Università di Foggia
Giurisprudenza

UNIVERSITÀ DI SIENA
1240

DIPARTIMENTO DI GIURISPRUDENZA

DOTTORATO IN SCIENZE GIURIDICHE

XXXVII CICLO

Tesi di dottorato in Diritto processuale penale

INTELLIGENZA ARTIFICIALE E PROCESSO PENALE UN CONNUBIO POSSIBILE?

Tutor: Chiar.mo Prof. Sergio Lorusso

SERGIO LORUSSO 23.02.2025 13:53:14 GMT+02:00

Dottoranda: Anna Chiara Dellerba

ANNA CHIARA DELLERBA 22.02.2025 12:15:09 GMT+02:00

Anno accademico 2023/2024

INTELLIGENZA ARTIFICIALE E PROCESSO PENALE.

UN CONNUBIO POSSIBILE?

CAPITOLO IV

DECISIONE ALGORITMICA E *STANDARD* DI GIUDIZIO

INTRODUZIONE

Con il presente lavoro si propone di analizzare la complessa relazione tra intelligenza artificiale (di seguito, *AI*) e processo penale al fine di ipotizzarne un possibile connubio.

Prima di entrare in *medias res*, è opportuna una precisazione terminologica. L'espressione "processo penale" è impiegata in questa sede nella sua accezione più ampia e omnicomprensiva, come insieme delle fasi che conducono all'adozione della decisione finale, *ivi* compreso il momento investigativo.

Tale scelta è giustificata dalla necessità di offrire una prospettiva a tutto tondo dei verosimili utilizzi dell'*AI* nel corso del "processo", pur riservando particolare attenzione alle dinamiche decisorie.

Lo studio prende le mosse da un dato inconfutabile: il tumultuoso avvento della tecnologica e, in particolare, dell'*AI* − che, in pochi decenni, è divenuta indiscussa protagonista del mondo contemporaneo – produce inevitabili riflessi anche sul versante giuridico; tale presa di coscienza induce lo studioso ad un'attenta riflessione sulle sorti della giustizia penale, nel tentativo di rispondere ai molteplici interrogativi che sorgono dal rapporto tra algoritmi e dinamiche processuali, ad oggi ancora privi di riscontro.

La tesi, dopo una prima parte ricostruttiva dello stato dell'arte della materia, anche attraverso la lente della comparazione, individua precisi spazi applicativi per i sistemi algoritmici nei vari segmenti processuali, con particolare attenzione alla possibile "automazione" delle dinamiche decisorie, non senza tener conto dei rischi e della potenzialità legati all'impiego dei modelli computazionali.

In particolare, dopo aver tratteggiato il perimetro della nozione di *AI*, così come intesa in ambito europeo ed extraeuropeo, si ripercorrono, punto per punto, le tappe del lungo cammino verso la regolamentazione.

Da anni, infatti, le istituzioni europee, con diverse iniziative legislative, hanno tentato di disciplinare il rapporto tra diritto e *AI* con fonti di *soft law*, troppo spesso disattese dai singoli Stati membri.

Da qui, la necessità di prevedere una disciplina organica che ha condotto all'approvazione del Regolamento europeo 2024/1689 sull'intelligenza artificiale

del 13 giugno 2024 (c.d. *AI Act*), che interviene sullo stratificato panorama normativo al fine di adottare un *legal framework* uniforme.

Più cauto è, invece, l'atteggiamento del legislatore italiano.

È in cantiere, difatti, il disegno di legge A.S. n. 1146 recante "Disposizioni e delega al governo in materia di intelligenza artificiale" del 23 aprile 2024 (attualmente al vaglio del Parlamento), che però, allo stato, sembrerebbe vietare a priori l'ingresso di *software* predittivi nelle aule di giustizia, ponendosi in prospettiva diversificata rispetto all'*AI Act*.

Occorre altresì volgere lo sguardo al panorama mondiale, atteso che, sebbene l'Europa si sia aggiudicata il ruolo di capofila adottando il primo documento legislativo di *hard law* in materia, anche altri Paesi stanno cercando di dotarsi di una disciplina organica per far fronte alla "rivoluzione dei bit".

Si passa quindi ad analizzare in chiave comparata le diverse sperimentazioni dei sistemi di *AI* nell'intero arco procedimentale: dalla fase pre-investigativa, prodromica all'acquisizione della *notitia criminis*, a quella delle indagini preliminari, sino a giungere alle dinamiche probatorie e ai meccanismi decisori conclusivi.

La diversa architettura dei sistemi processuali − di *common law* e di *civil law* − presi in considerazione spiega le resistenze esistenti circa l'ammissione di modelli algoritmici nella giurisdizione italiana, giustificandone, di contro, il massivo impiego fuori dalla frontiera europea.

Si parla ormai dell'uso di algoritmi di *pre-crime* che, sull'onda di ciò che sembrava soltanto finzione cinematografica e, malgrado lo scetticismo di gran parte della dottrina, hanno reso l'area investigativa il primo segmento del procedimento penale ad essere sedotto dal potere dell'*AI*.

Negli Stati Uniti dilaga, infatti, l'uso di *tools* di *predictive policing* basati su tecnologie algoritmiche, nonostante l'ostilità di coloro i quali denunciano importanti ricadute sul piano del trattamento dei dati personali.

Diversa è la questione che riguarda l'impiego, sempre nella fase delle indagini preliminari, dei sistemi di riconoscimento facciale.

Detto meccanismo, storicamente risalente al XVII secolo, si evolve nell'Ottocento, quando nasce l'antropometria.

Ai giorni nostri, ulteriori passi in avanti sono stati compiuti con l'*AI*; tuttavia, stante la pericolosa intrusività dell'algoritmo, il legislatore europeo ha dettato precise regole da rispettare e condizioni da soddisfare per ammetterne l'impiego in sede processuale.

Sul versante probatorio, invece, oltre ai meccanismi computazionali utilizzati come mezzo di ricerca della prova, di particolare rilievo è il tema della valutazione algoritmica del dato probatorio e quello della c.d. *digital evidence*, la cui naturale evoluzione è costituita dalle c.d. "prove algoritmiche" in senso stretto ovvero formate direttamente da meccanismi di *AI*.

Ampiamente diffusi nei sistemi di *common law* sono pure i *risk assessment tools:* si tratta di strumenti che attraverso *software* effettuano una "valutazione del rischio" riferita ad un determinato soggetto, restituendo, in sostanza, una prognosi relativa al verificarsi di possibili condotte delittuose.

Si richiede, dunque, a detti modelli computazionali di prevedere il comportamento futuro dell'indagato/imputato in base a determinati "fattori di rischio".

La prima sperimentazione pratica di tali applicativi è avvenuta negli Stati Uniti nel processo penale a carico di Eric Loomis − divenuto, ormai, il più noto *leading case* in materia − in cui la Corte territoriale ha impiegato l'algoritmo COMPAS per valutare la pericolosità sociale dell'imputato, avviando una vera e propria "rivoluzione giurisdizionale" sul metodo di accertamento della capacità di recidiva; l'uso processuale di detto strumento è stato in grado di attirare l'attenzione, a livello mondiale, dell'intera comunità scientifica che ha mostrato dubbi e perplessità circa l'ammissibilità di questi *tools* nelle dinamiche decisorie.

Ci si soffermerà quindi sul tema della decisone penale e, in particolare, sul multiforme nesso che potrebbe instaurarsi tra "giustizia predittiva", pericolosità sociale e *standard* di giudizio.

Si vaglierà la tenuta "algoritmica" dei vari moduli decisori – anche di carattere interlocutorio – del procedimento penale domestico, chiarendone i profili di compatibilità con le regole processuali e i punti di rottura rispetto agli *standard* di giudizio ivi impiegati.

La metodologia utilizzata per condurre detto studio è ancorata al dato normativo disponibile; è, infatti, attraverso la lente del Regolamento europeo sull'intelligenza

artificiale – in cui si categorizzano come "ad alto rischio" i sistemi artificiali di amministrazione della giustizia − che si ritiene di ipotizzare l'impiego di applicativi di *AI* nella sfera processuale, chiarendone, però, l'estensione operativa e i limiti di applicabilità.

L'esigenza di introdurre "agenti artificiali" nel processo penale deriva dalla consapevolezza di un significativo mutamento della figura del decisore che da "uomo senza volto", è divenuto giudice suggestivo, emotivo, sentimentale ed empatico.

È opportuno, dunque, chiedersi se è compatibile la categoria della pericolosità sociale con l'utilizzo di sistemi algoritmici.

La risposta a tale quesito richiede l'esame di ben quattro diversi momenti dell'*iter* procedimentale: dall'"universo parallelo" della giustizia preventiva alle dinamiche cautelari, sino alla fase del *sentencing* e a quella dell'esecuzione della pena.

La concreta fattibilità di dette proposte è subordinata alla messa a punto di precise linee guida da adottare nell'*iter* di formazione del *dataset* dei sistemi intelligenti, su cui è opportuna un'attenta riflessione anche al fine di tracciare un sentiero sicuro ove il legislatore nazionale potrebbe agilmente orientarsi.

Infine, ci si occupa dell'ammissibilità di una decisione algoritmica, alla luce degli *standard* di giudizio operanti nel processo penale, coinvolgendo, in particolare, il criterio della "ragionevole previsione di condanna" e quello dell'"oltre ogni ragionevole dubbio".

Partendo dalla problematica relativa alla incerta traducibilità del dato normativo, ci si sofferma sul valore, via via crescente, che sta assumendo il precedente giurisprudenziale, valutando la possibilità di immettere provvedimenti di merito e di legittimità (e non norme) nel *dataset* dell'applicativo algoritmico.

Tuttavia, coscienti delle problematiche emerse oltreoceano − tra opacità dell'algoritmo e *bias* cognitivi −, è certamente opportuno prevedere eventuali correttivi necessari per sopperire alle possibili distorsioni applicative legate all'impiego dell'*AI* in segmenti della decisione penale, non tralasciando i vantaggi legati all'impiego della tecnologia in termini di efficienza, efficacia e celerità dei tempi della giustizia.

Ebbene, affinché sia anche solo ipotizzabile uno scenario di questo tipo è altresì necessario regolamentare due aspetti fondamentali: il controllo umano e la (non) vincolatività della risposta algoritmica.

CAPITOLO I

IL LUNGO CAMMINO VERSO LA REGOLAMENTAZIONE DELL'*AI*

SOMMARIO: 1. Le "promesse" della rivoluzione digitale. 2. L'incerta nozione di intelligenza artificiale. 3. La strategia sovranazionale per la regolamentazione: dalla *soft law*... 4. …all'approvazione dell'*AI Act*. 5. Il cauto atteggiamento del legislatore italiano. 6. Oltre i confini europei (cenni).

1. Le "promesse" della rivoluzione digitale.

Il mito dell'intelligenza artificiale[1] (d'ora in poi, *AI*), in pochi decenni, si è trasformato da racconto fantascientifico a fenomeno reale e consolidato destinato a propagarsi, inarrestabile, nel mondo contemporaneo. Al giorno d'oggi viviamo in «società algoritmiche»[2] dominate da processi decisionali automatizzati[3];

[1] La paternità del concetto è riconosciuta ad Alan Turing il quale, già agli esordi della sua carriera scientifica nel 1936, ha sviluppato idee avanguardistiche che continuano, tuttora, ad influenzare il campo della tecnologia. Al matematico e scienziato britannico dev'essere attribuito il merito di aver introdotto l'idea stessa di "macchina pensante", tradotta nella c.d. macchina di Turing (strumento governato da algoritmi che consentiva di comprendere le modalità di calcolo impiegate per addivenire ad una determinata decisione) nonché di aver coniato il *Turing's Test* (che dimostrava l'impossibilità di distinguere il comportamento umano da quello artificiale). Pertanto, può certamente affermarsi che il suo contributo scientifico ha gettato le basi per la ricerca moderna sull'*AI*; tra i tanti scritti dell'Autore, si veda, TURING, *Computing Machinery and Intelligence*, in *Mind*, LIX, 236, 1 ottobre 1950, pp. 433 ss., nel quale propone di rispondere alla domanda «*can machines think*?» attraverso il c.d. «*imitation game*». Sul punto anche HEAVEN, *Macchine che pensano. La nuova era dell'intelligenza artificiale*, Bari, 2018.
Tuttavia, l'espressione "*artificial intelligent*" è stata utilizzata per la prima volta da John McCarthy, giovane assistente di matematica nel New Hampshire – che nel 1971 ha vinto il premio "Turing" per il contributo apportato alla ricerca − durante il convegno organizzato nel 1956 presso il Dartmouth College insieme ad altri tre ricercatori, Marving Minsky di Harvard, Nathan Rochester della IBM e Claude Shannon dei Bell Telephone Laboratories, avente ad oggetto lo sviluppo di macchine capaci di riprodurre il ragionamento umano. Per ulteriori approfondimenti, MCCARTHY - MINSKY - ROCHESTER - SHANNON, *A proposal for the Dartmouth Summer Research Project on Artificial Intelligent*, *August 31*, 1995, in *27 AI Magazine*, 2006; un estratto del progetto è rinvenibile sul sito https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth.
[2] L'espressione è di BALKIN, *The Three Laws of Robotics in the Age of Big Data*, in *Ohio State Law Journal*, 2017, p. 1219.
[3] In dottrina, senza pretesa di esaustività, si veda, BASILE, *Intelligenza artificiale e responsabilità penale: un'intelligenza tanto "umana" da poter essere punita?*, 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, p. 85, il quale ritiene che «le sue applicazioni pratiche si trovano nelle abitazioni, nelle automobili, negli uffici, nelle banche, negli ospedali, nel cielo e in *internet*, incluso "l'*internet* delle cose"; BODEN, *L'intelligenza artificiale*, Bologna, 2019, p. 3, secondo cui l'intelligenza artificiale è ovunque; CAIANIELLO, *Dangerous Liaisons. Potentialities and Risks Deriving from the Interaction between Artificial Intelligence and Preventive Justice*, in *European journal of crime, criminal law and criminal justice*, 2021, p. 2, afferma che l'*AI*, «*thanks to the Internet of Things, is constantly present in our lives*»; GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, cit., p. 52, prende atto

fallimentare, dunque, si rivelerebbe ogni tentativo di arrestare l'impetuosa avanzata della tecnologia[4].

Il motore di quella che potremmo definire la "quarta rivoluzione industriale" è proprio l'*AI*, che «cerca di avvicinare il funzionamento dei *computer* alle capacità della intelligenza umana» e «usa le simulazioni informatiche per fare ipotesi sui meccanismi utilizzati dalla mente»[5].

Detta catarsi digitale comporta nuove problematiche che coinvolgono il mondo giuridico[6], legate all'impiego di sistemi basati su algoritmi[7]; da qui, l'esigenza di

---

che «negli ultimi lustri, vi è stata un'espansione sensibile dell'IA nella nostra quotidianità: dalle macchine a guida automatica all'uso di *machine learning* nei servizi di implementazione del sistema sanitario, dalla materia assicurativa alle applicazioni industriali, dai dispositivi finalizzati a individuare le truffe *online*, fino agli assistenti domotici come *Google Home* e *Alexa*»; ITALIANO, *Intelligenza Artificiale, che errore lasciarla agli informatici*, in *Agenda digitale online*, 11 giugno 2019, osserva che «le tecnologie di ieri, come ad esempio la TV, la radio, l'elettricità, l'automobile [...] ci hanno concesso tutto il tempo per abituarci alle loro innovazioni, per avere nuove regole sul loro utilizzo, e per organizzare le nostre vite e le nostre società di conseguenza. Oggi, le tecnologie digitali irrompono molto più velocemente, e non ci danno affatto il tempo per organizzarci e per abituarci alle loro dirompenti innovazioni»; UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, cit., p. 9, sostiene che «l'intelligenza artificiale interviene (o può e potrà intervenire) sempre più in quasi ogni nostra attività, senza che noi ne siamo coscienti». In prospettiva comparata, si veda, METZ, *AI Is Trasforming Google Search. The Rest of the Web Is next,* in *Wired online*, 4 febbraio 2016.

[4] Eloquente la risposta del Presidente della Corte Suprema degli Stati Uniti, John Roberts, alla domanda se potesse prevedere il giorno in cui le *smart machines*, guidate da *AI*, potranno assistere il giudice nella ricostruzione del fatto o addirittura intervenire nel processo di *decision-making*: «*it's a day that's here and it's putting a significant strain on how the judiciary goes about doing things*», riportata nell'articolo di LIPTAK, *Sent to Prison by a Software Program's Secret Algorithms*, in *New York Times*, 1 maggio 2017; sul punto, si veda, altresì, KUGLER, *AI Judges and Juries*, in *Communications of the ACM*, 2018, 61, 12, p. 19.

[5] Così, FROSINI, *L'orizzonte giuridico dell'intelligenza artificiale*, in *Diritto dell'Informazione e dell'Informatica (II)*, I, 1 febbraio 2022, p. 6; di diverso parere, KAPLAN, *Intelligenza artificiale. Guida al futuro prossimo*, Roma, 2108, p. 21, secondo cui «ci sono poche ragioni, almeno per il momento, per ritenere che l'intelligenza delle macchine abbia molto in comune con quella umana».

[6] DORIGO, *Presentazione*, in AA.VV., *Il Ragionamento giuridico nell'era dell'intelligenza artificiale*, Dorigo (a cura di), Pisa, 2020, p. XVI, ritiene che la riflessione giuridica – e non il diritto – sia rimasta molto indietro sulla tecnologia e, in particolare, sulle sue origini e sulle implicazioni economiche e sociali che il progresso comporta. Per un quadro di sintesi sulle innovazioni prodotte dall'*AI* nel sistema giustizia, si veda, CASTELLI - PIANA, *Giusto processo e intelligenza artificiale*, Santarcangelo di Romagna, 2019, pp. 73 ss.

[7] Si tratta di un insieme di procedure di risoluzione dei problemi, basate su regole o istruzioni che, se seguite, producono un determinato *output*.

La giurisprudenza statunitense li ha intesi, invece, come procedure per risolvere un certo tipo di problema matematico, cfr. *Gottschalk v. Beson*, 409 US 63 S.Ct 253, 34, L.Ed.2d 273, 175 USPQ 673 (1972).

Secondo la definizione proposta in dottrina da GILLESPIE, *The relevance of Algorithms*, in AA.VV., *Media Technologies. Essays on Communication, Materiality, and* Society, Gillespie - Boczkowski - Foot (*edited by*), Cambridge, 2014, p. 167, «*algorithms need not be software: in the broadest sense, they are encoded procedures for transforming input data into a desired output, based on specified calculations. The procedures name both a problem and the steps by which it should be solved*». Sul

prevedere a tutti i costi una compiuta regolamentazione, avvertita sul fronte sovranazionale e interno, che ha condotto alla frenetica corsa alla legiferazione in cui l'Europa è protagonista[8].

Infatti, stante la loro «relazione complessa e, a tratti, antitetica»[9], è il diritto a dover rincorrere le nuove tecnologie che «con ritmo accelerato» caratterizzano «la dinamica della vita contemporanea trasformando aspetti di diritto penale sostanziale e processuale»[10] importanti, tentando di incanalare su adeguati binari le ricadute sociali e giuridiche che ne derivano[11].

Dunque è compito del giurista contemporaneo misurarsi con tale inedita dimensione della giurisdizione[12], tenendo conto delle potenzialità dell'*AI* e, al contempo, dei rischi che il suo utilizzo comporta[13].

---

punto si veda anche Reichman - Sartor, *Algorithms and Regulation*, in AA.VV., *Constituional Challenges in the Algorithmic Society*, Micklitz - Pollicino - Reichman - Simoncini - Sartor - De Gregorio (*edited by*), Cambridge, 2022, pp. 132 ss.

[8] Cfr., Cap. I, § 3 e 4.

[9] In questi termini si esprime ROMANO, *Diritto, robotica e teoria dei giochi: riflessioni su una sinergia*, in AA.VV., *Diritto e intelligenza artificiale*, Alpa (a cura di), Pisa, 2020, p. 103, secondo cui tra il mondo giuridico e quello digitale vi è «una sorta di osmosi: un flusso di impulsi forniti dalla scienza tecnologica all'ordinamento che, inizialmente con riluttanza e poi con maggior vigore, vengono assorbiti, manipolati e integrati all'interno di un nuovo schema basato su solidi, saldi principi».

[10] Così, FELICIONI, *L'attività valutativa del giudice tra ragione ed emozione*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, Baccari - Felicioni (a cura di), Milano, 2023, p. 3. Sui profili di diritto penale sostanziale, *ex plurimis*, BASILE, *Intelligenza artificiale e responsabilità penale: un'intelligenza tanto "umana" da poter essere punita?*, cit., pp. 85 ss.; BURCHARD, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *Rivista Italiana di Diritto e Procedura Penale*, 2019, pp. 1909 ss.; PICOTTI, *Diritto penale, tecnologie informatiche e intelligenza artificiale: una visione d'insieme*, in AA.VV., *Cybercrime*, Cadoppi - Canestrari - Manna - Papa (diretto da), Milano, 2023, pp. 3 ss.; PIERGALLINI, *Intelligenza artificiale: da "mezzo" a "autore" del reato*, in *Rivista Italiana di Diritto e Procedura Penale*, 2020, pp. 1745 ss.; ROYER - VANLEEUW, *Criminal law and tecnology*, in AA.VV., *Research Handbook on the Law of Artificial Intelligence*, Barfield - Pagallo (*edited by*), Cheltenham, 2018, pp. 190 ss.; SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Rivista Italiana di Diritto e Procedura Penale*, 2021, pp. 83 ss.

[11] In argomento, CALABRESI, *Scienza e diritto: alcune notazioni preliminari*, in AA.VV., *Scienza e diritto nel prisma del diritto comparato. Atti del convegno tenutosi a Pisa il 22-24 maggio 2003*, Comandè - Ponzanelli (a cura di), Torino, 2004, pp. 3 ss.; ROMANO, *Diritto, robotica e teoria dei giochi: riflessioni su una sinergia*, cit., p. 105.

[12] LORUSSO, *La sfida dell'intelligenza artificiale al processo penale nell'era digitale*, in *Sistema penale online*, 28 marzo 2024, p. 1, avverte che «sarebbe illusorio, peraltro, ritenere che l'operato del giurista possa frenare un'onda inarrestabile che ha investito e investe ormai ogni ambito dell'esistenza di ciascuno di noi, che – talora inconsapevolmente – ne viene ad essere condizionato».

[13] DE RENZIS, *Primi passi nel mondo della giustizia «high tech»: la decisione in un corpo a corpo virtuale tra tecnologia e umanità*, in AA.VV., *Decisione robotica*, Carleo (a cura di), Bologna, 2019, p. 139, si pone i seguenti quesiti: «le grandi o piccole dispute saranno affidate al sistema degli algoritmi predittivi? Si potrà parlare di una giustizia del futuro nella quale il diritto diviene perfettamente calcolabile e computabile? E il giudice? E gli avvocati? Scompariranno? Quale sarà la loro sorte?».

Con la presente tesi dottorale, dopo aver analizzato lo stato dell'arte in materia[14] e ricostruito in prospettiva comparata gli usi di *software* algoritmici nei vari contesti processuali, europei ed extraeuropei[15], ci si propone di individuare precisi spazi applicativi per i sistemi di *AI* nei diversi segmenti del procedimento penale, con particolare attenzione alla possibile "automazione" delle dinamiche decisorie[16], non senza tener conto dei rischi e della potenzialità di questa nuova tecnologia.

Tra le "promesse" dell'*AI* vi sono quelle di soluzioni innovative per le tradizionali problematiche che affliggono la giustizia penale[17]. In prospettiva investigativa, oltre ad assicurare una maggiore completezza e celerità della fase procedimentale, si realizzerebbe una efficace riduzione della criminalità con conseguente diminuzione dei reati commessi. In ottica processuale, invece, potrebbe, garantirsi il restringimento dell'alea del giudizio assicurando prevedibilità delle decisioni[18] e certezza del diritto[19]: la consistente diminuzione del tasso di errore giudiziario[20] potrebbe azzerare la c.d. *sentencing disparity*[21].

[14] Si veda *infra*, Cap. I, § 2, 3, 4, 5 e 6.

[15] Sul punto, *infra*, Cap. II.

[16] Cfr., *infra*, Cap. III e IV.

[17] BURCHARD, *L'intelligenza artificiale come fine del diritto penale?*, cit., pp. 1909 ss.; MANES - SANTANGELO, Mechanical judgement: *un processo* in action *di automazione della decisione penale?*, in AA.VV., *La trasformazione digitale della giustizia nel dialogo tra discipline*, Palmirani - Sapienza (a cura di), Milano, 2022, p. 139; in argomento, altresì, COVELLI, *Dall'informatizzazione della giustizia alla «decisione robotica»?*, *Il giudice del merito*, in AA.VV., *Decisione robotica*, cit., p. 126. Per una prospettiva *post* riforma Cartabia, GIALUZ - DELLA TORRE, *Giustizia per nessuno. L'inefficienza del sistema penale italiano tra crisi cronica e riforma Cartabia*, Torino, 2022.

[18] Sul principio di prevedibilità delle decisioni, inteso come espressione più moderna ed europea del principio di legalità, PALAZZO, *Considerazioni minime sulla prevedibilità della decisione giudiziale (tra miti, illusioni, pragmatismi)*, in *Cassazione penale*, 2022, pp. 941 ss. Si veda, altresì, VINCENTI, *Il «problema» del giudice-robot*, in AA.VV., *Decisione robotica*, cit., p. 111, secondo cui «la decisione robotica giudiziale, basata sulla mera relazione tra i dati digitalizzati raccolti, la funzione logico-matematica che li orienta e lo strumento elettronico che li processa, riuscirebbe, dunque, a soddisfare, quasi ineluttabilmente, una duplice, ma combinata esigenza: definire l'istanza che l'ha attivata in un ragionevole e concentrato lasso temporale e assumere essa stessa un rilevante grado di coerenza e prevedibilità».

[19] Da ultimo, in prospettiva critica, ERCOLE, *Contro la "giustizia predittiva". Per una lettura conservativa del principio di certezza del diritto*, Torino, 2024, pp. 1 ss.

[20] Sul tema, BLAIOTTA, *Giustizia, errore, intelligenza artificiale*, in *Sistema penale online*, 23 ottobre 2023, pp. 1 ss.

[21] VASTA, *Diritto dell'Unione Europea e intelligenza artificiale. Riflessi sul procedimento penale*, in *Rivista Italiana di Diritto e Procedura Penale*, 2024, p. 272.

Senza arretrare sull'obiettivo – ostentato dalle recenti riforme − di rendere effettivo il principio della ragionevole durata del processo[22], vi sarebbe anche un netto risparmio di tempi[23] e risorse[24] (anche se, probabilmente, non di costi).

