi processato.

dirittifondamentali.it

Nonostante i limiti posti da *IA Act*, sarà difficile immaginare che il giudice-uomo, nel segreto della sua stanza, si sottragga alla tentazione di interrogare l'algoritmo anche sulla soluzione giuridica del caso e nella redazione della motivazione, così come del dispositivo.

La sfida che si pone, allora, sta nel costruire un sistema in grado di governare una relazione inevitabile, nella quale l'affidamento umano sull'intelligenza artificiale è destinato ad aumentare, per l'innata progressiva assuefazione dell'uomo nei confronti delle macchine[67].

In questo quadro, al processo penale, oltre alla tradizionale funzione di accertamento di fatti penalmente rilevanti, viene riconosciuta una ulteriore funzione "istituzionale": diventa spazio privilegiato di «controllo significato»[68] del potere tecnologico, nel quale si realizza il bilanciamento tra esigenze di efficienza e tutela dei diritti fondamentali, evitando che l'innovazione si traduca in una riduzione delle condizioni di esercizio del diritto di difesa e del contraddittorio. Un controllo che va assicurato, in ugual modo e in ugual misura, a tutti i protagonisti del processo (all'imputato e alle altre parti private non meno che al pubblico ministero e al giudice), al fine di mantenere, di fronte agli strumenti IA, quell'equilibrio di forze che deve sempre caratterizzare le dinamiche processuali; «pur nella consapevolezza che l'atteggiarsi di quegli stessi diritti e di quelle stesse dinamiche saranno comunque destinati a subire mutamenti profondi per effetto dell'ingresso degli strumenti algoritmici nel processo»[69].

[67] Anche la giurisprudenza italiana ha iniziato a confrontarsi con i rischi derivanti dall'uso non verificato di strumenti di intelligenza artificiale generativa. La Cassazione, con la sentenza n. 25455/2025, ha annullato una decisione fondata su riferimenti giurisprudenziali inesatti, segnalando come il fenomeno possa coinvolgere la stessa funzione giudicante. Parallelamente, numerose pronunce di merito hanno censurato atti difensivi contenenti citazioni normative o giurisprudenziali inesistenti generate dall'IA, talora riconoscendo la responsabilità aggravata ex art. 96 c.p.c. e disponendo anche la trasmissione degli atti ai competenti Consigli dell'Ordine. Da ultimo, il Tribunale di Siracusa (sent. n. 338/2026) ha qualificato come colpa grave l'utilizzo non verificato di output generati dall'intelligenza artificiale, contribuendo a definire uno standard di diligenza professionale per gli operatori del diritto.

[68] G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Giuffrè Francis Lefevre, 2021, 9 ss.

[69] R. E. KOSTORIS, *Intelligenza artificiale, strumenti predittivi e processo penale*, cit., 3.

È in tale sede che le garanzie previste dal diritto europeo e dal diritto interno possono trovare concreta attuazione, trasformandosi da enunciazioni di principio in strumenti effettivi di tutela.

La legge n. 132/2025 si colloca in questo percorso, senza, tuttavia, fornire l'architrave per la costruzione di un modello di integrazione dell'intelligenza artificiale compatibile con i principi del giusto processo e con le esigenze di una democrazia costituzionale.

In attesa di una più dettagliata regolamentazione, il ruolo della giurisdizione si fa decisivo non solo nell'applicazione delle regole, ma come presidio che tali regole vengono "riempite di contenuto" attraverso il contraddittorio, la valutazione della prova, la motivazione della decisione e il controllo impugnatorio.

In questo contesto, la richiamata nozione di sicurezza algoritmica consente di ricondurre ad unità i diversi profili coinvolti — tecnici, procedurali e istituzionali — evidenziando come la compatibilità tra intelligenza artificiale e processo penale dipenda dalla sussistenza di condizioni che garantiscano l'affidabilità dei sistemi, la conoscibilità dei loro esiti e la riconducibilità della decisione ad un soggetto responsabile.

Giuristi ed algoritmica sono, dunque, chiamati a costruire un nuovo modello di conoscenza, condiviso e raffinato, connotato dalla controllabilità e giustificabilità delle decisioni, nel solco dei valori etici di spiegabilità, trasparenza, controllo umano significativo e autonomia del decisore[70].

In definitiva, la tenuta democratica degli ordinamenti contemporanei non dipenderà dalla capacità di arrestare il progresso tecnologico, ma dalla possibilità di orientarlo entro i confini tracciati dalla Costituzione e dai diritti fondamentali. La vera sfida consiste nel prevenire quelle fratture antropologiche che l'intelligenza artificiale può determinare e nel preservare una giustizia comprensibile, contestabile e, irriducibilmente, umana.

[70] N. LIPARI, *Il diritto del nuovo millennio tra giurisdizionalizzazione ed algoritmo*, in *Accademia*, 2024, 9 ss.

L'auspicio è che il Governo, nell'esercizio delle deleghe conferite dalla legge n. 32/2025, tenga adeguatamente conto di queste esigenze, impedendo che l'innovazione si traduca in una regressione delle garanzie, anziché in un'occasione di loro rinnovato consolidamento.

dirittifondamentali.it