La giustizia italiana potrebbe, dunque, risollevarsi dalla condizione di perenne affanno in cui versa, determinata dalla carenza di mezzi e di personale in rapporto all'elevatissimo numero di procedimenti pendenti nei nostri tribunali, offrendo, al contempo, un prodotto giudiziario più "pulito" e più "giusto"[25].

Con qualche ritocco alla struttura processuale attuale, si potrebbe insomma non rinunciare al potenziale dell'*AI*, salvaguardando, al contempo, le garanzie costituzionali[26].

Ci si pone, dunque, in un'ottica in cui gli algoritmi da "problema" diverrebbero possibile "soluzione", atteggiandosi a correttivo per le distorsioni della giustizia penale.

L'idea sarebbe quella di implementare "sistemi computazionali giuridici", ovvero applicativi pensati e creati *ad hoc* per lavorare negli interstizi della giurisdizione; nel dettaglio si tratterebbe di modelli, da un lato, capaci di incidere nella fase procedimentale e, dall'altro, di coadiuvare il giudice nei diversi momenti decisori, come antidoto all'inadeguatezza della giurisdizione[27].

A tal fine, si dovrebbe sollecitare quella auspicata forma di *reductio ad unum* tra diritto e tecnologia che da tempo si sta cercando di realizzare, attraverso soluzioni

---

[22] COVELLI, *Dall'informatizzazione della giustizia alla «decisione robotica»?*, cit., p. 125, afferma che «non abbiamo un processo efficiente e contenuto nei tempi né nel settore civile, né nel settore penale (nel quale, addirittura, in moltissimi casi, non si riesce a giungere alla definitiva affermazione della innocenza o colpevolezza dell'imputato, e l'esito del giudizio consiste nella declaratoria di prescrizione del reato)».

[23] Sul «fattore tempo», PALESU, *Intelligenza artificiale e giustizia penale. Una lettura attraverso i principi*, in *Archivio penale web*, 2022, p. 6.

[24] In tal senso, LA REGINA, *I.A. e ragionamento giuridico: la giustizia prevedibile*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, cit., p. 168.

[25] Evidenzia l'antitesi tra «*justice as fairness*» e «*justice as fitness*», GARAPON - LASSÈGUE, *La giustizia digitale. Determinismo tecnologico e libertà*, ed. it. a cura di Ferrarese, Bologna, 2021, pp. 237 ss. Estremizzando, CARRATTA, *Decisione robotica e valori del processo*, in *Rivista di diritto processuale*, 2020, pp. 491 ss., si chiede se una decisione esclusivamente robotica possa essere anche giusta.

[26] In argomento, MAFFEO, *Giustizia predittiva e principi costituzionali*, in i-lex. *Scienze Giuridiche, Scienze Cognitive e Intelligenza Artificiale-Rivista quadrimestrale online*, 2019, 12, pp. 277 ss. SACCOMANI, *L'impatto della giustizia algoritmica sul diritto all'equo processo*, in *Cassazione Penale*, 2023, pp. 628 ss.

[27] Su tale profilo, mi sia consentito rinviare ad un precedente scritto, DELLERBA, *La giustizia predittiva come possibile antidoto all'inadeguatezza della giurisdizione*, in *Sistema penale online*, 28 marzo 2024.

strutturate che consentano di rendere reale ed esente da rischi la collaborazione tra macchina e operatore del diritto.

Al contrario, inibire totalmente l'accesso di tali *software* nel procedimento penale significherebbe voler rinunciare ad un certo livello di qualità ed efficienza della giustizia, depurata da personalismi e decisioni emotive.

2. L'incerta nozione di intelligenza artificiale.

Preliminarmente, è necessario comprendere cosa sia effettivamente l'*AI*.

Grazie al continuo e impetuoso progresso tecnologico, si è passati, dal concetto di macchina quale mero calcolatore[28] alle c.d. *machine learning*[29] o *deep learning*[30] ovvero sistemi fondati sul *Knowledge-Based Systems* (*KBS*), che risolvono problemi complessi solitamente affidati ad un soggetto esperto con particolari competenze tecniche[31].

Capaci di interagire con il mondo esterno[32] e di inglobare un numero elevato di informazioni immesse nel sistema (*input*), individuano delle ricorrenze (*pattern*), «caratterizzate da una base statistica molto più solida di quelle che stanno al fondo dei giudizi umani»[33], e offrono una determinata risposta (*output*).

---

[28] Il riferimento è al tradizionale *computer*. Per una definizione in chiave giuridica, si veda, BORRUSO, voce *Informatica Giuridica*, in *Enciclopedia del diritto*, Aggiornamento I, Milano, 1997, pp. 642 ss.

[29] Si tratta di macchine caratterizzate da un insieme di metodi che consentono al *software* di adattarsi ed apprendere per svolgere un compito o una attività, senza che sia stato preventivamente programmato il modo in cui il sistema di *AI* deve comportarsi e/o reagire. In argomento, KAPLAN, *Intelligenza artificiale*, cit., pp. 56 ss. Analizza le diverse tipologie di approcci delle *machine learning*, REICHMAN - SARTOR, *Algorithms and Regulation*, cit., pp. 145 ss.

[30] Si fa riferimento a modelli di apprendimento ispirati alla struttura e al funzionamento della mente umana: operano sulla base di reti neurali che rimandano al modello della nostra rete neurologica e sono dotate di assoni, sinapsi e neuroni che entrano in gioco quando, ricevuto un determinato *input*, si deve generare un certo *output*.

[31] A differenza dei normali *computers* − che operano sulla base di algoritmi e codici stabiliti dal programmatore e modificabili solo attraverso un intervento sul *software* – queste macchine intelligenti analizzano una vasta quantità di dati e ricavano automaticamente algoritmi che poi verranno utilizzati per "prendere decisioni" ed "agire".

[32] Si veda, MAGLIULO, *L'Intelligenza Artificiale nel processo penale: progresso o rischio per la tutela dei diritti costituzionali?*, in *Il Processo*, 2022, p. 561.

[33] Così, 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 online*, 28 maggio 2019, p. 3.

Tali macchine, dunque, partendo da precise informazioni d'ingresso possono ottenere un certo risultato assumendo decisioni autonome e (presumibilmente) imparziali, in base alle finalità[34] per le quali sono state programmate.

Poste queste necessarie premesse, occorre cimentarsi nella ricostruzione degli aspetti definitori.

Non è affatto semplice fornire una nozione giuridica universalmente condivisa dalla comunità scientifica[35], atteso che «lo spettro semantico della locuzione "intelligenza artificiale" e delle sue varie qualificazioni è tanto cangiante quanto controverso»[36].

Tuttavia, è stato autorevolmente sostenuto che «*the idea behind digital computers may be explained by saying that these machines are intended to carry out any operations which could be done by a human computer*»[37].

Pertanto, in linea con il pensiero di Alan Turing, può affermarsi che le macchine intelligenti siano capaci di imitare «il pensiero umano, basato sull'apprendimento e sull'utilizzazione di generalizzazioni, che le persone usano per prendere le decisioni quotidiane»[38].

---

[34] Tra le varie possibili, vi sono l'estrazione (*data mining*), il confronto (*data matching*) o la profilazione (*data profiling*).

[35] Sul punto, si è espressa la Risoluzione del Parlamento europeo del 16 febbraio 2017, cons. C), secondo cui vi è la necessità di «creare una definizione generalmente accettata di *robot* e di intelligenza artificiale che sia flessibile e non ostacoli l'innovazione».
In dottrina, tra i tanti, si veda, ROMANO, *Diritto, robotica e teoria dei giochi: riflessioni su una sinergia,* cit., p. 107, il quale ritiene che la difficoltà preminente nel fornire una definizione sia legata all'ambiguità concettuale della nuova figura di "intelligenza", necessariamente legata al fattore umano, cui oggi si rinuncerebbe; UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, cit., p. 12, secondo cui un «livello minimo di accordo è raggiungibile nel riconoscere quali caratteristiche principali dell'intelligenza artificiale "a) l'uso di grandi quantità di dati e informazioni; b) una elevata capacità logico-computazionale; c) l'uso di nuovi algoritmi, come quelli del *deep learning* e dell'auto-apprendimento, che definiscono metodi per estrarre conoscenza dai dati per dare alle macchine la capacità di prendere decisioni corrette in vari campi di applicazione", senza escludere una modifica degli algoritmi originari»; WEAVER, *Regulation of artificial intelligence in the United States*, in AA.VV., *Research Handbook on the Law of Artificial Intelligence*, cit., p. 156, evidenzia che secondo Stuart Russel e Peter Noving ci son ben otto definizioni di intelligenza artificiale, organizzate in quattro categorie, tra cui "pensare umanamente" e "pensare razionalmente". Si veda, altresì, FLORIDI, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Milano, 2022, p. 40; GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, cit., p. 51; KAPLAN, *Intelligenza artificiale*, cit., 2108, pp. 21 ss.; SIGNORATO, *Giustizia penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo*, in *Rivista di diritto processuale*, 2020, pp. 605-606.

[36] L'espressione è di UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, cit., p. 12.

[37] In tal senso, TURING, *Computing Machinery and Intelligence*, cit., p. 436.

[38] Così, NIEVA-FENOLL, *Intelligenza artificiale e processo*, Torino, 2019, trad. it. a cura di Comoglio, p. 8.

Nella Dichiarazione di Montréal del 2018 si legge testualmente che con l'*AI* «possiamo creare sistemi autonomi in grado di eseguire compiti complessi finora riservati all'intelligenza naturale: elaborare grandi quantità di informazioni, eseguire calcoli e previsioni, apprendere e adeguare le risposte alle situazioni mutevoli, riconoscere e classificare gli oggetti», per cui «data la natura immateriale di questi compiti, e per analogia con l'intelligenza umana, definiamo questi sistemi ad ampio raggio con il termine generico di intelligenza artificiale»[39].

L'Università di Standford l'ha altresì descritta come «*a science and a set of computational technologies that are inspired by - but typically operate quite differently from - the ways people use their nervous systems and bodies to sense, learn, reason, and take action*»[40], configurandola come una macchina che riproduce le capacità cognitive dell'essere umano.

Sulla medesima scia si è posta pure l'Europa che, con fonti di vario rango, a partire dalla Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi del 3 e 4 dicembre 2018[41], alla Comunicazione del 25 aprile 2018 avente ad oggetto "L'intelligenza artificiale per l'Europa"[42], e

---

[39] Dichiarazione di Montréal del 2018, Premessa, consultabile al sito https://montrealdeclaration-responsibleai.com/the-declaration/, che prosegue affermando che «l'intelligenza artificiale rappresenta una forma elevata di progresso scientifico e tecnologico, in grado di generare considerevoli vantaggi sociali, migliorando le condizioni di vita e di salute, agevolando la giustizia, creando ricchezza e mitigando l'impatto delle attività umane sull'ambiente e sul clima. Le macchine intelligenti non si limitano a eseguire i calcoli meglio degli esseri umani, ma sono anche in grado di interagire con esseri senzienti, tener loro compagnia e prendersene cura». Allo stesso tempo, però, riconosce pure che il suo sviluppo «presenta quesiti etici e rischi sociali».

[40] Cfr. STONE - BROOKS - BRYNJOLFSSON - CALO - ETZIONI - HAGER - HIRSCHBERG - KALYANAKRISHNAN - KAMAR - KRAUS - LEYTON - BROWN - PARKES - PRESS - SAXENIAN - SHAH - TAMBE - TELLER, *Artificial Intelligence and life in 2030*, in *One hundred year study on Artificial Intelligence*, Stanford University, 16 settembre 2016, p. 4. L'ultimo studio aggiornato risale al 2021, cfr. STONE - ALTMAN - BRYNJOLFSSON - CONITZER - GRAY - GROSZ - HOWARD - LIANG - LIN - MANYIKA - MCLLRAITH - SONENBERG L. - WAJCMAN J., *Gathering Strenght, Gathering Storms*, in *One hundred year study on Artificial Intelligence*, *Stanford University*, settembre 2021.

[41] Cfr., Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi, adottata il 3 e 4 dicembre 2018, dalla Commissione Europea per l'Efficienza della Giustizia (CEPEJ), istituita dal Consiglio d'Europa, ha definito l'*AI* come l'«insieme di metodi scientifici, teorie e tecniche finalizzate a riprodurre mediante la macchina le capacità cognitive degli esseri umani. Gli attuali sviluppi mirano a far svolgere alle macchine compiti complessi precedentemente svolti da esseri umani» (cfr. Carta etica europea, App. III, Glossario, p. 47, https://rm.coe.int/carta-etica-europea-sull-utilizzo-dell-intelligenza-artificiale-nei-si/1680993348).

[42] Si veda la comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni del 25 aprile 2018, "L'intelligenza artificiale per l'Europa", che l'ha intesa al pari di «sistemi che mostrano un comportamento intelligente, analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi. I sistemi basati sull'IA possono consistere in *software* che agiscono nel mondo virtuale (per esempio assistenti vocali, programmi per l'analisi delle immagini,

sino al Libro bianco sull'intelligenza artificiale del 19 febbraio 2020 su "Un approccio europeo all'eccellenza e alla fiducia"[43], ha provato a fornire (diverse) nozioni.

Da ultimo, il Regolamento 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024, che "stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)", noto come *Artificial Intelligent Act* (c.d. *AI Act*), chiarisce che si tratta di «una famiglia di tecnologie in rapida evoluzione che contribuisce al conseguimento di un'ampia gamma di benefici» e conduce «a risultati vantaggiosi» anche nel settore «giustizia»[44].

Il Regolamento europeo introduce altresì la definizione delle tre "famiglie" di *AI*: predittiva (di «miglioramento delle previsioni»), organizzativa (di «ottimizzazione delle operazioni e dell'assegnazione delle risorse») e sartoriale (di «personalizzazione delle soluzioni digitali»)[45].

Il legislatore precisa altresì che la capacità inferenziale della *machina sapiens* «si riferisce al processo di ottenimento degli *output*, quali previsioni, contenuti, raccomandazioni o decisioni, che possono influenzare gli ambienti fisici e virtuali e alla capacità dei sistemi di IA di ricavare modelli algoritmici, o entrambi, da *input*

---

motori di ricerca, sistemi di riconoscimento vocale e facciale) oppure incorporare l'*AI* dispositivi *hardware* (per esempio in *robot* avanzati, auto a guida autonoma, droni o applicazioni dell'*Internet* delle cose). Utilizziamo l'IA quotidianamente, per esempio per tradurre le lingue, generare sottotitoli nei video o bloccare lo spam delle email. Molte tecnologie di IA richiedono dati per migliorare le loro prestazioni», (cfr. L'intelligenza artificiale per l'Europa, p. 1, fruibile all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52018DC0237).

[43] Si consulti il Libro bianco sull'intelligenza artificiale – "Un approccio europeo all'eccellenza e alla fiducia" del 19 febbraio 2020, che la definisce come un ecosistema e, in particolare, come «insieme di tecnologie che combina dati, algoritmi e potenza di calcolo. I progressi compiuti nell'ambito del calcolo e la crescente disponibilità di dati sono pertanto fattori determinanti per l'attuale crescita dell'IA. L'Europa può combinare i suoi punti di forza industriali e tecnologici con un'infrastruttura digitale di elevata qualità e un quadro normativo basato sui suoi valori fondamentali per diventare un *leader* mondiale nell'innovazione, nell'economia dei dati e nelle sue applicazioni, come indicato nella strategia europea per i dati. Su questa base l'Europa può sviluppare un ecosistema di IA che consenta alla sua società e alla sua economia nel loro complesso di godere dei benefici apportati dalla tecnologia» (cfr. Libro bianco, p. 2, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0065).

[44] Cfr. cons. 4), Reg. UE 2024/1689.

[45] Cfr. cons. 4), Reg. UE 2024/1689.

o dati»; le tecniche di apprendimento automatico[46] consentono di imparare «dai dati come conseguire determinati obiettivi e approcci basati sulla logica», sulla «conoscenza codificata» o sulla «rappresentazione simbolica del compito da risolvere»; «il termine "automatizzato" si riferisce al fatto che il funzionamento dei sistemi di AI prevede l'uso di macchine» che, peraltro, «dispongono di un certo grado di autonomia di azione rispetto al coinvolgimento umano» e di capacità di funzionare senza il suo intervento, mentre l'adattabilità del sistema «si riferisce alle capacità di autoapprendimento»[47], che consente di cambiare durante l'uso.

All'art. 3, n. 1), poi, offre la definizione puntuale di sistema automatizzato che «progettato per funzionare con livelli di autonomia variabili […] può presentare adattabilità dopo la diffusione»; inoltre, «per obiettivi espliciti o impliciti, deduce dall'*input* che riceve come generare *output* quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali»[48].

Tuttavia, la soluzione così congegnata dal legislatore comunitario continua a presentare profili di criticità: sembrerebbe − a meno che non si tratti di una sbavatura linguistica – che il meccanismo di funzionamento dei sistemi intelligenti sia, forse impropriamente, basato su congegni deduttivi (nel testo normativo si utilizza, infatti, l'espressione «deduce»), seguendo modalità di ragionamento che da un *input* di carattere generale conducono ad un *output* di tipo particolare, in cui la conclusione è inevitabile considerata la premessa da cui si parte.

Tutt'altro accadrebbe per gli "algoritmi giuridici", che dovrebbero essere strutturalmente calibrati per seguire un ragionamento di tipo induttivo ovvero quel

---

[46] Ne chiariscono le modalità di funzionamento, LAGIOIA - SARTOR, *Il sistema compas: algoritmi, previsioni, iniquità*, in AA.VV., *XXVI lezioni di diritto dell'intelligenza artificiale*, Ruffolo (a cura di), Bologna, 2019, p. 227: «l'uomo non fornisce alla macchina la conoscenza in base alla quale effettuare la predizione; le fornisce invece un metodo di apprendimento, da applicare ai dati cui la macchina ha accesso, per estrarre automaticamente da quei dati il modello in base al quale effettuare predizioni»; in argomento, si veda, altresì, ROVATTI, *Il processo di apprendimento algoritmico e le applicazioni nel settore legale*, in AA.VV., *XXVI lezioni di diritto dell'intelligenza artificiale*, cit., pp. 31 ss.

[47] Cfr. cons. 12), Reg. UE 2024/1689.

[48] Nella Proposta di Regolamento del Parlamento europeo e del Consiglio che *"*stabilisce regole armonizzate sull'intelligenza artificiale (Leggi sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione" del 21 aprile 2021, invece, il legislatore adottava una nozione a maglie larghe, parlando di «un *software* sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare *output* quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono» (cfr. Proposta di Reg., art. 3, n. 1, disponibile *on line* al seguente *link*: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206).

procedimento logico che consente di risalire dal caso particolare alla regola generale[49], in cui la conclusione è soltanto probabile alla luce delle premesse poste[50].

Quanto, invece, alla categorizzazione degli strumenti di *AI*, potrebbero essere identificate ben quattro macro aree ovvero quella simbolica, non-simbolica, sub-simbolica e ibrida[51], sebbene la distinzione più accreditata sia quella tra *software* ancorati al c.d. *standard* "debole"[52] o "forte"[53], già introdotta dalla citata Carta etica europea[54].

I primi, allo stato non ancora esistenti, sarebbero in grado di comprendere il mondo nella sua interezza e di contestualizzare in modo autonomo i problemi di più varia natura, in assenza del controllo umano; i secondi, gli unici attualmente noti, non godrebbero di una totale autonomia decisionale e sono capaci di eseguire

---

[49] Sulla composizione del *dataset* della macchina e sulla conseguente opportunità che segua un ragionamento induttivo, si veda, *infra*, Cap. IV, § 1.

[50] Segnala, infatti, PALMIRANI, *Interpretabilità, conoscibilità, spiegabilità dei processi decisionali automatizzati*, in AA.VV., *XXVI lezioni di diritto dell'intelligenza artificiale*, cit., p. 68, che «un aspetto interessante che il giurista deve tenere in conto è l'inclusione in questa galassia di algoritmi di modelli non più basati solo su un paradigma logico-deduttivo (*antecedente-conseguente* modello cognitivo molto caro al pensiero giuridico) e deterministico (stessi input, stessi output), ma su modelli predittivi (approssimativi), non-deterministici (i pesi dei nodi di una rete neurale possono cambiare nel tempo in modo continuamente dinamico e non prevedibile) e basati su correlazioni statistiche (anche spurie) che spesso non hanno una spiegazione casale, ma registrano solamente une fenomeno, un fatto, un accadimento il quale deve essere poi interpretato (*interpretability*) nei suoi significati».

[51] Così, PALMIRANI - SAPIENZA - BOMPREZZI, *Il ruolo dell'intelligenza artificiale nel sistema giustizia: funzionalità, metodologie, principi*, in AA.VV., *La trasformazione digitale della giustizia nel dialogo tra discipline*, cit., p. 1; RUSSEL - NORVIG, *Intelligenza artificiale. Un approccio moderno*, 1, 2005, Milano; si veda anche PALMIRANI, *Interpretabilità, conoscibilità, spiegabilità dei processi decisionali automatizzati*, cit., p. 68, secondo la quale l'*AI* simbolica si basa su regole logiche mentre quella sub-simbolica su teorie stocastiche e probabilistiche.

[52] Le *AI* "deboli", definite anche "ristrette" o "moderate" svolgono compiti per raggiungere obiettivi ben definiti. Non godono, quindi, di una vera e propria autonomia decisionale (tutte le possibili soluzioni tra cui l'algoritmo può optare sono già state previste dal programmatore) ma sono in grado di offrire alte prestazioni sulla base di un apprendimento automatico.

[53] Le macchine dotate di sistemi con *standard* "forte" sono capaci di comprendere il mondo nella sua interezza e di risolvere problemi di varia natura in maniera completamente autonoma, in assenza del controllo umano.

[54] Cfr., Carta etica europea, App. III, Glossario, p. 47, secondo cui vi sono *AI* "forti" (capaci di contestualizzare problemi specializzati di varia natura in maniera completamente autonoma) e *AI* "deboli" o "moderate" (alte prestazioni nel loro ambito di addestramento). Alcuni esperti sostengono che quelle "forti", per essere in grado di modellizzare il mondo nella sua interezza, necessiterebbero di progressi significativi della ricerca di base e non soltanto di semplici miglioramenti delle prestazioni dei sistemi esistenti. In dottrina, si veda KAPLAN, *Intelligenza artificiale*, cit., pp. 104-105.

prestazioni complesse esclusivamente nell'ambito in cui sono stati "addestrati", consentendo, così, all'uomo di mantenere il controllo della macchina[55].

Tornando alla complessità delle problematiche legate agli aspetti definitori, deve riferirsi che si è tentato di risolvere la questione rivolgendosi direttamente alla fonte. È stato chiesto a *ChatGPT* di rispondere alla seguente domanda: cos'è l'*AI*?

Il sistema ha affermato che trattasi di «un campo di ricerca e di sviluppo tecnologico che si occupa di creare macchine o sistemi informatici in grado di compiere attività che, se svolte da un essere umano, richiederebbero l'uso dell'intelligenza»; nel dettaglio, secondo l'applicativo generativo, l'*AI* «propone di creare macchine capaci di apprendere, ragionare, risolvere problemi, riconoscere immagini e suoni, parlare e interagire con gli esseri umani in modo simile a quello dei loro simili. Le tecniche utilizzate nell'IA includono il *machine learning*, il *deep learning*, la logica, la visione artificiale, l'elaborazione del linguaggio naturale e molti altri. L'IA viene utilizzata in una vasta gamma di applicazioni come la ricerca scientifica, la robotica, la finanza, la medicina, l'assistenza sanitaria, l'istruzione, il controllo di processo industriale, i giochi e molti altri campi»[56].

Ebbene, proprio alla luce della diffusione di detti sistemi artificiali, come *Open AI* e *ChatGPT*, il legislatore comunitario ha reputato opportuno fornire anche una definizione di *AI* "generativa"[57].

Nella fattispecie, l'*AI Act* offre una nozione di «modello di IA per finalità generali», che rispondono ad una precisa regolamentazione[58], e di «sistema di IA per finalità

---

[55] CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, cit., p. 129.

[56] È quanto riportato da COPPOLA, *Commisurazione della pena e intelligenza artificiale: una ipotesi di lavoro con l'algoritmo Ex-Aequo*, in *Archivio penale web*, 2023, 2, pp. 4-5.

[57] In argomento, BARONE, *Giustizia Predittiva e Certezza del Diritto*, Pisa, 2024, pp. 70 ss.; COSIMI, *Jerry Kaplan sull'AI generativa: "Non preoccupiamoci di cosa farà a noi ma guardiamo a quel che farà per noi"*, in *Wired online*, 31 ottobre 2024.

[58] Al legislatore europeo dev'essere riconosciuto il merito di aver attualizzato i contenuti del regolamento dedicando il Capo V ai "Modelli di ia per finalità generali", la cui utilizzazione è implosa negli ultimi due anni. Nel dettaglio, l'art. 51 offre una classificazione di detti modelli di *AI* per finalità generali con rischio sistemico precisando che: «1. Un modello di IA per finalità generali è classificato come modello di IA per finalità generali con rischio sistemico se soddisfa una delle condizioni seguenti: a) presenta capacità di impatto elevato valutate sulla base di strumenti tecnici e metodologie adeguati, compresi indicatori e parametri di riferimento; b) sulla base di una decisione della Commissione, *ex officio* o a seguito di una segnalazione qualificata del gruppo di esperti scientifici, presenta capacità o un impatto equivalenti a quelli di cui alla lettera a), tenendo conto dei criteri di cui all'allegato XIII. 2. Si presume che un modello di IA per finalità generali abbia capacità di impatto elevato a norma del paragrafo 1, lettera a), quando la quantità cumulativa di calcolo utilizzata per il suo addestramento misurata in operazioni in virgola mobile è superiore a 1025. 3.

generali»: i primi sono addestrati «con grandi quantità di dati utilizzando l'autosupervisione su larga scala» e sono caratterizzati da «una generalità significativa», in base alla quale riescono a «svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle»[59]; i secondi, invece, sono basati «su un modello di IA per finalità generali» e hanno «la capacità di perseguire varie finalità, sia per uso diretto che per integrazione in altri sistemi di IA»[60]. Vi sono, poi, i «grandi modelli di IA generativi» che «consentono una generazione flessibile di contenuti, ad esempio sotto forma di testo, audio, immagini o video, che possono prontamente rispondere a un'ampia gamma di compiti distinti»[61].

Ciò posto, è necessario chiarire a quale modello potrebbe idealmente farsi riferimento nelle dinamiche processuali.

Esula, per ovvie ragioni, dall'indagine *de qua* quell'*AI* "forte" che, lavorando in totale autonomia, pretenderebbe di sostituire il giudice in ogni sua funzione decisoria[62]. Al contrario, si prenderanno in esame esclusivamente i sistemi ancorati ad un paradigma "debole", utilizzabili nelle varie scansioni procedimentali quale mero supporto al magistrato.

3. La strategia sovranazionale per la regolamentazione: dalla *soft law*...

Da anni le istituzioni europee, con varie iniziative legislative, hanno tentato di disciplinare il rapporto tra diritto e *AI*; i provvedimenti adottati, però, hanno sempre assunto valore di fonti di *soft law*, troppo spesso disattese dai singoli Stati membri.

La Commissione adotta atti delegati a norma dell'articolo 97 per modificare le soglie di cui ai paragrafi 1 e 2 del presente articolo, nonché per integrare parametri di riferimento e indicatori alla luce degli sviluppi tecnologici in evoluzione, quali miglioramenti algoritmici o una maggiore efficienza dell'*hardware*, ove necessario, affinché tali soglie riflettano lo stato dell'arte».

[59] Cfr., art. 3, n. 63) e cons. 97), Reg. UE 2024/1689.

[60] Cfr., art. 3, n. 66), Reg. UE 2024/1689.

[61] Cons. 99), Reg. UE 2024/1689.

[62] CANZIO, *AI Act e processo penale: sfide e opportunità*, in *Sistema penale online*, 14 ottobre 2024, p. 1, precisa che «il modello "forte" di IA postula l'automazione del processo decisionale in luogo degli attori della giurisdizione (*machina sapiens*)» e impiega «schemi matematico-statistici nell'esercizio di quella che viene definita giustizia predittiva, indubbiamente inquietante e opaco, e però connotato da un'indubbia forza espansiva, a fronte della crisi di certezza, calcolabilità, uniformità e celerità delle procedure, che promette una risposta pronta e neutra alla domanda di giustizia, perciò deresponsabilizzante per il decisore, con l'ulteriore effetto negativo del conformismo e della sclerotizzazione del formante giurisprudenziale».

Ricostruendo, dunque, il frammentato dato normativo in materia si proverà a comprendere l'*iter* che, a piccoli passi, ha condotto all'approvazione del Regolamento europeo 2024/1689 sull'intelligenza artificiale.

Già in tempi non sospetti, con la Direttiva 2016/680 del Parlamento europeo e del Consiglio (c.d. Direttiva *Law Enforcement*) 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, che abroga la decisione quadro 2008/977/GAI"[63], preso atto che la «rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali»[64], è stata sollecitata la costruzione di un quadro normativo solido e coerente in materia. Ciò in quanto «la libera circolazione dei dati personali tra le autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali, inclusi la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, all'interno dell'Unione e il trasferimento di tali dati personali verso paesi terzi e organizzazioni internazionali, dovrebbe essere agevolata garantendo al tempo stesso un elevato livello di protezione»[65].

Non sono ammesse, dunque, le decisioni assunte unicamente con sistemi automatizzati e prive del fattore umano[66], ivi compresa la profilazione[67], in ragione del diritto dell'interessato a non subire una decisione «basata esclusivamente su un trattamento automatizzato e che produca effetti giuridici negativi nei suoi confronti o incida significativamente sulla sua persona»[68].

---

[63] Si tratta della *lex specialis* in materia di repressione dei reati rispetto al Regolamento 2016/679 sulla protezione dei dati personali del 27 aprile 2016, noto con l'acronimo *GDPR*.
[64] Cons. 3), Dir. UE 2016/680.
[65] Cons. 4), Dir. UE 2016/680.
[66] Sulla medesima lunghezza d'onda si pone l'art. 22 del Reg. UE 2016/679 e l'art. 8, d.lgs. 51/2018, di attuazione della citata Direttiva. Per un quadro sul processo decisionale automatizzato secondo la *GDPR*, si veda, DE FELICE, *Intelligenza artificiale e processi decisionali automatizzati: GDPR ed* ethics by design *come avamposto per la tutela dei diritti umani*, in AA.VV., *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, D'Aloia (a cura di), Milano, 2020, pp. 416 ss.
[67] Art. 11, Dir. UE 2016/680.
[68] Cons. 38), Dir. UE 2016/680.

Con tale divieto, però, che «sembrerebbe in linea col nostro modello legale di motivazione della sentenza»[69], non si inibisce *ex se* l'utilizzo di algoritmi, purché sia garantito l'intervento dell'uomo.

Tale quadro normativo sembrerebbe, quindi, aprire un varco per favorire l'ingresso di meccanismi di *AI* con *standard* "debole".

Nello stesso anno, la Commissione europea sull'efficacia della giustizia del Consiglio d'Europa (*CEPEJ*) − già da diversi anni occupata nella valutazione dell'impatto delle tecnologie dell'informazione e della comunicazione sui sistemi giudiziari − ha compiuto uno studio approfondito sull'uso di tali strumenti nei tribunali europei[70].

Di qualche anno successivo è l'approvazione della menzionata Carta etica europea[71], che poggia sull'importante studio in materia di *Algorithms and Human Right – Study on the human rights dimension of automated data processing techniques and possible regulatory implication*[72], pubblicato nel marzo 2018 dal *Committee of Experts on Internet Intermediaries* del Consiglio d'Europa; non dotata di valore cogente per i Paesi membri, è stata, però, considerata per anni come il principale strumento informativo per esaustività e autorevolezza in materia.

L'eloquente dato normativo, pur ammettendo che l'uso di tali tecnologie nel settore penale debba «essere esaminato con le massime riserve»[73], individua cinque principi irrinunciabili che i sistemi algoritmici devono necessariamente rispettare.

---

[69] MAFFEO, *Giustizia predittiva e principi costituzionali*, cit., p. 278.

[70] Cepej, Studio n. 24, *Rapport thématique: l'utilisation des technologies de l'information par les tribunaux en Europe*, 2016 (dati del 2014).

[71] Per un commento alla normativa, BARBARO, *Uso dell'intelligenza artificiale nei sistemi giudiziari: verso la definizione di principi etici condivisi a livello europeo?*, in *Questione giustizia*, 2018, 4, pp. 189 ss.; BARBARO, *Cepej, adottata la prima Carta etica europea sull'uso dell'intelligenza artificiale (AI) nei sistemi giudiziari*, in *Questione giustizia online*, 7 dicembre 2018; GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., pp. 12 ss.; MAFFEO, *Giustizia predittiva e principi costituzionali*, cit., p. 281; MILIZIA, *Carta etica europea sull'uso dell'intelligenza artificiale nei sistemi giudiziari e loro sviluppo*, in *Il Processo Telematico*, 20 marzo 2019; QUATTROCOLO, *Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi vs rischi e paure della giustizia digitale "predittiva"*, in *Cassazione Penale*, 2019, pp. 1748 ss.; QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *La legislazione penale*, 18 dicembre 2018; UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, cit., pp. 15 ss.

[72] Ne parla anche DONATI, *Intelligenza artificiale e giustizia*, in AA.VV., *Intelligenza artificiale e diritto*, cit., Milano, 2020, p. 262.

[73] Cfr. Carta etica europea, App. I (*Studio approfondito sull'utilizzo dell'intelligenza artificiale [IA] nei sistemi giudiziari, segnatamente delle applicazioni dell'intelligenza artificiale al trattamento di decisioni e dati giudiziari*), § 177 ss.

Irrinunciabile è il controllo da parte dell'utente[74]: da un lato, all'operatore del diritto deve essere garantita «la rivedibilità delle decisioni giudiziarie automatizzate»[75] e, dall'altro, il destinatario della decisione dev'essere informato «delle varie opzioni disponibili, del diritto ad avere un difensore e di quello di far giudicare il caso direttamente da un giudice»[76].

Imprescindibile è altresì il rispetto dei diritti dell'uomo[77]; alla luce della innegabile esistenza di gravi attriti con il diritto alla *privacy*[78] nonché considerata la grande mole di dati raccolti e impiegati nel funzionamento della macchina, è necessario mettere a punto precise procedure di *accountabilty*, volte ad evitare possibili lesioni dei diritti fondamentali[79].

Caposaldo è pure il divieto di discriminazione algoritmica[80]: al fine di sfuggire ai *bias* che potrebbero inficiare la validità del risultato finale dell'algoritmo, è necessario evitare di immettere nel sistema dati spuri. A tal fine, si dovrebbero impiegare procedure matematiche o statistiche appropriate, predisponendo altresì misure volte ad impedire il verificarsi di effetti discriminatori.

Siffatto obiettivo è legato a doppio filo con il principio di qualità e sicurezza dei dati impiegati[81], atteso che l'affidabilità della macchina discende direttamente dalla tipologia degli stessi.

Di fondamentale importanza, quindi, è la scelta del *dataset*, poiché in ossequio al principio socratico "*ex falso sequitur quodlibet*", la cui evoluzione nell'età informatica è costituita dal principio "*garbage in, garbage out*"[82], la macchina riflette inevitabilmente la qualità dei dati immessi o acquisiti autonomamente

---

[74] Cfr. Carta etica europea, p. 12, chiarisce che al destinatario della decisione dev'essere reso noto il «carattere vincolante o meno delle soluzioni proposte dagli strumenti di intelligenza artificiale, delle diverse possibilità disponibili, e del suo diritto a ricevere assistenza legale e di accedere a un tribunale».

[75] In tal senso, UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, cit., p. 16.

[76] UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, cit., p. 17.

[77] Cfr. Carta etica europea, p. 7.

[78] Sul punto, UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, cit., p. 14.

[79] In dottrina, sulla necessità che siano tutelati i diritti fondamentali, UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, cit., pp. 14 ss.

[80] Cfr. Carta etica europea, p. 8.

[81] Cfr. Carta etica europea, p. 10.

[82] In argomento, BARONE, *Intelligenza artificiale e processo penale: la linea dura del Parlamento europeo. Considerazioni a margine della risoluzione del Parlamento europeo del 6 ottobre 2021*, in *Cassazione Penale*, 2022, pp. 1180 ss.

dall'algoritmo, che determina – unitamente all'attendibilità della procedura risolutiva adottata − l'efficienza dell'intero sistema.

In ultimo, vi è il diritto alla trasparenza, all'imparzialità e all'equità delle metodologie usate dall'algoritmo[83], che pone l'accento sulla necessità di rendere accessibili e comprensibili le tecniche di trattamento dei dati utilizzate.

Affinché possa soddisfare l'esigenza di trasparenza del processo di decisione, l'algoritmo deve essere conoscibile, comprensibile e spiegabile[84] sin dalla sua creazione (*by-design*): solo con la certezza che si possa sempre giungere ad una spiegazione del funzionamento del sistema è possibile costruire un sentimento di fiducia, individuale e collettiva, in favore delle emergenti tecnologie.

Pertanto, pare corretto affermare che «tanto a livello di Consiglio d'Europa, quanto a livello di Unione europea» vi sono «una serie di regole che consentono, per un verso, di salvaguardare il ruolo dell'intelligenza umana nei processi decisionali e, per l'altro, di vietare alla radice l'impiego di *tools* che si basino sul trattamento di dati sensibili e che siano suscettibili di condurre a discriminazioni»[85].

Ancora, nel 2019 la Commissione europea ha pubblicato le *Draft Ethics Guidelines for Trustworthy AI*, elaborate dall'*High-Level Expert Group on Artificial*

---

[83] Cfr. Carta etica europea, p. 11.
In dottrina, BARBARO, *Uso dell'intelligenza artificiale nei sistemi giudiziari: verso la definizione di principi etici condivisi a livello europeo?*, cit., p. 195.

[84] Il legislatore unionista ha introdotto tale concetto nell'art. 22 del *GDPR*, che disciplina quei sistemi di *AI* basati su trattamento automatizzato e capaci di incidere sulla persona; ne evidenzia le debolezze, PALMIRANI, *Interpretabilità, conoscibilità, spiegabilità dei processi decisionali automatizzati*, cit., pp. 72 ss.
D'altronde è proprio su tale norma che la giurisprudenza amministrativa fonda le radici dei principi affermati in materia di utilizzabilità di algoritmi nella fase decisionale della Pubblica Amministrazione, cfr. Cons. Stato, sez. VI, 8 aprile 2019, n. 2270, in *Il Foro italiano*, 2019, 11, pp. 606 ss., con nota di CANALINI, *L'algoritmo come "atto amministrativo informatico" e il sindacato del giudice*, in *Giornale di diritto amministrativo*, 2019, pp. 781 ss.; Cons. Stato, sez. VI, 13 dicembre 2019, n. 8472, in *Giornale di diritto amministrativo*, 2020, pp. 366 ss., con nota di MASCOLO, *Gli algoritmi amministrativi: la sfida della comprensibilità*, in *Giurisprudenza italiana*, 2020, pp. 1190 ss.; Cons. Stato, 4 febbraio 2020, n. 881, in *Rivista di diritto processuale*, 2021, pp. 710 ss. con pedissequa nota di DELLA TORRE, *Le decisioni algoritmiche all'esame del Consiglio di Stato*, in *Rivista di diritto processuale*, 2021, pp. 713 ss., che offre una minuziosa analisi delle pronunce dei giudici amministrativi in ordine al tema della c.d. "decisione robotica". Ne analizzano l'attitudine al confronto con la tecnologia, PAJNO - BASSINI - DE GREGORIO - MACCHIA - PATTI - POLLICINO - QUATTROCOLO - SIMEOLI - SIRENA, *AI: profili giuridici. Intelligenza Artficiale: criticità emergenti e sfide per il giurista,* in *BioLaw Journal - Rivista di BioDiritto*, 2019, 3, p. 213.

[85] GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit. p. 19.

Intelligence (*AI HLEG*)[86], mentre il 19 febbraio 2020 è stato approvato il *White Paper On Artificial Intelligence – A European Approach to Excellence and Trust*[87] (corredato da una Relazione[88] e da due Comunicazioni[89]), che evidenzia, fin da subito, l'esigenza di dotarsi di una *AI* affidabile, etica ed antropocentrica[90].

Nel c.d. Libro bianco si evidenzia «l'impatto significativo che l'intelligenza artificiale può avere sulla nostra società e la necessità di creare maggiore fiducia, (per cui) è essenziale che l'IA europea sia fondata sui nostri valori e diritti fondamentali quali la dignità umana e la tutela della *privacy*». Già tra le pagine di questo documento, peraltro, è possibile scorgere la *summa divisio*, soltanto abbozzata, tra sistemi «ad alto rischio» e «non ad alto rischio»[91], che si ritroverà compiutamente elaborata nel Regolamento europeo sull'intelligenza artificiale[92].

Risale, poi, al luglio 2020 lo studio, commissionato dal Comitato LIBE al Parlamento europeo, concernente gli effetti dei sistemi di *AI* di *law enforcement* sui diritti fondamentali[93].

Del medesimo anno è lo Studio di fattibilità del quadro normativo internazionale "sulla concezione, lo sviluppo e l'applicazione dell'*AI*, fondato sulle norme del Consiglio d'Europa in materia di diritti dell'Uomo, democrazia e stato di diritto"[94],

---

[86] Tale gruppo indipendente di ben 52 esperti del settore ha, altresì, elaborato *A Definition of AI. Main Capobilites ad Scientific Disciplines* dell'8 aprile 2019 e la *Policy and Investment Recommendations for Trusworthy AI* del 26 giugno 2019.

[87] Per uno studio più approfondito sulla normativa, si veda, ZANICHELLI, *Ecosistemi, opacità, autonomia: le sfide dell'intelligenza artificiale in alcune proposte recenti della Commissione europea*, in AA. VV., *Intelligenza artificiale e diritto*, cit., pp. 67 ss.

[88] Si tratta del *Report on the Safety and Liability Implications of Artificiale Intelligence, the Internet of Things and Robotics*.

[89] Il riferimento è alla *A European Data Strategy,* che promuove l'economia agile basata sui dati, e alla *Shaping Europe's Digital Future*, che fissa obiettivi e azioni "chiave" da mettere in campo.

[90] In argomento, VASTA, *Diritto dell'Unione Europea e intelligenza artificiale*, cit., pp. 271 ss.; sull'impegno profuso in sede comunitaria per proporre una regolamentazione che promuova la "*Trustworthy AI*", RENDA, *Moral Machine*, in AA.VV., *The Cambridge Handbook of the Law of Algorithms*, cit., pp. 667 ss.

[91] Sul punto, MARINI BALESTRA, *L'intensità della regolazione: la necessità di graduare le regole in funzione di parametri di difformità*, in AA.VV., *Intelligenza artificiale e diritto: una rivoluzione?*, *Diritti fondamentali, dati personali e regolazione*, Pajno - Donati - Perrucci (a cura di), 1, Bologna, 2022, p. 533.

[92] Cfr. *infra*, Cap. I, § 4.

[93] Studio *Artificial intelligence and Law Enforcement − Impact on Fundamental Rights*, luglio 2020, disponibile al seguente sito: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf.

[94] Per un commento, si veda, BARBARO, *Lo studio di fattibilità di un nuovo quadro normativo sulla concezione, lo sviluppo e l'applicazione dei sistemi di Intelligenza Artificiale sulla base delle norme del Consiglio d'Europa. Il lavoro del Comitato ad hoc sull'intelligenza artificiale del Consiglio*

approvato dal Comitato *ad hoc* per l'intelligenza artificiale (CAHAI)[95] il 15-17 dicembre; alla luce della riscontrata frammentarietà della materia e dell'esistenza di lacune normative, si rendeva necessaria la creazione di un quadro giuridico internazionale vincolante a cui fare riferimento. Da un lato, si voleva creare uno strumento normativo orizzontale – come una Convenzione, una Convenzione quadro o un Trattato − per consolidare i principi comuni generali in materia; dall'altro, prevedere ulteriori strumenti vincolanti e non vincolanti per affrontare le sfide proposte dall'*AI* in settori peculiari come quello della giustizia[96].

Detti obiettivi sono stati raggiunti con la sottoscrizione a Vilnius (Lituania) del *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*[97] il 5 settembre 2024, che costituisce il primo strumento internazionale giuridicamente vincolante sull'*AI*, ponendosi in linea con il Regolamento europeo 2024/1689[98].

Facendo, però, un passo indietro, deve darsi atto che nel sin qui tracciato contesto "para-normativo", antecedente ai recenti approdi regolatori del Consiglio d'Europa e dell'Unione europea, il 6 ottobre 2021, il Parlamento europeo ha adottato la Risoluzione sull'intelligenza artificiale nel diritto penale e sul suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale[99].

Il documento, al punto 8, «sottolinea che l'uso di applicazioni basate sull'intelligenza artificiale come l'apprendimento automatico, compresi gli

---

d'Europa (CAHAI), in *Questione giustizia online*, 28 aprile 2021, che prevedeva, tra le possibili opzioni, quella di mettere a punto un trattato internazionale.

[95] Istituito dal Consiglio d'Europa, si compone di 47 Stati membri, 6 Stati osservatori e 72 fra rappresentanti di comitati, di istituzioni del Consiglio d'Europa, della società civile, del settore scientifico, del partenariato digitale del Consiglio d'Europa.

[96] Tale *modus procedendi* è stato condiviso dall'Assemblea parlamentare del Consiglio d'Europa, che ha invitato il Consiglio dei Ministri a predisporre una Convenzione del Consiglio d'Europa sulla materia.

[97] Tra i firmatari, oltre alla Commissione europea, ci sono l'Andorra, la Georgia, l'Islanda, la Norvegia, la Repubblica di Moldova, la Repubblica di San Marino, il Regno Unito, Israele e gli Stati Uniti d'America. La Convenzione quadro prescrive agli Stati di adottare normative interne sull'*AI* che assicurino il rispetto dei principi di dignità umana e libertà individuale (art. 7), trasparenza e supervisione (art. 8), responsabilità (art. 9), equità e non discriminazione (art. 10), *privacy* e protezione dei dati personali (art. 11) nonché affidabilità dei sistemi (art. 12), imponendo altresì la previsione di efficaci rimedi contro eventuali compressioni dei diritti individuali dell'uomo.
Per un primissimo commento, si veda, NIOLA, *IA, ecco il primo trattato internazionale: la Convenzione del Consiglio d'Europa*, in *Agenda digitale online*, 6 settembre 2024. Sul punto anche BARONE, *Giustizia Predittiva e Certezza del Diritto*, cit., pp. 30 ss.; CANZIO, *AI Act e processo penale: sfide e opportunità*, in *Sistema penale online*, 14 ottobre 2024, p. 3;

[98] Su cui *infra*, § 4.

[99] Per un commento, si veda, MANES - SANTANGELO, Mechanical judgement, cit., pp. 151 ss.

algoritmi sui quali sono basate tali applicazioni, potrebbe comportare distorsioni e discriminazioni»; detti risultati patologici possono essere intrinsechi «agli insiemi di dati di base, specie se si utilizzano dati storici, inseriti dagli sviluppatori degli algoritmi o generati quando i sistemi sono attuati in contesti reali»; ciò accade poiché «il risultato fornito dalle applicazioni di IA è necessariamente influenzato dalla qualità dei dati utilizzati», che sono astrattamente idonee a «perpetuare e amplificare le discriminazioni esistenti, in particolare nei confronti delle persone che appartengono a determinate minoranze etniche o comunità razziali».

Avvertita, dunque, l'esigenza di addivenire ad una precisa regolamentazione settoriale ci si è interrogati sulle modalità con le quali procedere; se in un primo momento la Commissione europea si è mostrata propensa alla modifica degli atti già in vigore[100], il Parlamento, poi, ha ritenuto opportuno creare un nuovo atto normativo *ad hoc*, che disciplini in maniera generale e organica la materia[101].

Da qui, la grande svolta avvenuta con la Proposta di Regolamento sull'intelligenza artificiale del 21 aprile 2021[102]. Atteggiandosi a «crocevia legislativo fondamentale nella regolamentazione dei sistemi AI in settori critici, compreso quello della giustizia»[103], ha costituito la base di lavoro per l'approvazione dell'agognato *AI Act*.

---

[100] Cfr. Libro bianco, p. 15, «la Commissione ritiene che il quadro legislativo possa essere migliorato per affrontare le situazioni e i rischi descritti di seguito […]».

[101] Evidenzia le difficoltà relative alla creazione di un quadro giuridico uniforme in materia di *AI*, ADINOLFI, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, in AA.VV., *Intelligenza artificiale e diritto: una rivoluzione?*, *Diritti fondamentali, dati personali e regolazione*, cit., p. 128: «l'azione normativa si muove, infatti, lungo un crinale assai stretto, i cui limiti sono, da un lato, il rafforzamento del ruolo dell'Unione nella competizione globale relativa alle tecnologie innovative e, dall'altro, l'esigenza di assicurare il rispetto dei valori europei, che costituiscono il perimetro entro il quale qualsiasi applicazione tecnologica deve collocarsi».

[102] Per un commento alla proposta, si veda, CASONATO - MARCHETTI, *Prime osservazioni sulla proposta di Regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal - Rivista di BioDiritto*, 2021, pp. 415 ss.; CONTISSA - GALLI - GODANO - SARTOR, *La nuova Proposta di Regolamento europeo sull'intelligenza artificiale: questioni giuridiche e approcci regolatori*, in AA.VV., *Nuove questioni di informatica forense*, Brighi (a cura di), Roma, 2022, pp. 387 ss.; DONATI, *Diritti fondamentali e algoritmi nella proposta di regolamento sull'intelligenza artificiale*, in AA.VV., *Intelligenza artificiale e diritto: una rivoluzione?*, *Diritti fondamentali, dati personali e regolazione*, *Diritti fondamentali, dati personali e regolazione*, cit., pp. 111 ss.; KOULU - SANKARI - HIRVONEN - HEIKKINEN, *Artificial intelligence and the law: can we and should we regulate Ai system?*, in AA.VV., *The Cambridge Handbook of the Law of Algorithms*, cit., pp. 427 ss.; LA VATTIATA, *Brevi note «a caldo» sulla recente Proposta di Regolamento Ue in tema di intelligenza artificiale*, in *Diritto penale e uomo online*, 2021, p. 1 ss.; MARINI BALESTRA, *L'intensità della regolazione*, cit., pp. 534 ss.

[103] BOMPREZZI - SAPIENZA, Algorithmic justice *e classificazione di rischio nella proposta* AI Act, in AA.VV., *La trasformazione digitale della giustizia nel dialogo tra discipline*, cit., p. 66.

A differenza della normativa adottata dalla Cina e dagli Stati Uniti[104], quella europea si caratterizza per l'approccio umano-centrico e per aver catalogato gli strumenti di *AI* in fasce di rischio[105], tecnica già sperimentata in materia di *privacy*. Già nei lavori preparatori, infatti, si delineava la costruzione della c.d. "piramide dei rischi". Sono state altresì gettate le basi delle pratiche di *data governance* e di gestione[106] dei *software*: affinché siano utilizzabili detti applicativi, infatti, devono rispondere a precisi criteri, dimostrandosi pertinenti, rappresentativi, esenti da errori, completi nonché statisticamente appropriati.

L'impalcatura della proposta già prevedeva adempimenti a carico dei *provider* che, prima dell'immissione sul mercato della macchina, devono rendere nota la documentazione tecnica del *software* affinché si possa verificare l'aderenza del sistema ai requisiti di conformità[107] di cui all'art. 19 della Proposta, agevolando così il controllo da parte delle autorità competenti[108].

Ancora, si profilava come irrinunciabile il controllo umano; nonostante l'espressa dichiarazione d'intenti, però, non è stata individuata – neppure nella versione definitiva del Regolamento − una precisa modalità attraverso la quale garantirlo[109].

---

[104] Sul punto, *infra*, § 6.

[105] Sull'approccio *risk-based* già sperimentato in materia di *privacy*, BOMPREZZI - SAPIENZA, Algorithmic justice *e classificazione di rischio nella proposta* AI Act, cit. pp. 65 ss.; MANES - SANTANGELO, Mechanical judgement, cit., pp. 148 ss.; in senso critico, FINOCCHIARO, *La Proposta di regolamento sull'intelligenza artificiale: il modello europeo bastato sulla gestione del rischio*, in *Diritto dell'Informazione e dell'Informatica (II)*, 2, 1 aprile 2022, pp. 303 ss.; ODDENINO, *Intelligenza artificiale e tutela dei diritti fondamentali: alcune notazioni critiche sulla recente Proposta di Regolamento della UE, con particolare riferimento all'approccio basato sul rischio e al pericolo di discriminazione algoritmica*, in AA.VV., *Intelligenza artificiale e diritto: una rivoluzione?*, *Diritti fondamentali, dati personali e regolazione*, cit., pp. 165 ss.

[106] In argomento, BOMPREZZI - SAPIENZA, Algorithmic justice *e classificazione di rischio nella proposta* AI Act, cit., pp. 84 ss.

[107] Il riferimento è all'art. 19 della Proposta di Reg.: «1. I fornitori dei sistemi di IA ad alto rischio garantiscono che il sistema di IA ad alto rischio sia sottoposto alla pertinente procedura di valutazione della conformità di cui all'articolo 43 prima della sua immissione sul mercato o messa in servizio. Se in seguito a tale valutazione i sistemi di IA risultano conformi ai requisiti di cui al capo 2 del presente titolo, i fornitori redigono una dichiarazione di conformità UE a norma dell'articolo 48 e appongono la marcatura CE di conformità a norma dell'articolo 49. 2. Per i sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettera b), immessi sul mercato o messi in servizio da fornitori che sono enti creditizi disciplinati dalla direttiva 2013/36/UE, la valutazione della conformità è effettuata nell'ambito della procedura di cui agli articoli da 97 a 101 di tale direttiva». La procedura da seguire poi era dettata dall'art 43, che identificava la conformità ad uno degli *standard* di cui all'art. 40. Il meccanismo era di tipo presuntivo, come stabilito dall'art. 42.

[108] Cfr. art. 11, Proposta di Reg.

[109] Tra i vari modelli di monitoraggio vi sono lo *human-in-the-loop* (HITL o a supervisione umana), lo *human-on-the-loop* (HOTL o a intervento umano) e lo *human-in-command* (UIC o a controllo umano); sul punto, BOMPREZZI - SAPIENZA, Algorithmic justice *e classificazione di rischio nella proposta* AI Act, cit., p. 88.

Smussandone le imperfezioni e adeguandone la struttura ai nuovi approdi della tecnologica, si è così giunti all'approvazione del bramato *AI Act*.

4. … all'approvazione dell'*AI Act.*

Il Regolamento europeo 2024/1689 sull'intelligenza artificiale del Parlamento europeo e del Consiglio, approvato il 13 giugno 2024, costruito in maniera «certamente non breve e puntigliosamente dettagliato»[110], interviene sullo stratificato panorama normativo al fine di adottare un *legal framework* uniforme.

Infatti, lo scopo del legislatore comunitario, già anticipato nel primo *desiderata* è quello di regolamentare le quattro fasi (sviluppo, immissione sul mercato, messa in servizio e uso) dei sistemi di *AI* in conformità ai valori dell'Unione[111].

Sulla medesima lunghezza d'onda si pone l'art. 1 che, riportando quasi pedissequamente il contenuto di detto considerando, chiarisce l'oggetto del Regolamento, ponendo come obiettivi da raggiungere «migliorare il funzionamento del mercato interno», promuovere la «diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile», garantire «un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione Europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA» e assicurare l'«innovazione»[112] tecnologica.

Considerato che l'*AI* può essere usata in un'ampia gamma di settori dell'economia e della società, è opportuno adottare «obblighi uniformi» per «garantire un livello di protezione costante ed elevato in tutta l'Unione»[113], mettendo in guardia i legislatori nazionali affinché non adottino normative difformi dal Regolamento, che determinerebbero una frammentazione del mercato interno con grave rischio per la certezza del diritto.

Dunque, la finalità è quella di rendere l'Europa «*leader* nell'adozione di un'IA affidabile»[114], pur mantenendo ben saldi i principi su cui è fondata.

---

[110] Così, CANZIO, *AI Act e processo penale: sfide e opportunità*, cit., p. 3, che offre un primo commento al Regolamento.
[111] Cfr. cons. 1), Reg. UE 2024/1689.
[112] Si veda, art. 1, Reg. UE 2024/1689.
[113] Cfr. cons. 3), Reg. UE 2024/1689.
[114] Cfr. cons. 2), Reg. UE 2024/1689.

Per cui, cosciente dei possibili rischi e degli eventuali pregiudizi che sarebbero arrecati agli interessi pubblici e ai diritti fondamentali[115], l'Unione si è dotata di una disciplina organica al fine di garantire un impiego sano di detti sistemi, provando a limitarne le possibili distorsioni[116].

Lo schema legislativo adottato dal Regolamento si basa sulla tecnica normativa del rinvio esterno: il primo è quello alla Carta dei Diritti Fondamentali dell'UE; poi, vi è il riferimento alla Dichiarazione europea sui diritti, ai Principi digitali per il decennio digitale e gli Orientamenti etici per un'IA affidabile del gruppo di esperti ad alto livello sull'intelligenza artificiale (*AI HLEG*)[117], oltre al Regolamento sulla *privacy*.

Adottando un «approccio basato sul rischio»[118], si è, infatti, posto in linea con la struttura normativa del *GDPR*.

---

[115] Cfr. cons. 5), Reg. UE 2024/1689; l'elenco dei diritti da proteggere è contenuto nel cons. 48): «il diritto alla dignità umana, il rispetto della vita privata e della vita familiare, la protezione dei dati personali, la libertà di espressione e di informazione, la libertà di riunione e di associazione e il diritto alla non discriminazione, il diritto all'istruzione, la protezione dei consumatori, i diritti dei lavoratori, i diritti delle persone con disabilità, l'uguaglianza di genere, i diritti di proprietà intellettuale, il diritto a un ricorso effettivo e a un giudice imparziale, i diritti della difesa e la presunzione di innocenza e il diritto a una buona amministrazione».
Considerata la necessità di garantire un alto livello di protezione dei dati personali, l'art. 59 detta precisi vincoli per l'«ulteriore trattamento dei dati personali per lo sviluppo nello spazio di sperimentazione normativa per l'IA di determinati sistemi di IA nell'interesse pubblico», prevedendo, al § 2, che «a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse, sotto il controllo e la responsabilità delle autorità di contrasto, il trattamento dei dati personali negli spazi di sperimentazione normativa per l'IA si basa su una specifica disposizione di diritto nazionale o dell'Unione ed è soggetto alle stesse condizioni cumulative di cui al paragrafo 1».

[116] Il legislatore europeo è consapevole che «l'IA presenta accanto a molti utilizzi benefici, la possibilità di essere utilizzata impropriamente e di fornire strumenti nuovi e potenti per pratiche di manipolazione, sfruttamento e controllo sociale. Tali pratiche sono particolarmente dannose e abusive e dovrebbero essere vietate poiché sono contrarie ai valori dell'Unione relativi al rispetto della dignità umana, alla libertà, all'uguaglianza alla democrazia e allo Stato di diritto e ai diritti fondamentali sanciti nella Carta, compresi il diritto alla non discriminazione, alla protezione dei dati e alla vita privata e i diritti dei minori» (cons. 28), Reg. UE 2024/1689).

[117] Cfr. cons. 7), Reg. UE 2024/1689; l'*AI HLEG* ha elaborato sette principi etici non vincolanti: «intervento e sorveglianza umani, robustezza tecnica e sicurezza, vita privata e *governance* dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale e responsabilità» (v. cons. 27).
In dottrina, sulla relazione tra etica e *AI*, DALY - HAGENDORFF - MANN - MARDA - WAGNER - WEI WANG, *AI, Governance and Ethics. Global Perspective*, in AA.VV., *Constitutional Challenges in the Algorithmic Society*, Micklitz - Pollicino - Reichman - Simoncini - Sartor - De Gregorio (*edited by*), Cambridge, 2022, pp. 182 ss.

[118] Cfr. cons. 26), Reg. UE 2024/1689.

Al vertice della piramide vi sono le «pratiche di IA inaccettabili»[119] e, dunque, vietate; seguono i «sistemi di IA ad alto rischio»[120], per i quali è necessario stabilire «requisiti obbligatori»[121]; in ultimo, gli apparati privi di rischio, ammessi di *default*, i quali devono, comunque, rispettare «obblighi di trasparenza»[122].

Si è deciso di trattare con cautela i c.d. *risk assessment tools* e, più in generale, gli algoritmi utilizzabili nell'amministrazione della giustizia penale[123], poiché, al pari dei sistemi applicabili dalle autorità di contrasto[124], potrebbero ledere «il diritto alla dignità e alla non discriminazione e i valori di uguaglianza e giustizia»[125].

Tuttavia, pur riconducendoli alla disciplina delle c.d. «pratiche di AI vietate» *ex* art. 5 dell'*AI Act*, ne è ammesso l'impiego unicamente «a sostegno della valutazione umana del coinvolgimento di una persona in un'attività criminosa, che si basa già su fatti oggettivi e verificabili»[126] direttamente connessi al fatto illecito, purché sia compiuta un'attenta analisi del rischio[127].

---

[119] Cfr. cons. 26), Reg. UE 2024/1689; sono, infatti, vietate le seguenti pratiche: manipolazione, sfruttamento e controllo sociale (v. cons. 28); orientamento subdolo verso una decisione che aggira la libera scelta umana (v. cons. 29); categorizzazione biometrica (v. cons. 30); attribuzione di un punteggio sociale alle persone fisiche (v. cons. 31); identificazione biometrica in tempo reale (v. cons. 32), con le eccezioni di cui ai cons. 33), 34), 35), 36), 37), 38) e 39); profilazione per determinare la futura commissione di un reato non ancora consumato (v. cons. 42); ampliazione delle banche dati biometriche (v. cons. 43); l'identificazione di emozioni o intenzioni (v. cons. 44). Si veda altresì art. 5, rubricato «pratiche di IA vietate» e All. II, che fornisce l'«elenco dei reati di cui all'articolo 5, paragrafo 1, primo comma, lettera h), punto iii)».

[120] Cfr. cons. 26), Reg. UE 2024/1689. Il legislatore europeo fornisce altresì una classificazione di sistemi "ad alto rischio", mettendo a punto un'articolata strategia di *compliance*, all'art. 6, rubricato «regole di classificazione per i sistemi di IA ad alto rischio», che rinvia pure all'All. III su «sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2», modificabile dalla Commissione con successivi atti delegati (art. 7).

[121] Cfr. cons. 46), Reg. UE 2024/1689, secondo cui è altresì «opportuno limitare i sistemi di IA identificati come ad alto rischio a quelli che hanno un impatto nocivo significativo sulla salute, la sicurezza e i diritti fondamentali delle persone nell'Unione, e tale limitazione dovrebbe ridurre al minimo eventuali potenziali restrizioni al commercio internazionale». Tra questi vi è la necessità che sia redatta, prima dell'immissione sul mercato, la documentazione tecnica ai sensi dell'art. 11 e che sia consentita la conservazione dei dati di *log ex* art. 12.

[122] Cfr. cons. 26), 71) e 72), Reg. UE 2024/1689.

[123] Cfr. cons. 61), Reg. UE 2024/1689.

[124] Cfr. cons. 59), Reg. UE 2024/1689.

[125] Cfr. cons. 31), Reg. UE 2024/1689.
In dottrina, sul rispetto della dignità umana quale minimo comun denominatore di ogni decisione, SIGNORATO, *Il diritto a decisioni penali non basate esclusivamente su trattamenti automatizzati: un nuovo diritto derivante dal rispetto della dignità umana*, in *Rivista di diritto processuale*, 2021, pp. 101 ss.

[126] Art. 5, comma 2, lett. d), Reg. UE 2024/1689.

[127] Cfr. cons. 52), 53), 54) e 65) Reg. UE 2024/1689; la *check list* degli adempimenti necessari è fornita dal cons. 66): 1. gestione dei rischi; 2. la qualità e la pertinenza dei set di dati utilizzati; 3. la documentazione tecnica; 4. la conservazione delle registrazioni; 5. la trasparenza e la fornitura di

Ciò in quanto, è evidente che l'indagato/imputato non può essere giudicato esclusivamente sulla base di un comportamento previsto come tale dall'*AI*, che si basa «sulla profilazione, sui tratti della personalità o su caratteristiche quali la cittadinanza, il luogo di nascita, il luogo di residenza, il numero dei figli, il livello di indebitamento o il tipo di automobile»[128], senza che vi sia un ragionevole sospetto che la persona sia coinvolta in affari illeciti che, in quanto tali, sono già stati accertati da un giudice.

Così, anche a livello europeo, viene attribuito alla macchina un ruolo ancillare e subalterno, mantenendo salda l'indipendenza del giudice che resta *dominus* dell'intero *iter* procedimentale.

D'altronde, fulcro della normativa europea è il concetto di «tecnologia antropocentrica»[129]: la supervisione umana è assolutamente necessaria in considerazione dell'impatto significativo che l'*AI* potrebbe avere sulla società e sull'intero mondo giuridico[130].

Anche secondo l'*Ethics Guidelines for Trustworthy Artificial Intelligent*[131] elaborati da un gruppo di esperti di alto livello del settore (*AI HLEG*), richiamate nel Regolamento, è opportuno preservare l'intervento umano.

Infatti, da un lato, i sistemi devono essere «sviluppati e utilizzati come strumenti al servizio delle persone, nel rispetto della dignità umana e dell'autonomia personale» e, dall'altro lato, occorre che funzionino «in modo da poter essere adeguatamente controllati e sorvegliati dagli esseri umani»[132].

---

informazioni ai *deployer*; 6. la sorveglianza umana e la robustezza; 7. l'accuratezza e la cyber-sicurezza.

[128] Cfr. cons. 42), Reg. UE 2024/1689.

[129] Cfr. cons. 6), Reg. UE 2024/1689, che la considera come «prerequisito» dell'intelligenza artificiale; il legislatore dedica, inoltre, l'intero art. 14 alla «sorveglianza umana».

[130] Cfr. cons. 73), Reg. UE 2024/1689.

[131] Per un commento sugli orientamenti etici, CASTETS - RENARD, *Human Rights and Algorithmic Impact Assesment for Predictive Policing*, in AA.VV., *Constituional Challenges in the Algorithmic Society*, cit., pp. 103 ss.

[132] Cfr. cons. 27), Reg. UE 2024/1689.

Affinché tale proposito sia realizzato è opportuno agevolare «l'alfabetizzazione»[133] in materia di *AI*, consentendo ai fornitori[134], ai *deployer*[135] e ai soggetti interessati di poter utilizzare al meglio i modelli computazionali, possedendo, così, le «nozioni necessarie per prendere decisioni informate»[136].

Infatti, com'è stato autorevolmente sostenuto, «quello che è veramente inquietante non è che il mondo si trasformi in un completo dominio della tecnica. Di gran lunga più inquietante è che l'uomo non è affatto preparato a questo radicale mutamento del mondo»[137].

Insomma, si è cercato di «assicurare che l'utile arricchimento delle fonti normative del giudice e le predizioni del modello statistico-matematico si coniughino sempre con il nucleo epistemologico tradizionale delle garanzie del giusto processo» e rispondano «a criteri di specifica responsabilità dell'uomo»[138].

Ciò in considerazione del fatto che gli algoritmi possono sfruttare «le vulnerabilità di una persona o di uno specifico gruppo di persone dovute all'età, a disabilità ai sensi della direttiva (UE) 2019/882 del Parlamento europeo e del Consiglio o a una specifica situazione sociale o economica», esponendo al rischio coloro che «vivono in condizioni di povertà estrema e le minoranze etniche o religiose»[139].

Per evitare di incorrere in tali *bias* è dunque necessario agire su due fronti.

Per un verso, escludere dal sistema le informazioni viziate basate su fattori quali la razza, le opinioni politiche, il contesto sociale di provenienza, l'orientamento sessuale e il genere[140]; per altro verso, includere nello sviluppo e nell'utilizzo di detti sistemi soggetti diversi con l'obiettivo di promuovere la parità di accesso,

---

[133] Cfr. artt. 3, n. 56), e 4; si veda pure, cons. 20), Reg. UE 2024/1689.

[134] L'art. 3, n. 3), Reg. UE 2024/1689, chiarisce che si tratta di «una persona fisica o giuridica un'autorità pubblica un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito».

[135] È definito dall'art. 3, n. 4), Reg. UE 2024/1689, come una «persona fisica o giuridica, un'autorità pubblica un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale»; si tratta, dunque, dell'utilizzatore finale professionale, sebbene sia ammissibile anche l'uso da parte di «persone diverse dal *deployer*» (cfr. anche cons. 13).

[136] Cons. 20), Reg. UE 2024/1689.

[137] Così, HEIDEGGER, *L'abbandono*, trad. it. a cura di Fabris, Genova, 1995, p. 36.

[138] CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale*, cit., p. 129.

[139] Cfr. cons. 29), Reg. UE 2024/1689.

[140] Cfr. art. 10, Reg. UE 2024/1689 su «dati e *governance* dei dati», dedicati ai dati di convalida, addestramento e prova.

l'uguaglianza di genere e culturale, azzerando gli effetti discriminatori e/o pregiudizievoli[141].

Dunque, la "pulizia" del *dataset* è fondamentale al fine di garantire l'immissione di informazioni di qualità e accessibili: «i dati di addestramento, convalida e prova» devono essere «pertinenti […], esenti da errori e completi»[142].

Infatti, dotando i *tools* di *training* coerenti e privi di elementi discriminatori l'*output* sarebbe, con ogni probabilità, preciso ed imparziale, anche rispetto alle decisioni umane troppo spesso contaminate dall'emotività[143].

Così, addirittura, l'affidabilità dell'algoritmo predittivo potrebbe superare quella umana, garantendo, in termini concreti, certezza e prevedibilità del diritto, senza rinunciare alla garanzia di terzietà e imparzialità del decisore[144].

Per salvaguardare il «diritto fondamentale alla protezione dei dati personali»[145] in tutto il ciclo di vita dei sistemi intelligenti[146], il Regolamento si pone in un'ottica di coordinamento rispetto alla disciplina in materia di *privacy* già vigente[147], imponendo precisi obblighi per i fornitori, per i *deployer* e per le altre parti, che si intensificano per l'*AI* ad alto rischio[148].

---

[141] Cfr. cons. 27), Reg. UE 2024/1689.

[142] Cfr. cons. 67), Reg. UE 2024/1689.

[143] Sul tema, ampiamente, FELICIONI, *L'attività valutativa del giudice tra ragione ed emozione*, cit., pp. 3 ss.; FORZA - MENEGONI - RUMIATI, *Il giudice emotivo. La decisione tra ragione ed emozione*, Bologna, 2017.

[144] Sull'affidabilità dell'algoritmo e sulla possibilità che l'*output* generato sia utilizzato dalle giurie nei sistemi di *common law* come "opinione di un esperto", KARNOW, *The Opinion of Machine*, in AA.VV., *The Cambridge Handbook of the Law of Alorithms*, cit., pp. 16 ss.

[145] Cfr. cons. 10), Reg. UE 2024/1689.

[146] Cfr. cons. 69), Reg. UE 2024/1689.

[147] Il riferimento è alla seguente normativa: Reg. UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati); Reg. UE 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il Regolamento CE 45/2001 e la decisione 1247/2002/CE; Dir. 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; Dir. 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

[148] Cfr. artt. 16 ss., Reg. UE 2024/1689.

Fin dalla loro progettazione i sistemi di *AI* devono, quindi, rispettare determinati codici di condotta.

Affinché ne sia assicurata l'accuratezza, la robustezza tecnica e la sicurezza[149], l'algoritmo deve essere trasparente, tracciabile e spiegabile, in modo tale da rendere l'utilizzatore consapevole delle metodologie usate e delle tecniche di trattamento impiegate[150].

Ciò in quanto l'opacità di funzionamento dei sistemi intelligenti, sottendendo quella che viene definitiva una *black box decision*[151], si renderebbe incompatibile con l'idea stessa di *fair trail*, collidendo con il «diritto alla motivazione»[152] e con quello al confronto nonché con il principio di parità delle armi.

Al fine di salvaguardare le garanzie difensive è stato messo a punto un sistema di valutazione dell'applicativo: da un lato, si è previsto un dialogo binario con il Comitato europeo per la protezione dei dati e con le autorità nazionali e, dall'altro, si è istituito un meccanismo di certificazione *ex ante*, che consente di validare il funzionamento del sistema con una omologazione autoritativa da parte delle istituzioni competenti.

Tale soluzione, seppur dai confini ancora nebulosi circa la concreta identità di coloro i quali saranno effettivamente deputati al controllo, pare essere l'unica strada in grado di assicurare una corretta programmazione dei *software*, atteso che un sistema non congegnato a regola d'arte «può provocare distorsioni che incidono profondamente sul piano di consolidati principi fondamentali»[153].

Nella struttura dei controlli, il legislatore europeo, «in considerazione della natura dei sistemi di IA e dei possibili rischi per la sicurezza e i diritti fondamentali associati al loro utilizzo, anche per quanto riguarda la necessità di garantire un adeguato monitoraggio delle prestazioni»[154] nel contesto reale, prescrive specifiche responsabilità anche nella fase di utilizzazione.

---

[149] Cfr. art. 15 nonché cons. 74) e 75), Reg. UE 2024/1689.

[150] Cfr. cons. 27), Reg. UE 2024/1689.

[151] Sul punto, MANES, *Intelligenza artificiale e giustizia penale*, in AA.VV., *XXVI lezioni di diritto dell'intelligenza artificiale*, cit., p. 282; PALMIOTTO, *The Black box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, in AA.VV., *Algorithmic governance and governance of algorithmic*, Ebers - Cantero Gamito (*edited by*), Cham, pp. 49 ss.

[152] L'espressione si deve a LORUSSO, *Il diritto alla motivazione*, in *Diritto penale contemporaneo online,* 8 novembre 2018.

[153] SIGNORATO, *Giustizia penale e intelligenza artificiale*, cit., p. 613.

[154] Cfr. cons. 91), Reg. UE 2024/1689.

In particolare, lasciando impregiudicati gli ulteriori obblighi già previsti dalla normativa comunitaria, si precisa che pure i *deployer* devono assicurare che «le persone alle quali è affidata l'attuazione delle istruzioni per l'uso e della sorveglianza umana […] dispongano delle competenze necessarie, in particolare un livello adeguato di alfabetizzazione, formazione e autorità in materia di IA»[155].

Più nel dettaglio, si tratta di adottare «misure tecniche e organizzative per garantire di utilizzare tali sistemi conformemente alle istruzioni per l'uso»[156]; affidare la sorveglianza «a persone fisiche che dispongano della competenza, della formazione e delle autorità necessarie»[157]; avere piena libertà di «organizzare le proprie risorse e attività»[158] al fine di esercitare il controllo sui dati di *input*, garantendo che siano «pertinenti e sufficientemente rappresentativi alla luce della finalità prevista dal sistema di IA ad alto rischio»[159]; monitorare il «funzionamento del sistema di IA ad alto rischio sulla base delle istruzioni per l'uso e, se del caso, informare i fornitori a tale riguardo»[160]; conservare i *file* di «*log* generati automaticamente da tale sistema di IA ad alto rischio»[161]; effettuare una «valutazione d'impatto»[162].

Ulteriori rischi, però, potrebbero derivare da utilizzi diversi rispetto a quelli per cui il sistema è stato progettato[163]: fondamentale, in tali casi, è il ruolo assunto dal *deployer*.

Inteso come utilizzatore in senso ampio, è colui che si trova «nella posizione migliore per comprendere come il sistema di IA ad alto rischio sarà utilizzato concretamente» e, pertanto, può «individuare potenziali rischi significativi non previsti nella fase di sviluppo, in ragione di una conoscenza più puntuale del contesto di utilizzo e delle persone o dei gruppi di persone che potrebbero essere interessati, compresi i gruppi vulnerabili».

---

[155] Cfr. cons. 91), Reg. UE 2024/1689.
[156] Cfr. art. 26, § 1, Reg. UE 2024/1689.
[157] Cfr. art. 26, § 2, Reg. UE 2024/1689.
[158] Cfr. art. 26, § 3, Reg. UE 2024/1689.
[159] Cfr. art. 26, § 4, Reg. UE 2024/1689.
[160] Cfr. art. 26, § 5, Reg. UE 2024/1689.
[161] Cfr. art. 26, § 6, Reg. UE 2024/1689.
[162] Cfr. art. 26, § 9, Reg. UE 2024/1689.
[163] Posto che l'utilizzo della macchina dovrebbe avvenire unicamente per la «finalità prevista» dal fornitore (cfr. art. 3, n. 12), è necessario evitare quantomeno l'«uso improprio ragionevolmente prevedibile» di cui all'art. 3, n. 13), Reg. UE 2024/1689.

Il *deployer* svolge altresì un ruolo informativo, cruciale per i soggetti coinvolti: dette spiegazioni dovrebbero avere ad oggetto la finalità prevista dal sistema e il tipo di decisioni da adottare, rendendo edotte le persone fisiche dell'esistenza del «diritto a una spiegazione»[164].

L'assenza di questo pacchetti di cautele e l'omissione della puntuale analisi del rischio[165], da svolgersi caso per caso, ovvero della valutazione d'impatto sui diritti fondamentali[166], condurrebbe alla deriva tecnocratica in cui lo spazio riservato

[164] Cfr. cons. 93), Reg. UE 2024/1689.

[165] Sul sistema di gestione dei rischi, cfr. art. 9, Reg. UE 2024/1689.

[166] Cfr. art 27, Reg. UE 2024/1689, «prima di utilizzare un sistema di IA ad alto rischio di cui all'articolo 6, paragrafo 2, ad eccezione dei sistemi di IA ad alto rischio destinati a essere usati nel settore elencati nell'allegato III, punto 2, i *deployer* che sono organismi di diritto pubblico o sono enti privati che forniscono servizi pubblici e i *deployer* di sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettere b) e c), effettuano una valutazione dell'impatto sui diritti fondamentali che l'uso di tale sistema può produrre. A tal fine, i *deployer* effettuano una valutazione che comprende gli elementi seguenti: a) una descrizione dei processi del *deployer* in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità prevista; b) una descrizione del periodo di tempo entro il quale ciascun sistema di IA ad alto rischio è destinato a essere utilizzato e con che frequenza; c) le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico; d) i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati a norma della lettera c), del presente paragrafo tenendo conto delle informazioni trasmesse dal fornitore a norma dell'articolo 13; e) una descrizione dell'attuazione delle misure di sorveglianza umana, secondo le istruzioni per l'uso; f) le misure da adottare qualora tali rischi si concretizzino, comprese le disposizioni relative alla governance interna e ai meccanismi di reclamo». Cfr. pure cons. 96), secondo cui prima di mettere in uso i *software* è necessario «svolgere una valutazione d'impatto sui diritti fondamentali», il cui obiettivo è «consentire al *deployer* di individuare i rischi specifici per i diritti delle persone o dei gruppi di persone che potrebbero essere interessati e di individuare le misure da adottare al concretizzarsi di tali rischi»; detta valutazione «dovrebbe essere svolta prima del primo impiego del sistema di IA ad alto rischio» e «aggiornata quando il *deployer* ritiene che uno qualsiasi dei fattori pertinenti sia cambiato», individuando i processi «in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità prevista e dovrebbe includere una descrizione del periodo di tempo in cui il sistema è destinato a essere usato e della relativa frequenza, nonché delle categorie specifiche di persone fisiche e gruppi che potrebbero essere interessati nel contesto specifico di utilizzo. La valutazione dovrebbe altresì comprendere l'individuazione di rischi specifici di danno che possono incidere sui diritti fondamentali di tali persone o gruppi. Nell'effettuare tale valutazione, il *deployer* dovrebbe tenere conto delle informazioni pertinenti per un'adeguata valutazione dell'impatto, comprese, tra l'altro, le informazioni trasmesse dal fornitore del sistema di IA ad alto rischio nelle istruzioni per l'uso. Alla luce dei rischi individuati, i *deployer* dovrebbero stabilire le misure da adottare al concretizzarsi di tali rischi, compresi, ad esempio, i meccanismi di *governance* in tale contesto specifico di utilizzo, quali le modalità di sorveglianza umana secondo le istruzioni per l'uso, o le procedure di gestione dei reclami e di ricorso, dato che potrebbero essere determinanti nell'attenuare i rischi per i diritti fondamentali in casi d'uso concreti. Dopo aver effettuato tale valutazione d'impatto, il *deployer* dovrebbe darne notifica alla pertinente autorità di vigilanza del mercato. Se del caso, per raccogliere le informazioni pertinenti necessarie a effettuare la valutazione d'impatto, i *deployer* di sistemi di IA ad alto rischio, in particolare quando i sistemi di IA sono utilizzati nel settore pubblico, potrebbero coinvolgere i portatori di interessi pertinenti, compresi i rappresentanti di gruppi di persone che potrebbero essere interessati dal sistema di IA, gli esperti indipendenti e le organizzazioni della società civile nello svolgimento di tali valutazioni d'impatto e nella progettazione delle misure da adottare al concretizzarsi dei rischi».

dell'autonomia del diritto potrebbe essere «occupato da sedicenti algoritmi che, in realtà, nascondono la vecchia ambizione di dominio, tipica dell'assolutizzazione del potere "oligarchico"»[167].

5. Il cauto atteggiamento del legislatore italiano.

Deve darsi atto che la tecnologia è già da tempo parte della fitta trama del procedimento penale[168] e con la c.d. riforma Cartabia − in ossequio alle indicazioni eurounitarie che deponevano a favore dell'utilizzo dell'informatica come strumento di efficientamento del sistema giustizia − è stata avviata la "transizione digitale del processo"[169].

---

[167] AVITABILE, *Il diritto davanti all'algoritmo*, in *Rivista italiana per le scienze Giuridiche*, 2017, 8, p. 327.

[168] Già da qualche tempo il progresso informatico ha inciso sul procedimento penale introducendo nella sfera giudiziaria nuove strumentazioni impiegabili nella fase investigativa: si pensi alle c.d. indagini atipiche quali la *digital forensic*, il *trojan* nelle intercettazioni, il GPS per il pedinamento elettronico e le videoregistrazioni quali mezzi di prova *ex* art. 189 c.p.p. In materia, ampiamente, SCALFATI (a cura di), *Le indagini atipiche*, II ed., Torino, 2019; si veda, altresì, CENTRORAME, *Le indagini tecnologiche ad alto potere intrusivo fra esigenze di accertamento e sacrale inviolabilità dei diritti della persona*, in *Rivista Italiana di Diritto e Procedura Penale*, 2021, pp. 499 ss.; SPANGHER, *Questioni in tema di investigazioni nella giustizia italiana*, in *Studium Iuris*, 2021, pp. 1039 ss.
Per un'analisi a tutto tondo del connubio tra tecnologia e procedimento penale, GALGANI, *Forma e garanzie nel prisma dell'innovazione tecnologica. Alla ricerca di un processo penale "virtuoso"*, Milano, 2022.

[169] Con la c.d. riforma Cartabia si è assistito al fenomeno della "digitalizzazione" del procedimento penale: sono state, infatti, inserite nel codice di rito disposizioni che elevano a regola aurea la modalità di deposito digitale, favorendo la circolazione smaterializzata degli atti e le notificazioni telematiche. Per una sintesi sul processo penale telematico, Relazione n. 2/23 a cura dell'Ufficio del Massimario della Corte di Cassazione, 5 gennaio 2023, pp. 1 ss.; in dottrina, senza pretesa di esaustività, si rinvia a CAIANIELLO - PUGLIESE, *Manifesto per la giustizia penale digitale: il processo penale telematico*, in AA.VV., *Riforma Cartabia. Le modifiche al sistema penale*, *Commentario diretto da Gian Luigi Gatta e Mitja Gialuz*, *Il procedimento penale tra efficienza, digitalizzazione e garanzie partecipative*, Caianiello - Gialuz - Quattrocolo (a cura di), I, Torino, 2024, pp. 165 ss.; DELVECCHIO, *Prospettive e tempi della digitalizzazione del processo*, in *Processo penale e giustizia*, 2022, pp. 8 ss.; DI NICOLA, *La semplificazione delle attività di deposito di atti, documenti e istanze*, in *Processo penale e giustizia*, fasc. straord., *Giustizia penale: la disciplina transitoria della c.d. riforma Cartabia*, Cimadomo (a cura di), 2023, pp. 25 ss.; GALGANI, *Il processo penale in "ambiente" digitale: ragioni e (ragionevoli) speranze*, in *Questione giustizia*, 2021, 4, pp. 181 ss.; GIALUZ, *Per un processo penale più efficiente e giusto. Guida alla lettura della riforma Cartabia. Profili processuali*, in *Sistema penale*, 28 ottobre 2022, pp. 5 ss.; NARDO, *La progressiva digitalizzazione del processo*, in *Processo penale e giustizia*, fasc. straord., *La disciplina transitoria della c.d. riforma Cartabia*, cit., 2023, pp. 21 ss.; SCACCIANOCE, *Notificazioni al difensore dirette all'imputato*, in *Processo penale e giustizia*, 2022, pp. 25 ss. Sulla celebrazione dei processi da remoto, si veda, GALGANI - AGOSTINO, *L'impiego dei collegamenti audiovisivi ai fini della partecipazione e dell'assunzione probatoria*, in AA.VV., *Riforma Cartabia. Le modifiche al sistema penale*, *Commentario diretto da Gian Luigi Gatta e Mitja Gialuz*, *Il procedimento penale tra efficienza, digitalizzazione e garanzie partecipative*, cit., pp. 213 ss.; MANES, *Intelligenza artificiale e giustizia penale*, cit., pp. 280-281.

Nonostante l'incisività dell'intervento normativo, nulla pare sia stato in grado di compiere quella svolta epocale che ci si aspettava: gli ingranaggi, ormai ossidati, della macchina processuale continuano ancora a funzionare a fatica.

Tra gli obiettivi (disattesi) cristallizzati nel "Piano Nazionale di Ripresa e Resilienza" (c.d. PNRR), oltre all'informatizzazione dell'*iter* processuale, vi era quello di sfruttare al massimo le opportunità offerte dalle nuove tecnologie, *ivi* compresi, quindi, i sistemi di giustizia predittiva.

Il riferimento è ai *tools* di valutazione della pericolosità sociale e del rischio di recidiva del *reo*, usufruibili nei diversi segmenti procedimentali e, finanche, dal giudice nel momento decisorio poiché potenzialmente idonei, da un lato, a supportarlo nella valutazione del caso senza travalicarne la discrezionalità e garantendone l'imparzialità, dall'altro, a contribuire all'abbattimento dei tempi della giustizia.

Tuttavia, il legislatore non ha colto l'occasione per tentare di regolamentarne l'utilizzo nella struttura del processo; tale cambio di passo non è stato realizzato neppure con la più recente stagione riformistica.

Da ultimo, nonostante l'Italia si sia guadagnata il ruolo di capofila nella frenetica corsa alla legiferazione con l'approvazione del disegno di legge A.S. n. 1146 recante "Disposizioni e delega al governo in materia di intelligenza artificiale" del 23 aprile 2024[170], ancora al vaglio del Parlamento, allo stato sembrerebbe vietato *a priori* l'ingresso di tali *software* nelle aule di giustizia[171]; insomma, potrebbe correttamente affermarsi che «non sempre l'arrivare per primi significa anche essere i migliori»[172].

Una proposta destinata a naufragare, se non opportunamente corretta, che rischia di esiliare l'intera nazione dal progresso, rendendola priva di strumenti regolatori per

---

[170] Per un primo commento al DDL, si veda, BARONE, *La regolamentazione dell'Intelligenza Artificiale: è "corsa agli armamenti"*, in *Diritto penale e processo*, 2024, pp. 991 ss.

[171] L'art. 14 sull'"utilizzo dell'intelligenza artificiale nell'attività giudiziaria" recita testualmente: «1. I sistemi di intelligenza artificiale sono utilizzati esclusivamente per l'organizzazione e la semplificazione del lavoro giudiziario nonché per la ricerca giurisprudenziale e dottrinale. Il Ministero della giustizia disciplina l'impiego dei sistemi di intelligenza artificiale da parte degli uffici giudiziari ordinari. Per le altre giurisdizioni l'impiego è disciplinato in conformità ai rispettivi ordinamenti. 2. È sempre riservata al magistrato la decisione sulla interpretazione della legge, sulla valutazione dei fatti e delle prove e sulla adozione di ogni provvedimento».

[172] Così, BARONE, *La regolamentazione dell'Intelligenza Artificiale: è "corsa agli armamenti"*, cit., p. 1001.

affrontare l'evoluzione tecnologica sul versante processuale: è certo, infatti, che l'*AI* irromperà nelle aule di giustizia; l'unica fattore dubbio è "come" lo farà.

Ebbene, il compito del legislatore è proprio quello di mettere a punto precise coordinate su cui collocare i modelli computazionali; solo attraverso una disciplina attenta e meditata si potrebbe evitare il crollo dei pilastri del giusto processo.

Tuttavia, è opportuno interrogarsi sulle ragioni di un tale atteggiamento che si pone in evidente controtendenza rispetto a quanto stabilito a livello comunitario[173].

Inutile celare la timidezza del legislatore italiano dietro lo scudo dell'incertezza dei possibili esiti della rivoluzione algoritmica; al contrario, accogliere benevolmente le novità che propone nel campo del diritto significherebbe tentare di adeguare la fisionomia del procedimento penale ai nuovi strumenti digitali attraverso una precipua regolamentazione, provando altresì a correggere le attuali distorsioni del sistema giustizia.

Dunque, è fondamentale tracciare il sentiero da percorrere, affinché nel (prossimo) futuro si riesca, anche a livello nazionale, a coniare regole *ad hoc* in grado di far fronte alla catarsi tecnologica[174].

6. Oltre i confini europei (cenni).

Sebbene, nel panorama mondiale, l'Europa si sia aggiudicata il primato nella regolamentazione dell'*AI* con l'adozione del primo documento legislativo di *hard law* in materia, anche altri Paesi stanno cercando di dotarsi di una disciplina organica per far fronte alla impellente "rivoluzione dei *bit*".

La Cina, da sempre capofila (insieme agli Stati Uniti) nella promozione del progresso computazionale, ha emanato nel 2017 il *New-Generation AI Development Plan* (*AIDP*), ponendosi l'obiettivo di aumentare gli investimenti per conquistare il titolo di *leader* mondiale nell'innovazione dell'*AI*; il Consiglio di

[173] Il Reg. UE 2024/1689, infatti, pur considerando "ad alto rischio" (art. 6 e All. III) i sistemi algoritmici impiegati per scopi repressivi, ne ammette l'uso purché ricorrano determinate condizioni, vedi § 4.

Da ultimo, deve segnalarsi che, con il parere del 5 novembre 2024, la Commissione ha evidenziato le molteplici incongruenze tra le disposizioni nazionali (contenute nel DDL) e quelle comunitarie (di cui all'*AI Act*), sollecitando l'Italia a conformarsi agli *standard* sovranazionali e a rivedere alcuni punti cruciali del testo legislativo.

[174] Sull'impatto della rivoluzione sul processo penale, LUPARIA DONATI, *La promessa della giustizia tecnologica*, in *Sistema penale online*, 1 agosto 2024, pp. 1 ss.

Stato cinese si è prefissato, altresì, quale proposito intermedio, quello di formulare nuove leggi, regolamenti e norme etiche per disciplinare la materia in maniera puntuale entro il 2025[175].

In Canada, invece, nel 2018 è stata firmata la già citata *Déclaration de Montréal pour un développement responsable de l'intelligence artificielle* ovvero una dichiarazione di principi generali e astratti nonché di valori etici che ogni sistema di *AI* deve rispettare. Tra i traguardi da raggiungere: formare un quadro etico per lo sviluppo e l'implementazione delle macchine computazionali; guidare la transizione digitale in modo che tutti traggano vantaggio dal progresso tecnologico; avviare un *forum* di discussione a livello nazionale e internazionale con l'obiettivo di sviluppare applicativi algoritmici in modo equo, inclusivo ed ecosostenibile[176].

In tale prospettiva si è posta pure l'Australia che nel 2019, su proposta del *Data 61* e del CSIRO dell'*Australian Commonwealth − Department of Industry, Innovation and Science*, ha adottato l'*Australian AI Ethical Framework*, che ha stabilito principi fondamentali per costruire un solido quadro etico di riferimento. Detti principi, perfezionati dopo una consultazione pubblica, sono i seguenti: «*human, social and environmental wellbeing; humans-centred values; fairness; privacy protection and security; reliability and safety; transparency and explainability; contestability; and accountability*»[177].

L'India, invece, − al pari degli Stati Uniti d'America, quantomeno fino al 2019[178] − non si è preoccupata di mettere a punto un vero e proprio quadro etico che tenga conto della salvaguardia dei diritti fondamentali dell'uomo. Tuttavia, l'assenza di una precipua normazione non ha frenato la diffusione della tecnologia algoritmica sul terreno operativo: nel luglio 2019, infatti, il Ministero dell'Interno indiano ha annunciato l'utilizzo, a livello nazionale, di sistemi di riconoscimento facciale automatizzato (*AFRS*), che utilizzerebbero immagini estratte da telecamere a

[175] Sullo stato dell'arte cinese, si veda, DALY - HAGENDORFF - MANN - MARDA - WAGNER - WEI WANG, *AI, Governance and Ethics. Global Perspective*, in AA.VV., *Constitutional Challenges in the Algorithmic Society*, cit., p. 187.

[176] Cfr., Dichiarazione di Montréal.

[177] DALY - HAGENDORFF - MANN - MARDA - WAGNER - WEI WANG, *AI, Governance and Ethics. Global Perspective*, cit., p. 186.

[178] Invero, solo nel febbraio 2019, a seguito dell'ordine impartito dall'esecutivo Trump circa il mantenimento della *leadership* americana in materia di intelligenza artificiale, è stato istituito dal *National Science and Technology Council* (*NSTC*) il *Select Committee on Artificial Intelligent*.

circuito chiuso, al fine di agevolare il compito della polizia di identificare i criminali, creando una migliore rete di informazione tra i singoli uffici[179].

Al fine di scongiurare, per l'ennesima volta, il c.d. "effetto Bruxelles", anche gli Stati Uniti d'America si sono avviati – in verità, solo timidamente – al cammino verso la regolamentazione dell'*AI* con l'adozione dell'*AI Bill of Right* del 4 ottobre 2022[180]. Dopo alcune proposte di legge cadute nel vuoto, il 30 ottobre 2023 l'*ex* Presidente, Joe Biden, ha adottato un *Executive Order (14100) on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, che detta norme minime sull'uso dell'*AI*[181].

Ebbene, il prospettato mosaico normativo (e applicativo) globale consente di scorgere un evidente e preoccupante stato di impreparazione.

Si dovrebbe, a livello mondiale, migliorare i meccanismi − legislativi e, solo dopo, operativi − attraverso i quali interfacciarsi con le nuove tecnologie governate da sistemi di *AI*; tale lacuna dev'essere al più presto colmata, evitando così di mettere in campo sistemi algoritmici che, in assenza di un preciso apparato legislativo cui fare riferimento, potrebbero funzionare senza tener conto delle garanzie difensive, infrangendo i delicati equilibri del procedimento penale.

[179] Per una ricostruzione della precaria normativa indiana e delle applicazioni pratiche dell'*AI*, DALY - HAGENDORFF - MANN - MARDA - WAGNER - WEI WANG, *AI, Governance and Ethics. Global Perspective*, cit., p. 194.

[180] Il testo integrale è consultabile al sito www.whitehouse.gov. Per un primo commento alla normativa, si veda, HEIKKILA, *The White House just unveiled a new Bill of Rights*, in *MIT Technology Review online*, 4 ottobre 2024.

[181] Sul punto, BARONE, *Giustizia Predittiva e Certezza del Diritto*, cit., pp. 42 ss.

CAPITOLO II

LA SPERIMENTAZIONE DI MODELLI ALGORITMICI NEL PROCEDIMENTO PENALE: UN'INDAGINE COMPARATA

SOMMARIO: 1. Uno sguardo ai sistemi di *common law*. 2. Gli algoritmi di *pre-crime*. 3. Agli esordi del riconoscimento facciale. 4. L'impiego probatorio dell'*AI*. 5. I *risk assessment tools* nel momento decisorio. 6. I riflessi del caso *Loomis*.

1. Uno sguardo ai sistemi di *common law*.

Com'è noto i sistemi di *AI* sono maggiormente utilizzati nei paesi di *common law*, rispetto a quanto accade nei modelli processuali derivanti dal diritto romano.

Ciò in quanto i primi s'imperniano sul valore del precedente giurisprudenziale sulla cui base la macchina decide, cosa che non potrebbe accadere nei secondi, per definizione, fondati sul diritto scritto, sul paradigma del giudice quale bocca della legge ed ancorati al principio di stretta legalità.

Dunque, considerata l'incerta traducibilità algoritmica delle regole decisorie vigenti[1], i sistemi giuridici di *civil law* potrebbero, *prima facie*, dimostrarsi inadeguati ad ospitare tali avanguardie.

Peraltro, i processi penali di *common law* si caratterizzano per la tradizionale scissione tra accertamento della colpevolezza (*verdict*) e quantificazione della pena (*sentencing*), per cui il coinvolgimento di sistemi digitali non comporterebbe alcuna «compressione e compromissione del ruolo giurisdizionale»[2]; al contrario, ciò probabilmente avverrebbe nel nostro ordinamento, in cui il momento decisorio risulta unitario ed è affidato interamente all'organo giudicante.

Pur senza coinvolgere le garanzie difensive, questo spiegherebbe le resistenze all'ammissione di modelli algoritmici nella giurisdizione italiana, giustificandone, di contro, il massivo impiego fuori dai confini europei.

---

[1] Su cui, *infra*, Cap. IV, § 1.

[2] QUATTROCOLO, *Risk assessment: sentencing o non sentencing?*, 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, p. 76.

In effetti nelle Corti statunitensi sin dai primi anni del XXI secolo[3], sono stati utilizzati *evidence-based risk assessment tools*[4] ovvero *software* di valutazione quantitativa del rischio di recidiva *post* condanna e dell'ammontare della cauzione nell'eventuale *release on bail* dell'imputato[5], al fine di comprimere l'elevato tasso di detenzione registrato.

Allo stato nessuna fase dello schema procedimentale d'oltreoceano pare sia sfuggita al fascino dell'*AI*[6]; dall'analisi dei documenti nota come *e-discovery*[7] al momento

[3] Nel 2004 la Conferenza Giudiziaria degli Stati Uniti ha approvato un piano volto a garantire un "approccio strategico", attraverso una riorganizzazione del sistema giustizia finalizzata alla "riduzione della recidiva". Cfr. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal-Rivista di Biodiritto*, 2019, 1, p. 72.
Tuttavia, già nel 1994 lo Stato della Virginia aveva ideato un proprio strumento di *risk assessment*, destinato ad essere applicato nella fase del *sentencing*.

[4] Sulla nascita di tali modelli di valutazione del rischio negli Stati Uniti, QUATTROCOLO, *Risk assessment*, cit., p. 71 ss.

[5] 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 online*, 28 maggio 2019, p. 9, sottolinea come l'istituto del *bail* comporti una serie di problematiche, ragion per cui si sta tentando di correggerne il tiro. Nel dettaglio, infatti, «il Kentucky ha adottato un progetto pilota – denominato "*Administrative Pretrial Release Program*" – in 20 giurisdizioni su 120, poi esteso nel 2017 all'intero Stato, basato su un utilizzo peculiare del *PSA*. Al fine di incrementare l'efficienza del sistema e salvare le risorse per i prevenuti più pericolosi, in tale Paese si prevede che per una serie di reati i *pretrial officers* possano ordinare il rilascio immediato dei prevenuti, il cui rischio di fuga e commissione di reati risulti sulla base del *tool* in questione basso o moderato, senza l'intervento di un giudice». Nel 2018, invece, in California si è adottato il "*Money Bail Reform Act*", secondo cui «il *Pretrial Assessment Services* è tenuto a rilasciare direttamente, senza l'intervento di un giudice, i prevenuti il cui livello di rischio di fuga risulti basso, a seguito dello svolgimento di un test per il tramite di uno dei *risk assessment tools* accreditati, contenuti in una lista stilata dal *Judicial Council* della California».
Sul punto anche LIVNI, *Nei tribunali del New Jersey è un algoritmo a decidere chi esce su cauzione*, in www.internazionale.it, 2017, che evidenzia come nello Stato del New Jersey le udienze per la concessione della libertà su cauzione siano state sostituite da valutazioni algoritmiche del rischio: chiunque può essere rilasciato, se non ritenuto pericoloso dall'*AI*, anche senza pagare una somma di denaro; precisa, però, che la valutazione del *software* serve esclusivamente come guida per la decisione e non si sostituisce nell'attività di giudizio del magistrato.

[6] GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., p. 4.

[7] Si tratta dello studio dei documenti prodotti dalle parti affidato a programmi di *AI* (c.d. *tecnology assisted*) capaci di garantire una maggiore velocità ed una più elevata precisione rispetto a quanto potrebbe fare l'uomo, atteso che «*humans can be swayed by emotion. Humans can be convinced. Humans get tired or have a bad day*», (così, KUGLER, *AI Judges and Juries*, in *Communications of the ACM*, 2018, 61, 12, p. 19), mentre la macchina sarebbe imparziale poiché meno propensa a contaminazioni esterne. Sul punto anche DIXON, *Artificial Intelligence: Benefits and Unknown Risks*, in www.americanbar.org, 15 gennaio 2021; KAPLAN, *Intelligenza artificiale. Guida al futuro prossimo*, Roma, 2018, pp. 137 ss.

investigativo[8], dalla dimensione probatoria[9] alle valutazioni cautelari sul rilascio del *defendant*, sino a giungere alla determinazione del *quantum* di pena da infliggere al condannato all'esito di un verdetto di colpevolezza[10]: l'influenza dei sistemi computazionali sembra, dunque, inarrestabile.

L'*appeal* della tecnologia ha conquistato le dinamiche decisorie al punto che in circa metà delle giurisdizioni statali è ormai ammesso l'utilizzo di algoritmi di *risk assessment*.

Intesi, infatti, come strumenti «di misura del comportamento antisociale, (e) non (come) una risposta al comportamento antisociale medesimo»[11], sia nella *pre-trial detention*[12] che nella fase del *sentencing*[13], garantiscono il diritto di difesa dell'imputato mediante la possibilità di contestarne i risultati servendosi del manuale d'uso del *software*.

Sperimentazioni di tali sistemi intelligenti sono state registrate anche nel Regno Unito, ove la comunità accademica è particolarmente attenta allo studio di soluzioni idonee a coniugare il mondo digitale a quello della giustizia penale[14].

Tuttavia, se negli ordinamenti giuridici di *common law* la sperimentazione dell'*AI* sembra destinata ad assumere valore portante a livello globale, nel perimetro nazionale, tra entusiasmi e reticenze, pare ancora una conquista lontana e utopistica.

---

[8] Diversi dipartimenti di polizia si avvalgono di strumenti algoritmici utili ad acquisire eventuali notizie di reato e orientare l'attività di prevenzione e di repressione dei delitti. Sul tema, BARBARO, *Uso dell'intelligenza artificiale nei sistemi giudiziari: verso la definizione di principi etici condivisi a livello europeo?*, in *Questione giustizia*, 2018, 4, pp. 193 ss.; SLOBOGIN, *Assessing the Risk of Offending through Algorithms*, in AA.VV., *The Cambridge Handbook of the Law of Algorithms*, Barfield (*edited by*), Cambridge, 2021, pp. 444 ss. Sull'impiego di *AI* per *Computational Crime Analysis*, si veda, LETTIERI, *Law in Turing's Cathedral*, in AA.VV., *The Cambridge Handbook of the Law of Algorithms*, cit., pp. 699 ss.

[9] Sui primi casi di testimonianza digitale, ATERNO, Alexa *testimone in tribunale: i vantaggi per gli investigatori e le garanzie per la difesa*, in *Agenda digitale online*, 20 marzo 2020.

[10] Tali strumenti di valutazione offrono una proiezione futura della possibile pericolosità dell'autore del reato e sono basati, da un lato, sull'individuazione di "fattori di rischio" c.d. "statici" (genere, età del primo arresto) o "dinamici" (età anagrafica, lavoro svolto, etc.) del comportamento illecito e, dall'altro lato, su "fattori di protezione" che servono per controbilanciare il pericolo di una condotta illecita. Tuttavia, come autorevolmente affermato da QUATTROCOLO, *Risk assessment*, cit., p. 75, il loro compito è calcolare «la possibilità di una condotta antisociale, e devono misurarla in termini non statici ma dinamici, perché la persona è un soggetto che cambia nel tempo».

[11] QUATTROCOLO, *Risk assessment*, cit., p. 73.

[12] SLOBOGIN, *Assessing the Risk of Offending through Algorithms*, cit., pp. 442 ss.

[13] SLOBOGIN, *Assessing the Risk of Offending through Algorithms*, cit., pp. 436 ss.

[14] PALMIRANI - SAPIENZA - BOMPREZZI, *Il ruolo dell'intelligenza artificiale nel sistema giustizia: funzionalità, metodologie, principi*, in AA.VV., *La trasformazione digitale della giustizia nel dialogo tra discipline*, Palmirani - Sapienza (a cura di), Milano, 2022, p. 21.

Ciò nonostante, pare opportuno volgere lo sguardo a tali esperienze giuridiche, pur tenendo conto delle differenze strutturali che ne caratterizzano l'architettura processuale, al fine di trarre nuove consapevolezze spendibili nel contesto processuale italiano.

2. Gli algoritmi di *pre-crime*.

Sull'onda del film *Minority Report*[15], malgrado lo scetticismo di gran parte della dottrina[16], quella investigativa è stata la prima aerea del procedimento penale ad essere sedotta dal potere dell'*AI*[17].

Negli Stati Uniti dilaga – ormai da un po' di anni − l'uso di *tools* di *predictive policing*[18] basati su tecnologie algoritmiche e di riconoscimento facciale[19].

La rapida diffusione di tale fenomeno ha reso necessario un attento approfondimento della tematica.

Infatti, già nel 2009, l'*Office of Justice Assistance*, in collaborazione con il *Los Angeles Police Department*, ha organizzato un incontro di studi tra esperti del settore – ricercatori, criminologi, sociologi, giuristi e funzionari di polizia − per

[15] La trama del film di Steven Spielberg – che si rifà a DICK, *Rapporto di minoranza e altri racconti*, trad. it a cura di Prezzavento, 2002, Roma – prefigura un futuro distopico in cui nella città di Washington, grazie ad un sistema chiamato *Precrime*, che si basa sulle predizioni di tre *Pre-cogs* dai poteri extra-sensoriali, non si verificano più omicidi, poiché la polizia ha la possibilità di intervenire prima che avvengano, arrestando i "colpevoli" di aver avuto l'intenzione di uccidere qualcuno. Richiamano la pellicola, in prospettiva giuridica, COPPOLA, *Commisurazione della pena e intelligenza artificiale: una ipotesi di lavoro con l'algoritmo Ex-Aequo*, in *Archivio penale web*, 2023, 2, pp. 1 ss.; CAMALDO, *Intelligenza artificiale e investigazione penale predittiva*, in *Rivista Italiana di Diritto e Procedura Penale*, 2024, 1, p. 234; LORUSSO, *Il contributo degli esperti alla formazione del convincimento giudiziale*, in *Archivio penale*, 2011, pp. 809 ss.; NICOLÌ, *La predizione nell'attività di polizia*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, cit., p. 45.

[16] Si veda, tra i tanti, NICOLÌ, *La predizione nell'attività di polizia*, cit., p. 45, il quale ritiene che prevedere con certezza la commissione di un delitto sia pure fantascienza.

[17] Sull'ampio utilizzo di algoritmi nelle indagini statunitensi, ROTH, *The Use of Algorithms in Criminal Adjudication*, in AA.VV., *The Cambridge Handbook of the Law of Algorithms*, cit., pp. 407 ss.

[18] Sul punto, PERRY - MCINNIS - PRICE - SMITH - HOLLYWOOD, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, Santa Monica, 2013, p. 1, chiariscono che «*predictive policing is the application of analytical techniques − particularly quantitative techniques − to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions*».

[19] GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., p. 2.

discutere e valutare l'impatto degli strumenti di polizia predittiva sui diritti fondamentali dell'uomo e sulla *privacy*[20].

Nonostante le resistenze di coloro i quali denunciano importanti ricadute sul piano del trattamento dei dati personali, tale *trend* risulta ancora attuale poiché giustificato da esigenze di contrasto alla criminalità.

Infatti, i dipartimenti di polizia di Chicago, New York, Los Angeles e Miami continuano ad utilizzare sistemi di "polizia predittiva"[21] nel tentativo di arginare il massivo e incontrollato uso di armi nelle aree cittadine, problematica che affligge da tempo il continente americano.

L'investigazione predittiva rivela, sulla base di dati statistici, sia profili soggettivi (chi commetterà il reato) che oggettivi (quale reato sarà commesso, dove e quando), proprio al fine di evitare *ab origine* il verificarsi di eventi delittuosi[22].

Tuttavia, per compiere una valutazione di fattibilità circa l'impiego di tali *tools* nella fase delle indagini è necessario comprenderne il reale funzionamento.

In primis è opportuno precisare la genesi del *dataset* impiegato dalla macchina intelligente.

Il sistema produce un preciso *output* incrociando due diverse categorie di dati.

Da un lato, le informazioni relative «a notizie di reati precedentemente commessi, agli spostamenti e alle attività di soggetti sospettati, ai luoghi in cui si svolgono le azioni criminali, al periodo dell'anno e alle condizioni atmosferiche»[23] in cui si sono verificate le condotte illecite.

---

[20] Più in generale, a livello nazionale, sulla complessa relazione tra *privacy* e giustizia penale alla luce dell'evoluzione tecnologica, LUPARIA DONATI, Privacy, *diritti della persona e processo penale*, in *Rivista di diritto processuale*, 2019, pp. 1488 ss.

[21] Una definizione è proposta da BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Diritto Penale e Uomo*, 2019, 10, p. 10, secondo cui «per "polizia predittiva" possiamo intendere l'insieme delle attività rivolte allo studio e all'applicazione di metodi statistici con l'obiettivo di "predire" chi potrà commettere un reato, o dove e quando potrà essere commesso un reato, al fine di prevenire la commissione dei reati stessi».

[22] Sul punto, BASILE, *Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione*, in AA.VV., *Diritto penale e intelligenza artificiale. Nuovi scenari*, Balbi - De Simone - Esposito - Manacorda (a cura di), Torino, 2022, pp. 6 ss.; CONTISSA - LASAGNI, *When it is (also) Algorithms and AI that decide on Criminal Matters: In Search of an Effective Remedy*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2020, pp. 280 ss.; PERRY - MCINNIS - PRICE - SMITH - HOLLYWOOD, *Predictive Policing*, cit., pp. 1 ss.

[23] CAMALDO, *Intelligenza artificiale e investigazione penale predittiva*, cit., p. 234.

Dall'altro, quelle afferenti «all'origine etica, al livello di scolarizzazione, alle condizioni economiche, alle caratteristiche somatiche»[24] dei possibili sospettati.

Il procedimento algoritmico si articola in tre fasi: l'inserimento dei dati nel sistema, l'analisi algoritmica degli stessi, la produzione della risposta e l'uso della medesima da parte degli operatori di polizia.

Sulla base del responso generato dall'*AI* è, infatti, possibile organizzare meglio il piano di pattugliamento di determinate zone della città, mettendo a punto precise strategie preventive, oltre che repressive.

Dunque, la diffusione degli strumenti tecnologici di *law enforcement* ha determinato un repentino mutamento di approccio.

Si è passati dall'atteggiamento "reattivo" − che vedeva la polizia protagonista di interventi mirati alla ricerca dell'autore di un reato già commesso – al metodo "proattivo"[25], ove l'azione della forza pubblica precede l'attività criminosa con l'obiettivo di evitare che si verifichi.

Insomma, si tratta di una vera e propria modifica sostanziale delle priorità, atteso che non si percorre più unicamente la strada della repressione del delitto consumato − sino ad ora l'unica ad essere battuta − ma si è scelto di adottare la diversa prospettiva della prevenzione del crimine.

Due sono le tipologie di sistemi algoritmici investigativi attualmente in uso: i *place-based systems*[26] e i *person-based systems*[27].

I primi prevedono, in tempo reale, la possibile commissione del reato (indicandone la specie) in un determinato spazio territoriale, consentendo così alle forze dell'ordine un più attento monitoraggio delle zone metropolitane c.d. "a rischio" con una migliore gestione delle attività di *patrolling*.

La *ratio* di tale innovativa tecnica investigativa riposa nel principio secondo cui «gli eventi criminali hanno luogo al ricorrere di determinati fattori spazio-temporali

[24] CAMALDO, *Intelligenza artificiale e investigazione penale predittiva*, cit., p. 235.
[25] Ne parla CASTETS - RENARD, *Human Rights and Algorithmic Impact Assessment for Predictive Policing*, in AA.VV., *Constitutional Challenges in the Algorithmic Society*, Micklitz - Pollicino - Reichman - Simoncini - Sartor - De Gregorio (*edited by*), Cambridge, 2022, p. 95.
[26] In argomento, ALGERI, *Intelligenza artificiale e polizia predittiva*, in *Diritto penale e processo*, 2021, pp. 724 ss.
[27] Sul tema, CAMALDO, *Intelligenza artificiale e investigazione penale predittiva*, cit., p. 238.

ovvero alla convergenza di delinquenti, di vittime o di obiettivi in contesti specifici in un tempo e in uno spazio definiti»[28].

In sostanza, attraverso l'analisi dei dati relativi alla c.d. criminalità ambientale, il *software* è capace di creare un *output* che consente una migliore «allocazione delle forze di polizia al fine di neutralizzare e prevenire la commissione di reati, riducendo così la vittimizzazione»[29] e ottenendo indagini più approfondite e celeri.

A questa prima tipologia appartiene il *software PredPol*[30], testato nei dipartimenti di polizia statunitensi di Los Angeles e Chicago nonché nella Contea inglese del Kent[31]. In base ai *data input* di cui è dotato ovvero le informazioni contenute negli archivi di polizia (le denunce, i verbali di arresto e la documentazione delle telefonate d'emergenza effettuate dai cittadini) riesce a prevedere in modo accurato tempi e luoghi di commissione di un determinato reato; individua gli *hotspots* sulla base dei modelli statistici utilizzati in sismologia, permettendo alle autorità di pubblica sicurezza di ripatire in modo migliore le proprie risorse in precisi contesti urbani.

Altro dispositivo predittivo è il *Palantir*[32], utilizzato a Los Angeles, New York e New Orleans, che restituisce previsioni del rischio di commissione di reati generando una griglia geografica e temporale. Il *dataset* utilizzato è molto ampio e include «*crime history*», «*historical information which is not directly connected to crime*» e «*custody data*»[33].

Diversa struttura hanno, invece, i *person-based systems* che elaborano il profilo seriale di un singolo individuo, permettendo alle autorità investigative di esercitare un più attento controllo sul soggetto interessato.

A differenza degli *hotspots analysis*, tali sistemi analizzano comportamenti criminosi reiterati con l'obiettivo di giungere all'identificazione del soggetto attivo

---

[28] CAMALDO, *Intelligenza artificiale e investigazione penale predittiva*, cit., p. 236.

[29] MANES, *Intelligenza artificiale e giustizia penale*, in AA.VV., *XXVI lezioni di diritto dell'intelligenza artificiale*, Ruffolo (a cura di), Torino, 2021, p. 281.

[30] Si tratta di un *software* commerciale ideato dalla società americana *PredPol Inc*.

[31] Per un approfondimento sull'applicativo *PredPol*, CASTETS - RENARD, *Human Rights and Algorithmic Impact Assessment for Predictive Policing*, cit., p. 96.

[32] È stato messo a punto dalla società *Palantir Technologies Inc*., con sede in California, la quale detiene il brevetto *Crime Risk Forecasting* (ottenuto l'8 settembre 2015), che costituisce un insieme di *software* di polizia predittiva.

[33] Offre un'analisi approfondita del funzionamento di *Palantir*, CASTETS - RENARD, *Human Rights and Algorithmic Impact Assessment for Predictive Policing*, cit., p. 98.

di reato; sono, dunque, basati sulla serialità individuale dell'autore (*crime linking*) e prevedono come, dove e quando quel determinato soggetto commetterà ulteriori delitti.

Nel contesto nazionale sono già utilizzati sistemi tecnologici di *law enforcement* allo scopo di prevenire la commissione di un reato: si pensi, ad esempio, alle intercettazioni − specie quelle preventive − nonché alle videoregistrazioni di circuiti di videosorveglianza pubblici o privati[34], utilizzabili poi in dibattimento come prove documentali.

Tuttavia, con l'avvento dell'*AI*, nonostante le ostilità della dottrina, sono stati sperimentati anche sistemi predittivi che funzionano sulla falsa riga di quelli adottati oltreoceano[35].

Tali applicativi hanno una natura che potremmo definire "ibrida": costituiscono una perfetta sintesi tra le due diverse modalità operative poc'anzi menzionate ovvero il *place-based system* e il *person-based system*.

Ne sono esempi i *software* come *Keycrime*, ideato da Mario Venturini, dirigente della Polizia di Stato presso la Questura di Milano per prevenire condotte seriali come rapire, truffe agli anziani, furti in appartamento e violenze sessuali, e *XLAW*, messo a punto da Elia Lombardo, Ispettore di Polizia della Questura di Napoli, e

[34] Le definisce come «*surveillance technology*», GALLI, *Law Enforcement and Data-Driven Predictions at the National and EU Level. A Challenge to the Presumption of Innocence and Reasonable Suspicion?*, in AA.VV., *Constitutional Challenges in the Algorithmic Society*, cit., p. 114.

[35] Già nel 2019, il documento di presentazione del Convegno annuale di esperti di Polizia su "*Artificial Intelligence and Law Enforcement*", organizzato dall'OSCE, precisava che «nei loro sforzi per aumentare l'efficienza e l'efficacia e per stare al passo con le innovazioni tecnologiche, le autorità e le agenzie di *law enforcement* di tutto il mondo stanno esplorando sempre più i potenziali dell'IA per il loro lavoro. La crescente quantità di dati ottenuti e archiviati dalla polizia ha anche richiesto metodi e strumenti più sofisticati per la loro gestione e analisi, per l'identificazione di modelli (*pattern*), la previsione dei rischi e lo sviluppo di strategie per allocare le risorse umane e finanziarie dove sono maggiormente necessarie. Anche se l'uso dell'IA nel lavoro delle forze dell'ordine è un argomento relativamente nuovo, alcuni strumenti basati sull'intelligenza artificiale sono già stati testati e sono persino attivamente utilizzati dai servizi di polizia di diversi Paesi del mondo. Questi includono software di analisi di video e immagini, sistemi di riconoscimento facciale, di identificazione biometrica, droni autonomi e altri robot e strumenti di analisi predittiva per prevedere le "zone calde" del crimine o anche per identificare potenziali criminali futuri, in particolare i criminali ad elevata pericolosità»; il documento completo può essere consultato sulla Rivista *Diritto penale e uomo*, *Redazione*, *Artificial Intelligence and Law Enforcement: an Ally or an Adversary?*, 23 settembre 2019.

completato dal Dipartimento di Pubblica Sicurezza del Ministero dell'Interno, attualmente utilizzato in diverse regioni della penisola[36].

Nel dettaglio, quest'ultimo è pensato per contrastare i reati contro il patrimonio (rapine, furti e borseggi), che assumono carattere di serialità e ciclicità, in quanto tendenzialmente «messi in atto da soggetti deviati e modestamente organizzati, che usano questi espedienti per costruire un profitto in un arco di tempo relativamente breve»[37].

Attraverso l'elaborazione di una enorme quantità di dati estratti dalle denunce-querele pervenute alle forze dell'ordine, dalle banche dati di polizia e dai *social network* (*ivi* comprese, quindi, le caratteristiche del sospettato come genere, altezza, nazionalità, aspetti biometrici e altri segni distintivi) genera un preciso *output*.

Lavora individuando fattori ricorrenti quali la commissione di più rapine nei medesimi luoghi, i tratti comuni dei prevenuti (possesso dello stesso tipo di casco o di moto) nonché l'identità del *modus operandi* adottato[38].

Dunque, il sistema basandosi su controlli selettivi e sequenziali si aggiorna ogni trenta minuti, offrendo degli *alert* con cui descrive – con ben due ore di anticipo − il tipo di reato che potrebbe essere commesso, le modalità di esecuzione nonché l'identità sia del soggetto attivo di reato che di quello passivo.

Offrendo una mappatura del crimine che mette insieme sociologia, matematica e statistica, circoscrive zone e orari "caldi" e «*"hot people"*»[39], permettendo alle forze di polizia di impedire la commissione del crimine o – nella peggior ipotesi – di cogliere in flagranza di reato il malvivente, potendo così azionare i meccanismi codicistici pre-cautelari dell'arresto e del fermo.

Peraltro, il principio impiegato è quello del *crime linking*, che consente di collegare tra loro diversi eventi delittuosi commessi dal medesimo soggetto in tempi e luoghi differenti: così, per un verso, rivela anche il "chi ignoto" si renderà autore della

[36] In particolare, oltre alla città di Napoli, l'applicativo è stato testato anche a Prato, Salerno, Venezia, Modena e Parma, affinché migliori la prevenzione dei delitti nelle aree urbane.

[37] CAMALDO, *Intelligenza artificiale e investigazione penale predittiva*, cit., p. 236.

[38] Dal 2008 al 2017 i reati contro il patrimonio sono diminuiti del 57% e sono stati scoperti i responsabili 3 volte su 4, con un danno patrimoniale evitato pari a 2.5 milioni di euro. Per ulteriori approfondimenti, si veda, il sito internet ufficiale dell'applicativo, www.xlaw.it.

[39] Così, SLOBOGIN, *Assessing the Risk of Offending through Algorithms*, cit., p. 432.

condotta criminosa e, per altro verso, costruisce le basi per valutare ipotesi di connessione processuale *ex* art. 12 c.p.p.

In questo modo, a seguito dell'arresto, possono essere contestati al *reo* i delitti commessi, in rapporto di concorso formale ai sensi dell'art. 81, comma 1, c.p. ovvero uniti dal vincolo della continuazione *ex* art. 81, comma 2, c.p.

Questa strategia consente di risparmiare tempo e risorse: l'assegnazione del ruolo effettuata in favore di un magistrato potrebbe attrarre a sé anche gli ulteriori episodi delittuosi della medesima natura, condensandoli in un unico capo d'imputazione o comunque in un solo fascicolo, evitando di dover disporre la riunione in un momento successivo.

In questo modo, alla persona sottoposta alle indagini preliminari potrebbe essere altresì consentito di accedere al rito differenziato dell'applicazione della pena su richiesta delle parti di cui all'art. 444 c.p.p. per il complesso di reati contestati, assicurando una risposta dello Stato più veloce ed efficace.

Inoltre, *XLAW* riuscirebbe anche ad attribuire un indice di rischio alla cattura del potenziale soggetto attivo di reato, indicando pure la possibilità che questi sia armato.

Il successo riscontrato dall'impiego di detto sistema si è tradotto in una consistente riduzione della criminalità[40] e in un miglioramento della capacità decisionale degli operatori di polizia; al contempo, la razionalizzazione degli interventi ha comportato una netta riduzione dei costi, anche in termini di carburante speso, grazie alla diminuzione dei chilometri percorsi. Non meno importante, la netta ottimizzazione dell'operatività del personale di pubblica sicurezza, per il quale si è registrato un evidente calo di *stress* emotivo, nonché l'incremento positivo della percezione pubblica delle forze armate, che induce i cittadini a nutrire nuovamente un sentimento di fiducia nel lavoro svolto dagli organi di pubblica sicurezza.

[40] CAMALDO, *Intelligenza artificiale e investigazione penale predittiva*, cit., p. 237, riporta le dichiarazioni rese dall'ideatore di *XLAW* durante una intervista televisiva del 29 dicembre 2018, dalle quali è emerso che «il sistema ha contribuito ad abbattere il tasso di criminalità, assestandosi su una percentuale del -22% nella città di Napoli e -39% in quella di Prato».

Altro sistema, analogo al *software* che abbiano appena analizzato, è *Pelta Suite*[41]: ideato per garantire la sicurezza urbana, è rappresentato dallo *slogan* «vedere per prevedere, prevedere per provvedere»[42].

Si tratta di un servizio messo a disposizione della polizia locale per frenare la diffusione di fenomeni illeciti e di degrado nelle città, risparmiando anche sui costi di gestione della sicurezza; frutto di studi multidisciplinari[43], si basa su principi euristici e lavora attraverso un modello innovativo di analisi del rischio, adottando una logica probabilistica e preventiva.

Tuttavia, al netto di ogni entusiasmo ottimistico, residua un margine di fallibilità della macchina che potrebbe rivelarsi fatale per il soggetto sottoposto alle indagini. Molteplici sono i possibili rischi da scongiurare: l'anticipazione della soglia di punibilità, ritenuta inaccettabile in un sistema democratico; la lesione del diritto alla presunzione di non colpevolezza costituzionalmente tutelata; lo spostamento del «baricentro del diritto penale dall'accertamento del fatto ad una verifica avente ad oggetto esclusivamente, o comunque eminentemente, l'autore di quel fatto»[44].

Viepiù che nel contesto comunitario i sistemi di polizia predittiva rientrano nelle "pratiche vietate" *ex* art. 5, atteso che «in linea con la presunzione di innocenza, le persone fisiche nell'Unione dovrebbero sempre essere giudicate in base al loro comportamento effettivo» e non «sulla base di un comportamento previsto dall'IA» soprattutto nel caso in cui non ci sia «un ragionevole sospetto che la persona sia coinvolta in un'attività criminosa sulla base di fatti oggettivi verificabili e senza una valutazione umana al riguardo»[45].

---

[41] Sull'uso di *Pelta Suite* nel contesto urbano veneziano e, in particolare, nella città di Caorle, si veda, BIARELLA, *Polizia Predittiva: al via la sperimentazione a Caorle*, in *Altalex online*, 24 maggio 2021.

[42] Ne parla CAMALDO, *Intelligenza artificiale e investigazione penale predittiva*, cit., p. 237.

[43] Come precisato da CAMALDO, *Intelligenza artificiale e investigazione penale predittiva*, cit., p. 237, «il *software* nasce da uno studio accreditato da più centri di ricerca sui fenomeni di insicurezza urbana quali furti, scippi, rapine, borseggi, spaccio di stupefacenti, abusi di ogni genere, prostituzione e incidenti stradali, soprattutto quelli che hanno una correlazione con comportamenti illeciti come, ad esempio, la guida in stato di ebrezza o l'uso di sostanze stupefacenti oppure quelli generati da insidie presenti sul manto stradale».

[44] Così, MANES, *Intelligenza artificiale e giustizia penale*, cit., p. 282. In argomento, cfr. altresì, RICCIO, *Ragionando su intelligenza artificiale e processo penale*, in *Archivio penale web*, 21 novembre 2019, p. 8; UBERTIS, *Intelligenza artificiale e giustizia predittiva,* in *Sistema penale online*, 16 ottobre 2023, p. 4.

[45] Cfr., cons. 42), Reg. UE 2024/1689.

Di conseguenza «dovrebbero essere vietate le valutazioni del rischio effettuate in relazione a persone fisiche intese a determinare la probabilità che queste ultime commettano un reato o volte a prevedere il verificarsi di un reato effettivo o potenziale»[46].

Considerato che, nel nostro ordinamento giuridico, le indagini preliminari sono deputate alla ricerca dell'autore di una condotta criminosa già consumata, il valore che potrebbe essere riconosciuto ai sistemi di *predictive policing*, oltre a rendere più efficace la gestione delle risorse e dei tempi processuali nei casi di connessione *ex* art. 12 c.p.p., sarebbe quello di ottenere una ben ponderata adozione di misure pre-cautelari, offrendo, al contempo, soluzioni investigative più esaurienti.

Il rischio − comune a tutti i *software* di *AI* − è, però, che l'applicativo sia incline a riprodurre schemi discriminatori, atteso che tali sistemi «possono basarsi su informazioni che finiscono con l'alimentare una sorta di circolo vizioso, per cui alla fine, ad essere criminalizzata, è la povertà»[47].

Inoltre, come evidenziato dal Regolamento europeo sull'intelligenza artificiale, «tenuto conto del loro ruolo e della loro responsabilità, le azioni delle autorità di contrasto che prevedono determinati usi dei sistemi di IA sono caratterizzate da un livello significativo di squilibrio di potere e possono portare alla sorveglianza, all'arresto o alla privazione della libertà di una persona fisica, come pure avere altri impatti negativi sui diritti fondamentali garantiti nella Carta»[48].

---

[46] Cfr., cons. 42), Reg. UE 2024/1689.

[47] D'ALOIA, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in AA.VV., *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, D'Aloia (a cura di), Milano, 2020, p. 35.

[48] Cfr., cons. 59), Reg. UE 2024/1689.

In dottrina, più in generale, sul concetto di asimmetria di potere che potrebbe derivare dall'uso di *software* di *AI*, non solo da parte delle autorità di contrasto ma anche ad opera dei magistrati, LA REGINA, *I.A. e ragionamento giuridico: la giustizia prevedibile*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, Baccari - Felicioni (a cura di), Milano, 2023, p. 177, secondo la quale si ripercuoterebbe «in maniera inesorabile tanto sul diritto dell'interessato a ricostruire il ragionamento del giudice che si sia avvalso del risultato algoritmico quanto sull'area di quei diritti che declinano lo statuto di un giusto processo». Sul punto anche QUATTROCOLO, *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *MediaLaws*, 3, 2020, p. 127, la quale evidenzia che, «invero, lo squilibrio conoscitivo è fenomeno che si riscontra nel processo penale sin da quando, per la soluzione di casi complessi, si è iniziato a fare ricorso a competenze tecniche, scientifiche o artistiche».

Eccezione consentita dal legislatore comunitario è quella che riconduce alcuni strumenti predittivi utilizzati dalle autorità di contrasto alla categoria dell'*AI* "ad alto rischio" *ex* art. 6 del Regolamento, dunque, ammessi con "riserva".

In questa categoria rientrano i sistemi «per determinare il rischio per una persona fisica di diventare vittima di reati», di macchine «come poligrafi e strumenti analoghi», di applicativi «per valutare l'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati», di *software* «per determinare il rischio di commissione del reato o di recidiva in relazione a una persona fisica non solo sulla base della profilazione delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 o per valutare i tratti e le caratteristiche della personalità o il comportamento criminale pregresso di persone fisiche o gruppi» nonché di algoritmi per «effettuare la profilazione delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 nel corso dell'indagine, dell'accertamento e del perseguimento di reati»[49].

Per tali modelli computazionali è, dunque, necessario verificare la sussistenza di determinati requisiti dettati *ex lege*[50]: tra questi vi è la elevata qualità dei dati, il soddisfacimento degli *standard* di prestazione, accuratezza o robustezza, l'adeguata progettazione e verificazione dei modelli affinché non ci sia il rischio che profilino e individuino le persone in modo discriminatorio, errato o ingiusto.

Ex adverso, ammettendone l'utilizzo indiscriminato verrebbe «ostacolato l'esercizio di importanti diritti procedurali fondamentali […] nel caso in cui tali sistemi di IA non siano sufficientemente trasparenti, spiegabili e documentati».

Da qui, la classificazione come sistemi "ad alto rischio", precisando che «l'accuratezza, l'affidabilità e la trasparenza risultano particolarmente importanti per evitare impatti negativi, mantenere la fiducia dei cittadini e garantire la responsabilità e mezzi di ricorso efficaci»[51].

Neppure può essere ignorato l'impatto dei *predictive policing* sul diritto di difesa dell'indagato, in ragione della difficoltà nel reperire «informazioni significative sul

[49] Cfr. All. III, § 1, n. 6), Reg. UE 2024/1689,
[50] Sul punto, *supra*, Cap. I, § 4.
[51] Cfr., cons. 59), Reg. UE 2024/1689

funzionamento di tali sistemi e la difficoltà che ne risulta nel confutarne i risultati in tribunale»[52].

In sostanza, «bisogna evitare il rischio che l'ampliamento delle "indagini digitali" quale frutto degli strumenti di intelligenza artificiale possa aumentare il rischio di radicalizzare questa deriva del processo inquisitorio=autoritario»[53], consegnando il processo nella mani del pubblico ministero, come peraltro già da qualche anno accade.

Dunque, dinanzi a questo scenario composito, occorre soppesare attentamente rischi e benefici mettendo a punto un solido apparato normativo di tipo nazionale che, muovendosi sul sentiero tracciato dal legislatore europeo, sia in grado di tutelare a tutto tondo i diritti – processuali e non − della persona coinvolta nella valutazione algoritmica; allo stesso tempo, però, si dovrebbe poter sfruttare al massimo le potenzialità offerte dall'*AI* in termini di completezza delle indagini e riduzione dei tempi di durata delle medesime.

3. Agli esordi del riconoscimento facciale.

L'esigenza di agevolare l'identificazione di indagati e imputati a fini procedimentali attraverso la raccolta di dati biometrici risale al XVII secolo, quando Eliseo Masini[54], noto inquisitore, esortava ad annotare in maniera dettagliata i tratti somatici degli autori di condotte criminose affinché, in futuro, fosse più agevole il loro riconoscimento.

Il bisogno di perfezionare tale opera di memorizzazione della fisionomia dei prevenuti con l'ausilio di un metodo scientifico è stato avvertito pure nell'Ottocento, periodo storico in cui autorevoli criminologi hanno avviato i primi studi in materia, fondando l'antropometria.

Oggi, grazie all'avvento dell'*AI*, un ulteriore passo in avanti è stato compiuto con l'introduzione dei sistemi di riconoscimento facciale[55].

---

[52] Cfr., cons. 59), Reg. UE 2024/1689.

[53] RICCIO, *Ragionando su intelligenza artificiale e processo penale*, cit., p. 8.

[54] Lo cita DELLA TORRE, *Quale spazio per i* tools *di riconoscimento facciale nella giustizia penale?*, in AA.VV., *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, Di Paolo - Presacco (a cura di), Napoli, 2022, pp. 13-14 e nota n. 31.

[55] Per una panoramica sull'utilizzo di tali sistemi a livello globale, si veda il seguente *link*, www.privacyinternational.org/examples/predictivepolicing.

Si sta, infatti, delineando una nuova frontiere investigativa dominata da «*artificial agents*»[56] basati sull'identificazione biometrica[57] che operano in *real-time* o in differita: analizzano il volto di un soggetto, non identificato, ritratto in una foto o in un video e lo associano, poi, ad un preciso individuo, "pescandone" l'identità nel *database* di cui sono dotati.

Operano mediante algoritmi capaci di individuare precisi punti biometrici sul volto del soggetto da esaminare, così da ricavarne l'impronta facciale (*faceprint*), individuata grazie ad uno studio dei tratti somatici come la distanza degli occhi, la conformazione nasale, la struttura del mento e delle orecchie.

Ogni esaltazione della tecnologia al servizio della giustizia penale, però, deve scontrarsi con la realtà e con i tipici rischi legati all'uso dell'*AI*.

Fra tutti vi è il principio di generale fallibilità della macchina: l'errore, infatti, può avvenire a causa di fattori endogeni, quali la scarsa qualità dell'immagine o del *frame* da analizzare, o esogeni, come un "allenamento" dell'algoritmo non adeguato.

Tale orizzonte prospettico induce a ritenere che l'impatto dei *software* di riconoscimento facciale potrebbe rivelarsi asimmetrico, incidendo in modo significativamente più severo su di una minoranza di soggetti attraverso la riproduzione di tendenze razziste determinate dell'immissione di dati di addestramento non neutrali.

L'efficacia di tali algoritmi è, infatti, già stata messa in discussione quando, durante la finale di *UEFA Champions League* di Cardiff del 2017, «oltre 2.000 persone innocenti sono state identificate quali possibili criminali da un *tool* di *facial recognitions*»[58].

Il dibattito mondiale circa l'utilizzabilità di tali applicativi in sede investigativa ha raggiunto l'apice con lo scandalo "*Clearview AI*".

In dottrina, si veda, tra i tanti, DELLA TORRE, *Quale spazio per i* tools *di riconoscimento facciale nella giustizia penale?*, in AA.VV., *Intelligenza artificiale e processo penale*, cit., pp. 7 ss.; TORRE, *Intelligenza artificiale e indagini penali: prospettive future e garanzie di sistema. Il sistema automatico di riconoscimento immagini*, in AA.VV., *Cybercrime*, Cadoppi - Canestrari - Manna - Papa (diretto da), Milano, 2023, pp. 1731 ss.

[56] Così, FLORIDI - SANDERS, *On the Morality of Artificial Agents*, in *Minds and Machines*, 2004, p. 349.

[57] Cfr. art. 3, n. 35), Reg. UE 2024/1689.

[58] DELLA TORRE, *Quale spazio per i* tools *di riconoscimento facciale nella giustizia penale?*, cit., p. 18.

Tale *software*, utilizzato da oltre 2.400 agenzie di polizia (tra cui l'FBI) utilizzava una *app* di riconoscimento facciale dotata di un *dataset* illegittimo poiché si nutriva di dati biometrici "rubati" dai *social network* come *Facebook*, *Twitter*, *Instagram* e altre applicazioni analoghe.

Sul punto si è espresso anche il Garante della *privacy* che, nel febbraio 2022, ha imposto alla società creatrice una sanzione di ben 20 milioni di euro, atteso che dall'istruttoria è stato accertato l'illecito tracciamento anche di cittadini italiani e di persone collocate nel territorio nazionale[59].

In particolare, i dati personali detenuti dalla società, inclusi quelli biometrici e di geo-localizzazione, sono stati tratti, senza consenso degli interessati, da piattaforme digitali, in palese violazione della normativa vigente; ciò in quanto le fotografie postate sui profili virtuali di ognuno, seppur pubbliche, non sono state immesse in rete con lo scopo di essere impiegate per finalità investigative.

Memore di tale esperienza, il legislatore europeo con il Regolamento sull'*AI*, ha posto il divieto di ampliare le banche dati biometriche «mediante *scraping* non mirato di immagini facciali da *internet* o da filmati di telecamere a circuito chiuso» poiché «tale pratica accresce il senso di sorveglianza di massa e può portare a gravi violazioni dei diritti fondamentali, compreso il diritto alla vita privata»[60].

Considerate le enormi potenzialità dell'*AI*, anche nel territorio italiano si è provato, a livello ministeriale, a introdurre – pur non senza resistenze − un sistema di riconoscimento facciale noto come SARI (Sistema Automatico di Riconoscimento delle Immagini).

Impiegato dal 2017 dalla Polizia di Stato, a Brescia ha rivelato le sue capacità: analizzando i *frame* delle videoregistrazioni dalle telecamere presenti nell'abitazione nella quale è avvenuto il furto, è stato possibile risalire alle generalità dei malviventi responsabili del delitto.

L'applicativo lavora sulla base di due algoritmi che, attraverso l'identificazione biometrica, rapportano l'identità ignota di un soggetto raffigurato in una immagine fotografica a milioni di soggetti ritratti in foto segnaletiche contenute nel *database*.

---

[59] Si veda l'Ordinanza di ingiunzione nei confronti di *Clearview AI* del 10 febbraio 2022, n. 9751362, consultabile al *link* https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9751362.

[60] Cfr., cons. 43), Reg. UE 2024/1689.

Tale sistema può operare in modalità *enterprise* o *real-time*.

La prima prevede la ricerca dell'identità di un volto staticamente raffigurato in una immagine, attraverso l'analisi di ben due schedari (una di circa dieci milioni di immagini[61] e l'altra ricca di impronte digitali e dati anagrafici[62]).

La seconda, invece, agevola l'attività di controllo del territorio, offrendo un'analisi in tempo reale delle immagini che vengono comparate con la c.d. *watch list*; inserita l'immagine di interesse, il programma la analizza e produce una *candidate list* ovvero un elenco di profili a cui viene assegnato un punteggio di compatibilità rispetto all'effettivo autore del reato.

Al fine di promuoverne l'utilizzo nel contesto procedimentale nazionale, si potrebbero ricondurre tali applicativi nell'alveo dell'art. 189 c.p.p.[63], trattandosi di attività investigative effettuate attraverso strumenti atipici quali i *software* di riconoscimento facciale.

In sostanza, si potrebbe pensare di agganciarli ai classici referenti codicistici dell'identificazione (art. 349 c.p.p.), dell'individuazione (art. 361 c.p.p.), della ricognizione formale (art. 213 ss. c.p.p.) e del riconoscimento fotografico con l'aggiunta di un elemento di novità costituito, per l'appunto, dall'algoritmo.

Tuttavia, il dibattito interno è nettamente polarizzato.

Da un lato, le forze di polizia esaltano questa nuova tecnologia, considerandola una importantissima innovazione e, dall'altro lato, il Garante della *privacy*, dopo aver svolto ben due istruttorie sulla compatibilità di tale sistema con i diritti fondamentali dell'individuo, ha posto un freno agli entusiasmi.

Con provvedimento del 25 marzo 2021 il Garante della *privacy* ha ritenuto che il trattamento di immagini per identificare le persone nel contesto pubblico è estremamente delicato e necessita di una ponderata valutazione d'insieme, che non muti in maniera irreversibile la relazione tra individuo ed autorità. Prosegue

---

[61] Si tratta, secondo le indicazioni del Ministero, della banca dati *AFIS* (*Automated Fingerprint Identification System*), che contiene 18 milioni di cartellini segnaletici.

[62] L'immagine fotografica, infatti, viene inserita nel sistema e filtrata in meno di 1 minuto.

[63] Sul concetto di prova atipica anche CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Diritto penale e processo*, 2018, p. 1211, secondo cui l'evoluzione tecnologica potrebbe fare il suo ingresso nei meccanismi della giustizia attraverso l'art. 189 c.p.p., aggiungendo però che detta norma «non è tale da alterare i connotati del disegno complessivo: essa stabilisce che la prova innominata entra nel processo penale se è idonea ad accertare e non lede la libertà morale, previo contraddittorio dinanzi al giudice».

precisando che «occorre in particolare considerare che il sistema in argomento realizza un trattamento automatizzato su larga scala che può riguardare, tra l'altro, anche coloro che siano presenti a manifestazioni politiche e sociali, che non sono oggetto di "attenzione" da parte delle forze di Polizia».

Per cui se pure la «valutazione di impatto indica che i dati di questi ultimi sarebbero immediatamente cancellati, nondimeno, l'identificazione di una persona in un luogo pubblico comporta il trattamento biometrico di tutte le persone che circolano nello spazio pubblico monitorato, al fine di generare i modelli di tutti per confrontarli con quelli delle persone incluse nella "*watch-list*"». Tale condizione non è accettabile poiché «determina una evoluzione della natura stessa dell'attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale»[64].

Tuttavia, deve darsi atto che «l'impianto codicistico non abbia retto all'"urto" della prassi»[65].

Dunque, per superare ogni criticità, il Ministero ha provato a consentire l'impiego di SARI, a codice invariato, per scopi investigativi e probatori, facendo leva su una diversa interpretazione del dato codicistico che, comunque, non si è dimostrata persuasiva.

Secondo la soluzione prospettata il "combinato disposto" tra esito del *tool* e conferma dell'operatore umano andrebbe catalogato in seno alla categoria degli accertamenti tecnici *ex* art. 359 c.p.p. e non tra le evidenze probatorie atipiche[66].

Tuttavia, lo stato di incertezza e criticità derivante dall'impiego di *facial recognition system* ha comportato lo sviluppo di «un ampio ed eterogeneo movimento di pensiero, teso a frenare l'avanzata delle "tecnologie del controllo" in ambito penale»[67].

---

[64] Per ulteriori approfondimenti, si veda il testo integrale del Parere del Garante della *privacy* sul sistema *Sari Real Time* del 25 marzo 2021, n. 9575877, disponibile al *link* https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575877.

[65] In questi termini, DELLA TORRE, *Quale spazio per i* tools *di riconoscimento facciale nella giustizia penale?*, cit., p. 31.

[66] Cfr., DELLA TORRE, *Quale spazio per i* tools *di riconoscimento facciale nella giustizia penale?*, cit., p. 40.

[67] Così, DELLA TORRE, *Quale spazio per i* tools *di riconoscimento facciale nella giustizia penale?*, cit., p. 25.

Dunque, pur non escludendo a priori l'impiego di strumenti di identificazione biometrica, si ritiene opportuno imporre garanzie minime per salvaguardare i diritti fondamentali dell'uomo.

È questo, infatti, l'approccio adottato del legislatore europeo che con l'*AI Act* tenta di fare chiarezza: dapprima offre una definizione di dati biometrici[68], di identificazione biometrica[69] e di categorizzazione biometrica[70]; poi distingue tra «sistema di identificazione biometrica remota»[71], «sistema di identificazione

[68] Cfr., cons. 14), Reg. UE 2024/1689, secondo cui «la nozione di "dati biometrici" utilizzata nel presente regolamento dovrebbe essere interpretata alla luce della nozione di dati biometrici di cui all'articolo 4, punto 14, del regolamento (UE) 2016/679, all'articolo 3, punto 18, del regolamento (UE) 2018/172 e all'articolo 3, punto 13, della direttiva (UE) 2016/680. I dati biometrici possono consentire l'autenticazione, l'identificazione o la categorizzazione delle persone fisiche e il riconoscimento delle emozioni delle persone fisiche» e art. 3, n. 34), Reg. UE 2024/1689, «i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali le immagini facciali o i dati dattiloscopici».

[69] Cfr., cons. 15), Reg. UE 2024/1689, che fa riferimento al «riconoscimento automatico di caratteristiche fisiche, fisiologiche e comportamentali di una persona, quali il volto, il movimento degli occhi, la forma del corpo, la voce, la prosodia, l'andatura, la postura, la frequenza cardiaca, la pressione sanguigna, l'odore, la pressione esercitata sui tasti, allo scopo di determinare l'identità di una persona confrontando i suoi dati biometrici con quelli di altri individui memorizzati in una banca dati di riferimento, indipendentemente dal fatto che la persona abbia fornito il proprio consenso. Sono esclusi i sistemi di IA destinati a essere utilizzati per la verifica biometrica, che include l'autenticazione, la cui unica finalità è confermare che una determinata persona fisica è la persona che dice di essere e confermare l'identità di una persona fisica al solo scopo di accedere a un servizio, sbloccare un dispositivo o disporre dell'accesso di sicurezza a locali» e art. 3, n. 35), Reg. UE 2024/1689, secondo cui trattasi del «riconoscimento automatizzato delle caratteristiche umane fisiche, fisiologiche, comportamentali o psicologiche allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di individui memorizzati in una banca dati».

[70] Cfr., cons. 16), Reg. UE 2024/1689, che la definisce come «l'assegnazione di persone fisiche a categorie specifiche sulla base dei loro dati biometrici. Tali categorie specifiche possono riguardare aspetti quali il sesso, l'età, il colore dei capelli, il colore degli occhi, i tatuaggi, i tratti comportamentali o di personalità, la lingua, la religione, l'appartenenza a una minoranza nazionale, l'orientamento sessuale o politico. Ciò non comprende i sistemi di categorizzazione biometrica che sono una caratteristica puramente accessoria intrinsecamente legata a un altro servizio commerciale, il che significa che l'elemento non può, per ragioni tecniche oggettive, essere utilizzato senza il servizio principale e che l'integrazione di tale caratteristica o funzionalità non rappresenta un mezzo per eludere l'applicabilità delle norme del presente regolamento. Ad esempio, i filtri che classificano le caratteristiche facciali o del corpo utilizzate sui mercati online potrebbero costituire una tale caratteristica accessoria, in quanto possono essere utilizzati solo in relazione al servizio principale che consiste nel vendere un prodotto consentendo al consumatore di visualizzare in anteprima il prodotto su sé stesso e aiutarlo a prendere una decisione di acquisto. Anche i filtri utilizzati nei servizi di *social network* online che classificano le caratteristiche facciali o del corpo per consentire agli utenti di aggiungere o modificare immagini o video potrebbero essere considerati una caratteristica accessoria, in quanto tale filtro non può essere utilizzato senza il servizio principale dei servizi di social network consistente nella condivisione di contenuti online» e art. 3, n. 40), Reg. UE 2024/1689, che parla di «un sistema di IA che utilizza i dati biometrici di persone fisiche al fine di assegnarle a categorie specifiche, a meno che non sia accessorio a un altro servizio commerciale e strettamente necessario per ragioni tecniche oggettive».

[71] Cfr., cons. 17), Reg. UE 2024/1689, secondo cui «è opportuno definire a livello funzionale la nozione di "sistema di identificazione biometrica remota" di cui al presente regolamento, quale

biometrica remota "in tempo reale"»[72] e, con una nozione ricavata *a contrario*, «sistema di identificazione biometrica remota a posteriori»[73].

Il Regolamento stabilisce un generale divieto di avvalersi di sistemi di categorizzazione biometrica basati sui dati «quali il volto o le impronte digitali, per trarre deduzioni o inferenze in merito alle opinioni politiche, all'appartenenza sindacale, alle convinzioni religiose o filosofiche, alla razza, alla vita sessuale o all'orientamento sessuale di una persona»[74]; vietato è pure l'impiego di sistemi di identificazione biometrica remota "in tempo reale" delle persone fisiche in spazi accessibili al pubblico a fini di attività di contrasto, atteso che si tratta di impieghi estremamente invasivi dei diritti e delle libertà dei soggetti coinvolti «nella misura in cui potrebbe avere ripercussioni sulla vita privata di un'ampia fetta della popolazione», facendola sentire «costantemente sotto sorveglianza», scoraggiando così «in maniera indiretta l'esercizio della libertà di riunione e di altri diritti fondamentali»[75].

---

sistema di IA destinato all'identificazione, tipicamente a distanza, di persone fisiche senza il loro coinvolgimento attivo mediante il confronto dei dati biometrici di una persona con i dati biometrici contenuti in una banca dati di riferimento, a prescindere dalla tecnologia, dai processi o dai tipi specifici di dati biometrici utilizzati. Tali sistemi di identificazione biometrica remota sono generalmente utilizzati per percepire più persone o il loro comportamento simultaneamente al fine di facilitare in modo significativo l'identificazione di persone fisiche senza il loro coinvolgimento attivo. Sono esclusi i sistemi di IA destinati a essere utilizzati per la verifica biometrica, che include l'autenticazione, la cui unica finalità è confermare che una determinata persona fisica è la persona che dice di essere e confermare l'identità di una persona fisica al solo scopo di accedere a un servizio, sbloccare un dispositivo o disporre dell'accesso di sicurezza a locali. Tale esclusione è giustificata dal fatto che detti sistemi hanno probabilmente un impatto minore sui diritti fondamentali delle persone fisiche rispetto ai sistemi di identificazione biometrica remota, che possono essere utilizzati per il trattamento dei dati biometrici di un numero elevato di persone senza il loro coinvolgimento attivo. Nel caso dei sistemi "in tempo reale", il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono tutti istantaneamente, quasi istantaneamente o in ogni caso senza ritardi significativi. A tale riguardo è opportuno impedire l'elusione delle regole del presente reg. per quanto attiene all'uso "in tempo reale" dei sistemi di IA interessati prevedendo ritardi minimi. I sistemi "in tempo reale" comportano l'uso di materiale "dal vivo" o "quasi dal vivo" (ad esempio filmati) generato da una telecamera o da un altro dispositivo con funzionalità analoghe. Nel caso dei sistemi di identificazione a posteriori, invece, i dati biometrici sono già stati rilevati e il confronto e l'identificazione avvengono solo con un ritardo significativo. Si tratta di materiale, come immagini o filmati generati da telecamere a circuito chiuso o da dispositivi privati, che è stato generato prima che il sistema fosse usato in relazione alle persone fisiche interessate».

[72] Cfr., art. 3, n. 42), Reg. UE 2024/1689: trattasi di «un sistema di identificazione biometrica remota in cui il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono senza ritardi significativi, il quale comprende non solo le identificazioni istantanee, ma anche quelle che avvengono con brevi ritardi limitati al fine di evitare l'elusione».

[73] Si veda, art. 3, n. 43), Reg. UE 2024/1689, che lo definisce come «un sistema di identificazione biometrica remota diverso da un sistema di identificazione biometrica remota "in tempo reale"».

[74] Cfr., cons. 30), Reg. UE 2024/1689.

[75] Cfr., cons. 32), Reg. UE 2024/1689.

Ciò in quanto «le inesattezze di carattere tecnico dei sistemi di IA destinati all'identificazione biometrica remota delle persone fisiche possono determinare risultati distorti e comportare effetti discriminatori»; a ciò si aggiunga che «l'immediatezza dell'impatto e le limitate opportunità di eseguire ulteriori controlli o apportare correzioni in relazione all'uso di tali sistemi che operano "in tempo reale" comportano inoltre un aumento dei rischi per quanto concerne i diritti e le libertà delle persone interessate nell'ambito delle attività di contrasto, o che sono da queste condizionate»[76].

All'interno della c.d. "piramide dei rischi" tracciata dall'*AI Act* i *software* di *facial recognition* occupano un ruolo privilegiato, costituendo una sorta di intercapedine tra la categoria delle «pratiche vietate» e quella delle «pratiche ad alto rischio»[77].

Tale impostazione consente di ammettere un'eccezione al generale divieto di identificazione biometrica "in tempo reale" «per perseguire un interesse pubblico rilevante»[78].

Dunque, in determinate situazioni, definite in maniera puntuale e rigorosa dal legislatore comunitario[79], è consentito utilizzare tali sistemi per attività di *law enforcement* finalizzate alla ricerca di determinate vittime di reato e di persone scomparse, nei casi di minacce alla vita e all'incolumità delle persone fisiche, nelle ipotesi di un attacco terroristico ovvero per la localizzazione o l'identificazione di

---

[76] Cfr., cons. 32), Reg. UE 2024/1689.

[77] Cfr., cons. 54), Reg. UE 2024/1689, «poiché i dati biometrici costituiscono una categoria particolare di dati personali, è opportuno classificare come ad alto rischio diversi casi di uso critico di sistemi biometrici, nella misura in cui il loro uso è consentito dal pertinente diritto dell'Unione e nazionale. Le inesattezze di carattere tecnico dei sistemi di IA destinati all'identificazione biometrica remota delle persone fisiche possono determinare risultati distorti e comportare effetti discriminatori. Il rischio di tali risultati distorti ed effetti discriminatori è particolarmente importante per quanto riguarda l'età, l'etnia, la razza, il sesso o le disabilità. I sistemi destinati all'identificazione biometrica remota dovrebbero pertanto essere classificati come ad alto rischio in considerazione dei rischi che comportano. Tale classificazione esclude i sistemi di IA destinati a essere utilizzati per la verifica biometrica, inclusa l'autenticazione, la cui unica finalità è confermare che una determinata persona fisica è chi dice di essere e confermare l'identità di una persona fisica al solo scopo di accedere a un servizio, sbloccare un dispositivo o disporre dell'accesso sicuro a locali. Inoltre, è opportuno classificare come ad alto rischio i sistemi di IA destinati a essere utilizzati per la categorizzazione biometrica in base ad attributi o caratteristiche sensibili protetti a norma dell'articolo 9, paragrafo 1, del regolamento (UE) 2016/679 sulla base di dati biometrici, nella misura in cui non sono vietati a norma del presente regolamento, e i sistemi di riconoscimento delle emozioni che non sono vietati a norma del presente regolamento. I sistemi biometrici destinati a essere utilizzati al solo scopo di consentire la cybersicurezza e le misure di protezione dei dati personali non dovrebbero essere considerati sistemi di IA ad alto rischio».

[78] Cfr., cons. 33), Reg. UE 2024/1689.

[79] Si veda, art. 5, § 1, lett. h), Reg. UE 2024/1689.

autori di reati o sospettati di delitti di cui all'Allegato II[80] del Regolamento, se tali fattispecie criminose sono punite nello Stato membro interessato con una pena edittale non inferiore a quattro anni. Ciò in quanto detta soglia «contribuisce a garantire che il reato sia sufficientemente grave da giustificare potenzialmente l'uso di sistemi di identificazione biometrica remota "in tempo reale"»[81].

In tali casi, l'impiego per attività di contrasto di sistemi di riconoscimento facciale in *real time*, preventivamente autorizzato dall'autorità giudiziaria o da un'autorità amministrativa indipendente[82], in spazi aperti al pubblico, dovrebbe essere limitato a confermare l'identità della persona interessata, nel rispetto di determinate coordinate spazio-temporali[83].

Invece, nell'ipotesi in cui si debba procedere con soluzioni di *law enforcement* che prevedono l'uso di sistemi di identificazione biometrica a posteriori − purché tale attività sia documentata nel relativo fascicolo di polizia, poi messo a disposizione delle competenti autorità − è necessario che il *deployer* chieda un'autorizzazione «*ex ante* o senza indebito ritardo ed entro 48 ore, da parte di un'autorità giudiziaria o amministrativa la cui decisione è vincolante e soggetta a controllo giurisdizionale»[84]; se respinta, l'impiego del *software* collegato alla richiesta è immediatamente interrotto e i dati personali collegati cancellati.

Ad ogni buon conto, il Regolamento precisa che in nessun caso è possibile utilizzare un sistema di identificazione biometrica remota *ex post* per «fini di contrasto in modo non mirato, senza alcun collegamento con un reato, un procedimento penale, una minaccia reale e attuale o reale e prevedibile di un reato o la ricerca di una determinata persona scomparsa», atteso che «occorre garantire che nessuna

---

[80] L'allegato, suscettibili di aggiornamento, fa riferimento ai seguenti reati: «terrorismo; tratta di esseri umani; sfruttamento sessuale di minori e pornografia minorile; traffico illecito di stupefacenti o sostanze psicotrope; traffico illecito di armi, munizioni ed esplosivi; omicidio volontario, lesioni gravi; traffico illecito di organi e tessuti umani; traffico illecito di materie nucleari e radioattive; sequestro, detenzione illegale e presa di ostaggi; reati che rientrano nella competenza giurisdizionale della Corte penale internazionale; illecita cattura di aeromobile o nave, violenza sessuale; reato ambientale; rapina organizzata o a mano armata; sabotaggio; partecipazione a un'organizzazione criminale coinvolta in uno o più dei reati elencati sopra».

[81] Cfr., cons. 33), Reg. UE 2024/1689.

[82] Cfr., cons. 35), Reg. UE 2024/1689

[83] Cfr., cons. 34), Reg. UE 2024/1689.

[84] Cfr. art. 26, § 10, Reg. UE 2024/1689 che pone un'eccezione a tale meccanismo autorizzativo quando il sistema sia «utilizzato per l'identificazione iniziale di un potenziale sospetto sulla base di fatti oggettivi e verificabili direttamente connessi al reato», precisando che «ogni uso è limitato a quanto strettamente necessario per le indagini su uno specifico reato».

decisione che produca effetti giuridici negativi su una persona possa essere presa dalle autorità di contrasto unicamente sulla base dell'*output* di tali sistemi»[85].

Tra l'altro, la «natura invasiva dei sistemi di identificazione biometrica remota a posteriori»[86] impone che l'uso di tali sistemi sia soggetto a tutele.

In particolare, «dovrebbero sempre essere utilizzati in modo proporzionato, legittimo e strettamente necessario e quindi mirato, per quanto riguarda le persone da identificare, il luogo e l'ambito temporale» purché ciò avvenga «sulla base di un *set* di dati chiuso di filmati acquisiti legalmente» e non per finalità di «sorveglianza indiscriminata»[87].

Ad ogni buon conto, il trattamento di dati biometrici a scopo di contrasto deve avvenire, sempre che sia strettamente necessario, in conformità a quanto stabilito dal Regolamento[88] che, sul punto, opera anche un rinvio esterno all'art. 10, Direttiva (UE) 2016/680.

Tale disciplina generale può essere, però, disattesa (soltanto) *in peius* dai singoli Stati membri, che restano liberi «di non prevedere affatto tale possibilità o di prevederla soltanto per alcuni degli obiettivi idonei a giustificare l'uso autorizzato di cui nel presente regolamento»[89].

L'ultima parola resta, dunque, al legislatore nazionale, che realizzando un delicato bilanciamento tra esigenze opposte deve «da un lato, da salvaguardare il "nucleo essenziale" del diritto e, dall'altro lato, da consentire, entro certi limiti, l'impiego di nuovi strumenti investigativi in grado di fornire un contributo importantissimo alle indagini»[90].

Tuttavia, è evidente come il Parlamento italiano si sia dimostrato restio ad ammettere l'ingresso di soluzioni algoritmiche nel procedimento penale, escludendone ogni possibile applicazione anche nella fase delle indagini preliminari. Un atteggiamento di questo tipo si potrebbe rivelare controproducente,

---

[85] Cfr. art. 26, § 10, Reg. UE 2024/1689, chiarisce altresì che «gli Stati membri possono introdurre, in conformità del diritto dell'Unione, disposizioni più restrittive sull'uso dei sistemi di identificazione biometrica remota a posteriori».

[86] Cfr., cons. 95), Reg. UE 2024/1689.

[87] Cfr., cons. 95), Reg. UE 2024/1689.

[88] Cfr., cons. 94), Reg. UE 2024/1689.

[89] Cfr., cons. 37), Reg. UE 2024/1689.

[90] Così, TORRE, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Diritto penale e processo*, 2021, p. 1043.

sabotando il tentativo di adeguamento della giustizia e, in particolare delle tecniche investigative, rispetto ai mutamenti della società e della tecnologia.

Nel fosco e complesso quadro giuridico delineato, dunque, pare opportuno ammettere l'impiego di sistemi algoritmici nella c.d. "istruzione primaria" o – volendo recuperare la nota "teoria dei contesti" – all'interno del "contesto di scoperta" finalizzato «all'individuazione delle fonti e degli elementi di prova utili per le determinazioni concernenti l'esercizio dell'azione penale»[91], purché siano sviluppati in ossequio alla logica delle indagini, nel rispetto della rigida regolamentazione europea e (*de iure condendo*) nazionale.

4. L'impiego probatorio dell'*AI*.

Anche sul versante probatorio[92], al netto dei possibili impieghi dei *tools* di riconoscimento facciale e di *predictive policing*, possono essere individuati diversi spazi applicativi per l'*AI*: oltre ai meccanismi artificiali utilizzati come mezzo di ricerca della prova[93], merita approfondimento il tema della valutazione algoritmica della prova e quello c.d. *digital evidence*[94].

Pur senza eludere i principi fondamentali dell'ordinamento giuridico in materia probatoria[95], si è parlato delle c.d. "prove algoritmiche" in senso stretto ovvero di quei dati probatori generati automaticamente attraverso applicativi di *AI*[96], che costituiscono la naturale evoluzione della frontiera delle "prove tecnologiche"[97].

---

[91] PRESACCO, *Intelligenza artificiale e ragionamento probatorio nel processo penale*, in AA.VV., *Intelligenza artificiale e processo penale*, cit., p. 113.

[92] In argomento, *ex multis*, SALLANTIN - SZCZECINIARZ (a cura di), *Il concetto di prova alla luce dell'intelligenza artificiale*, Milano, 2005.

[93] In argomento, BACCARI - PECCHIOLI, *I.A. e giudizio sul fatto: gli strumenti di* e-evidence *per la cognizione*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, cit., pp. 118-119. Sull'utilizzo della *chatbot*, sino ad ora ricondotti dalla dottrina al paradigma dei mezzi di ricerca della prova, BACCARI - MARRAFFINO, *Le prospettive di utilizzo delle* chatbot *nel procedimento penale*, in *Diritto penale e processo*, 2021, pp. 1008 ss.

[94] In argomento, si veda, LORUSSO, Digital evidence*,* cybercrime *e giustizia penale 2.0*, in *Processo penale e giustizia*, 2019, pp. 821 ss.

[95] GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, cit., p. 56, che richiama, da un lato, i diritti e le garanzie «che tutelano la sfera intima dell'individuo, erigendo una barriera, uno scudo protettivo rispetto alle intrusioni esterne» (artt. 14 e 15 Cost., 8 CEDU e 7 Carta di Nizza), nonché, dall'altro, «quelle garanzie che assicurano un confronto dialettico paritario e una verifica sull'attendibilità della fonte di prova (artt. 111, commi 2, 3 e 4, Cost. e 6 CEDU).

[96] QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Springer, 2020, pp. 73 ss.

[97] Si pensi alla disciplina dei "dati" esterni di una comunicazione telefonica (durata, localizzazione dei dispositivi impiegati e soggetti coinvolti) che, sebbene raccolti dai gestori telefonici per finalità

In effetti, il legame tra *digital evidence* e *governance* algoritmica sta diventando sempre più stretto, atteso che i dispositivi domotici presenti nelle abitazioni di ciascuno di noi potrebbero offrire dettagliate informazioni sull'evento delittuoso consumato tra le mura domestiche.

È quanto avvenuto nel noto "caso *Alexa*", conosciuto come il primo processo in cui vi è stata una "testimonianza digitale"[98].

In particolare, il caso risale al 2015, quando, in Arkansas, James Bates è stato accusato dell'omicidio di primo grado di Victor Collins trovato nella sua vasca idromassaggio, in cui la polizia ha sequestrato il dispositivo *Alexa* come prova; le rivelazioni dell'assistente vocale presente sulla scena del delitto, considerate alla stregua di "dichiarazioni" testimoniali, sono risultate utili per la ricostruzione della dinamica del reato.

Quale anno dopo, nel 2017, in un altro procedimento relativo all'omicidio di due donne, Christine Sullivan e Jenna Pellegrini, accoltellate a Timothy Verrill, Farmingto, il giudice del New Hampshire ha ordinato ad *Amazon* di fornire registrazioni dal dispositivo *Alexa* per trarre elementi utili ad accertare i fatti.

Nel tentativo di negare valore probatorio alle informazioni contenute nel *software*, si potrebbe opporre la *Hearsay's Rule* che limita l'ammissibilità del contributo dichiarativo umano unicamente a ciò che è stato percepito dal testimone con i propri sensi[99].

Al contrario, la giurisprudenza americana tende ad escludere che le informazioni generate da algoritmi siano frutto di "sentito dire" e, per tale ragione, non risultano soggette a tale *exclusionary rule* e, dunque, sono utilizzabili nel processo.

---

aziendali, possono essere impiegati nel processo penale; ad un elettrodomestico che, rilevando la temperatura interna dell'ambiente in cui si trova, può fornire informazioni sulla presenza di determinate persone sulla scena del crimine; alle scatole nere delle autovetture o gli assistenti vocali virtuali, che producono prove documentali dalla formidabile efficacia rappresentativa.

[98] In argomento, si veda, ATERNO, Alexa *testimone in tribunale: i vantaggi per gli investigatori e le garanzie per la difesa*, cit.; PARISE, *"Alexa, chi è l'assassino?": anche in Italia gli smartspeaker potrebbero essere testimoni*, in *Agenda Digitale online*, 22 novembre 2019.

[99] ROTH, *The Use of Algorithms in Criminal Adjudication*, cit., p. 419, precisa che «*"Hersay" is an out-of-court statement by a human declarant, offender to prove the truth of the matter asserted by the declarant, and is presumptively inadmissible in American trials*».

Anche nel processo penale italiano vale la medesima regola, codificata all'art. 195 c.p.p. che disciplina l'ipotesi di testimonianza indiretta o *de relato* e impone peculiari limiti di utilizzabilità di tali dichiarazioni.

Pur tralasciando il discorso relativo ai limiti probatori che potrebbero essere opposti nel nostro ordinamento giuridico all'acquisizione di una prova generata dall'*AI*, deve ammettersi che l'uso di tale inedito strumento potrebbe essere letto come una concreta opportunità per un più completo accertamento dei fatti, sempre che «non si sottragga al processo la ricca fucina di materiale gnoseologicamente significativo»[100]; da maneggiare con cura atteso che, in assenza di idonei riscontri atti a saggiare l'autenticità delle "dichiarazioni algoritmiche", potrebbero essere messi in pericolo i diritti di difesa dell'imputato (dal contraddittorio, alla parità delle armi, sino al *right to confrontation*)[101], per cui è opportuno dotare le parti di un completo armamentario idoneo a fronteggiare tale deriva[102].

Disattendendo l'idea secondo la quale la valutazione della prova è un «giardino proibito»[103], si aprirebbero le porte a nuove sollecitazioni della tecnologia anche in tale settore.

Deve darsi atto, però, che il ragionamento probatorio evoca uno scenario ambiguo: «da un lato, consente di circoscrivere l'indagine alle attività funzionali alla ricostruzione dei fatti; dall'altro, reca con sé la vasta e complessa tematica della cosiddetta "logica del giudice"»[104].

Viene da chiedersi, dunque, quali nuovi orizzonti probatorio potremmo raggiungere grazie all'intervento dell'*AI*.

Un primo ambito di interesse potrebbe essere costituito dalla collaborazione tra algoritmo e giudice: rispolverando l'antica questione circa l'utilizzabilità del metodo *bayesiano* per la determinazione della probabilità di una ipotesi[105], si palesa la possibilità di una valutazione algoritmica della prova.

---

[100] BACCARI - PECCHIOLI, *I.A. e giudizio sul fatto: gli strumenti di* e-evidence *per la cognizione*, cit., p. 154.

[101] PRESACCO, *Intelligenza artificiale e ragionamento probatorio nel processo penale*, cit., p. 99, afferma che la categoria della *automated generated evidence* genera un «grave squilibrio conoscitivo (*knowledge impairment*) tra le parti processuali, ponendo in tal modo a repentaglio il fondamentale principio di parità delle armi», a causa della «difficoltà che incontrerebbero le medesime parti processuali – in particolare, la difesa – nel contestare l'accuratezza e l'attendibilità degli elementi di prova ottenuti tramite l'ausilio delle nuove tecnologie di IA».

[102] BACCARI - PECCHIOLI, *I.A. e giudizio sul fatto: gli strumenti di* e-evidence *per la cognizione*, cit. p. 154, secondo i quali è necessario «limitare al massimo la lesione del diritto dell'imputato ad un effettivo confronto con la macchina che lo accusa».

[103] FERRUA, *Un giardino proibito per il legislatore: la valutazione delle prove*, in *Questione giustizia*, 1988, pp. 587 ss.

[104] PRESACCO, *Intelligenza artificiale e ragionamento probatorio nel processo penale*, cit., p. 93.

[105] UBERTIS, *La valutazione* bayesiana *delle prove incerte*, in *Cassazione penale*, 2021, pp. 1093 ss.

Nel dettaglio, si tratta di sistemi computazionali che dovrebbe essere in grado di vagliare l'attendibilità del teste anche attraverso applicativi di riconoscimento delle emozioni o di mera analisi della dichiarazione resa.

Stabilirebbero, dunque, se il dichiarante si trovava nelle migliori condizioni soggettive (stato d'animo e psicologico) e oggettive (spazio-temporali, di luce e fisiche) per percepire l'accaduto o per descriverlo nei termini indicati; analizzerebbero anche la prova orale per valutarne la coerenza – intesa come assenza di contraddizioni −, la capacità di contestualizzazione del teste – ci si riferisce alla descrizione precisa della scena in cui si sono verificati gli eventi – e l'esistenza (o meno) di commenti opportunistici non richiesti, che mirano a rinforzare retoricamente la credibilità della dichiarazione.

Proprio la testimonianza, infatti, si presta ad un elevato ed efficace livello di modellizzazione, poiché può essere apprezzata in base a criteri oggettivi come le condizioni atmosferiche e di luminosità in cui è avvenuta la percezione sensoriale del testimone, la distanza dell'osservatore dalla scena del crimine, le eventuali condizioni suggestive al momento dell'osservazione dei fatti narrati.

Con l'*AI* sarebbe, dunque, garantita una certa omogeneità nelle modalità di escussione del testimone e di valutazione della prova.

In prospettiva, l'obiettivo da porsi potrebbe essere quello di consolidare delle *best practices*, con l'ausilio di strumenti intelligenti, predisponendo una griglia di parametri di valutativi della prova dichiarativa (e non solo).

Ebbene, nella realtà processuale anglosassone è già stata avviata la sperimentazione pratica – in verità, perlopiù nel processo civile − del sistema algoritmico "*ADVOKATE*"[106], creato dall'Università di Edimburgo.

Tale applicativo, pensato per saggiare l'attendibilità della prova dichiarativa, potrebbe servire ad epurare il processo da contributi fuorvianti; in effetti, a renderli incerti vi sono una pluralità di fattori come l'inaffidabilità della memoria del testimone, considerato che l'eccessiva durata dei procedimenti penali produce un

[106] *ADVOKATE* è l'acronimo delle otto domande utilizzate con *input* per la valutazione della competenza e dell'affidabilità dei testimoni che, tradotte in lingua italiana, corrispondono a tempo, distanza, visibilità, ostacoli, pregressa conoscenza dell'oggetto della testimonianza, particolari ragioni per cui il ricordo possa essersi fissato nella mente, tempo trascorso dal fatto, errori o discrepanze.

consistente scarto temporale tra il momento in cui si è assistito al fatto storico di reato e quello in cui si è chiamati a rendere testimonianza.

Ebbene, leggendo tale esperienza attraverso la lente dell'*AI Act*, si potrebbe provare ad identificare tali *software* alla stregua di sistemi di «riconoscimento delle emozioni»[107], anche se, in tal modo, difficilmente avrebbero ingresso nelle nostre aule di giustizia, alla luce del divieto probatorio di cui all'art. 188 c.p.p.

Ad ogni buon conto, il Regolamento europeo, pur considerando gli strumenti di valutazione della prova alla stregua di *AI* "ad alto rischio"[108], ne ammette l'utilizzabilità, nel rispetto dei requisiti *ivi* imposti[109].

Nella stessa direzione, seppur con ambiti di applicabilità più circoscritti, si potrebbe prevedere anche l'utilizzo di sistemi valutativi della prova documentale, in grado di identificare anche un "falso".

Le avanguardie cui si fa riferimento potrebbero rivelarsi essenziali in dibattimento, aiutando i protagonisti della scena processuale a individuare le circostanze che influenzano la credibilità del testimoniane oculare o la genuinità di un documento.

Neppure dev'essere escluso a detti applicativi il ruolo di *supporter* processuali per una migliore gestione della *cross examination*: l'*AI* potrebbe agilmente suggerire al giudice nuovi temi di prova ai sensi dell'art. 506 c.p.p. oppure individuare tempestivamente la presenza di domande suggestive o nocive *ex* art. 499, commi 2 e 3, c.p.p.

Altro potenziale ambito applicativo riguarderebbe la prova scientifica.

Detti *software* potrebbero rivelarsi utili per individuare il soggetto più idoneo a cui conferire l'incarico peritale, atteso che il sistema riuscirebbe efficacemente ad immagazzinare una enorme quantità di dati, *ivi* compresi quelli contenuti nei *curriculum* dei singoli esperti, formulando proposte e "candidature" in base agli ambiti di specializzazione di ciascuno; immettendo gli *input* giusti potrebbe altresì riuscire a formulare i quesiti da rivolgere all'esperto.

---

[107] Cfr., art. 3, n. 39), Reg. UE 2024/1689.

[108] Cfr., All. III, § 1, n. 6), Reg. UE 2024/1689, secondo cui sono ammessi i *software* di «attività di contrato, nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso: […] c) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto per valutare l'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati».

[109] Sul punto, *supra*, Cap. I, § 4.

Queste, dunque, solo alcune delle possibili connessioni tra *AI* e prove.

Sul punto, però, deve farsi rilevare che nonostante le fervide denunce di chi prevede l'approssimarsi di irreparabili derive tecnocratiche[110], si ritiene che i sistemi algoritmici in tale ambito processuale potrebbero rivelarsi uno strumento utile a perfezionare la ricostruzione dei fatti purché, ovviamente, rigorosamente assoggettati al governo della legge e all'irrinunciabile controllo dell'uomo.

5. I *risk assessment tools* nel momento decisorio.

Ampiamente diffusi nei sistemi di *common law* sono pure i *risk assessment tools* ovvero strumenti che effettuano una "valutazione del rischio" algoritmica riferita ad un determinato soggetto, restituendo, in sostanza, una prognosi relativa al verificarsi di possibili condotte delittuose[111].

Si richiede, dunque, all'*AI* di prevedere il comportamento futuro dell'indagato/imputato in base a determinati "fattori di rischio" classificabili in elementi statici e dinamici[112]: i primi sono costituiti dai precedenti penali del soggetto (condanne, arresti, violazione della libertà condizionale) ovvero da dati storici non modificabili e indipendenti dalle decisioni prese dall'autore del reato; i secondi concernono, invece, il genere, l'età, le lesioni della vittima, il contesto sociale in cui vive il reo (stabilità familiare, lavorativa, psicologica e relazionale) e, pertanto, dipendono dalle sue scelte di vita.

Tali applicativi di giustizia predittiva sono prevalentemente utilizzati in due momenti significativi: l'«incidente per l'applicazione delle misure cautelari (in particolare, per quanto riguarda gli ordinamenti di *common law*, la decisione sul

---

[110] BACCARI - PECCHIOLI, *I.A. e giudizio sul fatto: gli strumenti di* e-evidence *per la cognizione*, cit., p. 162, sostiene che «il potente impatto della prova a genesi algoritmica sulla dinamica conoscitiva del processo penale rischia di riportare in auge linee argomentative siffatte, che minacciano, per un verso, di dequotare, fino ad azzerarlo, il senso della dialettica di parte sull'acquisizione di tali strumenti per la cognizione e, per l'altro, di erodere dall'interno l'impregiudicatezza e la libertà di convincimento che sono espressione pregnante dell'imparzialità cui deve in ogni momento ammantarsi l'operare del giudice».

[111] In argomento, D'AGOSTINO, *Gli algoritmi predittivi per la commisurazione della pena. A proposito dell'esperienza statunitense nel c.d.* evidence-based sentencing, in *Diritto penale contemporaneo - Rivista trimestrale*, 2019, 2, pp. 354 ss.; SLOBOGIN, *Assessing the Risk of Offending through Algorithms*, cit., p. 432.

[112] Per un'analisi sui possibili "fattori di rischio", SLOBOGIN, *Assessing the Risk of Offending through Algorithms*, cit., pp. 433 ss.

bail)» e la «deliberazione della sentenza, con specifico riguardo alla commisurazione della pena e al riconoscimento di alcuni benefici»[113].

Nel giudizio cautelare statunitense il più noto strumento digitale impiegato è il c.d. PSA (*Public Safety Assessment*)[114], in base al quale i giudici decidono sul *released on (or without) bail* dell'imputato[115].

L'algoritmo utilizza i *reports* di 750.000 casi, afferenti a oltre 300 giurisdizioni statali, garantendo così la conoscibilità delle informazioni di partenza e, più in generale, la trasparenza della decisione. Per eliminare i potenziali effetti discriminatori dell'applicativo, sono stati escluse dal *dataset* impiegato tutte le informazioni relative alle condizioni economiche, razziali e di genere[116]; tale scelta è dipesa dalla significativa incidenza *in pejus* di detti fattori sul giudizio di pericolosità.

Elabora, dunque, tre diversi indici, sintomatici delle esigenze cautelari da soddisfare con l'applicazione della misura: *failure to appear*, *new criminal activity index* e *new violent criminal activity index*[117].

Se il secondo e terzo sono più vicini alla logica del *risk assessment*, è il primo quello più evanescente; in questo caso, infatti, la *machina sapiens* compie una elaborazione statistica dei dati immessi nel sistema e, in particolare, delle mancate costituzioni in altri giudizi, riferiti al biennio precedente a quello in corso nonché a tutto l'arco di vita del soggetto indagato. Non vi è, pertanto, «alcun tipo di approfondimento scientifico, di tipo psicologico, circa l'effettivo rapporto causale tra tali statistiche e il rischio di non comparizione dell'imputato nel procedimento

---

[113] QUATTROCOLO, *Risk assessment*, cit., pp. 71 ss.

[114] Tale modello computazionale, creato dalla *Laura and John Arnold Foundation*, è utilizzato in 28 giurisdizioni (di cui 3 statali). È completamente attuariale poiché si basa su 9 parametri (età al momento dell'arresto, precedenti per *misdemeanors*, precedenti per *felonies*, precedenti per reati commessi con violenza, contumacia dell'imputato negli ultimi due anni e in quelli precedenti, pregresse condanne a pene detentive) e per generare l'*output* non richiede alcun contatto con l'indagato.

[115] Il Kentucky ha adottato un progetto pilota, noto come *Administrative Pretrial Release Program*, in 20 giurisdizioni su 120 (esteso nel 2017 all'intero Stato), basato su un utilizzo peculiare del *PSA*, secondo il quale per una serie di reati i *pretrial officers* è possibile ordinare, senza l'intervento di un giudice, il rilascio immediato degli indagati, il cui rischio di fuga e/o di commissione di reati risulta basso o moderato.

[116] Sul tema, GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., pp. 7-8.

[117] Rispettivamente, l'indice di rischio che il soggetto non si presenti in giudizio o che commetta nuovi reati nonché il potenziale rischio di un nuovo comportamento criminoso o violento.

pendente»[118] sicché si tende a dubitare della sua affidabilità, poiché non corroborato da fattori esterni.

Sotto altro profilo, come noto, è consentito all'organo giudicante di impiegare algoritmi basati sulla prognosi di pericolosità del condannato per determinare il *quantum* di pena da irrogare o per riconoscere benefici premiali.

Tali strumenti di calcolo della probabilità di recidiva[119] sono stati sperimentati sia nel panorama anglosassone − che vanta l'utilizzo del *software* HART (*Harm Assessment Risk Tool*)[120] − che in quello statunitense che ha sperimentato l'algoritmo *COMPAS* (*Correctional Offender Management Profiling for Alternative Sanctions*) [121] e il sistema *VRAG* (*Violence Risk Appraisal Guide*)[122].

Anche nella giurisdizione penale minorile si sta diffondendo l'uso di algoritmi predittivi: il Tribunale penale per i minorenni dell'Ohio utilizza l'applicativo *Watson* di IBM che genera relazioni complete circa la pregressa storia criminosa di coloro i quali propongono domanda di *sentencing or probation review*[123]; dinanzi alla Sezione minorile della Corte Suprema del Wisconsin del *District of Columbia*,

---

[118] QUATTROCOLO, *Risk assessment*, cit., p. 78.

[119] In argomento, ampiamente, QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings*, cit., pp. 131 ss.

[120] Questo modello restituisce giudizi predittivi per verificare il rischio che un soggetto arrestato commetta reati nei due anni successivi. Nel dettaglio, il *tools* restituisce un *output* sulla base del quale la persona viene catalogata come ad alto, moderato o basso rischio, a seconda della previsione per cui commetterà, probabilmente, un reato grave, un delitto di live entità ovvero alcuna condotta che potrebbe essere sussumibile in una fattispecie incriminatrice. Per approfondimenti, GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., pp. 10 ss.

[121] Creato dalla società privata *Equivant*, specializzata nello sviluppo di strumenti digitali di supporto alla giustizia, assegna all'imputato un punteggio probabilistico (*score*) da 1 a 10, per quantificarne la pericolosità sociale e la possibilità di commissione di un nuovo crimine. La previsione viene emessa incrociando una serie di dati riferibili a fatti pregressi: da un lato, i precedenti giudiziari e, dall'altro, 137 "*items*" ovvero quesiti su vari argomenti (precedenti penali, contesto sociale di appartenenza, infrazioni commesse durante eventuali periodi di detenzione) cui l'interessato dovrà rispondere, oltre alle ulteriori variabili non note e non conoscibili, poiché coperte dalla proprietà intellettuale imposta dalla società creatrice. Sul punto, FIORIO, *Predizione algoritmica e giurisdizione di sorveglianza*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, cit., pp. 252 ss.

Tuttavia, è il caso di segnalare che vi sono molti altri protocolli di previsione del rischio di recidiva, meno noti di *COMPAS*, impiegati negli Stati Uniti. In argomento, NIEVA-FENOLL, *Intelligenza artificiale e processo*, Torino, 2019, trad. it. a cura di Comoglio, p. 58; SLOBOGIN, *Assessing the Risk of Offending through Algorithms*, cit., pp. 436 ss.

[122] Utilizzato in diverse giurisdizioni statunitensi e in Canada, lavora prendendo in esame ben dodici fattori di rischio quali il punteggio nella *Psychopathy Checklist*, la storia scolastica, le diagnosi psichiatriche, la presenza della famiglia in età adolescenziale, lo stato civile della vittima, gli eventuali abusi di alcol e droghe. Sul punto, SLOBOGIN, *Assessing the Risk of Offending through Algorithms*, cit., p. 436.

[123] ROTH, *The Use of Algorithms in Criminal Adjudication*, cit., p. 417.

invece, è in corso la sperimentazione del sistema *SAVRY* che, non trattandosi di un modello algoritmico di tipo giuridico, viene somministrato per il tramite di un professionista[124].

Il fascino sprigionato da questi sistemi di *AI* raggiunge inarrivabili vette quando promette di ridurre – se non evitare del tutto – gli errori giudiziari, mitigando i *bias* cognitivi del giudicante[125].

Viene, però, da chiedersi se tale lettura non sia eccessivamente ottimistica.

Sebbene l'algoritmo sia di per sé neutrale, trattasi pur sempre di una creazione dell'uomo; in quanto tale potrebbe riflettere (anche amplificandone la portata), le discriminazioni e i pregiudizi di colui che l'ha progettato.

Affinché si possano sfruttare le "promesse" della giustizia predittiva è necessario concentrarsi sulla scelta del *dataset* che dovrebbe essere opportunamente selezionato nel contraddittorio tra le parti, salvaguardando le esigenze difensive.

A tal proposito, per individuare soluzioni percorribili finalizzate a limitare l'uso improprio di tali sistemi, pare opportuno il riferimento ad un caso pratico che ha suscitato l'attenzione – e, per certi versi, lo sgomento – della comunità scientifica e non solo.

6. I riflessi del caso *Loomis*.

L'algoritmo *COMPAS* è stato impiegato per la prima volta negli Stati Uniti nel processo penale a carico di Eric Loomis[126], divenuto, ormai, il più noto *leading case* in materia; il sistema è attualmente utilizzato in California, Michigan, New York, Wisconsin e Florida.

---

[124] MONTAGNA, *Prognosi personologica, commisurazione della pena e applicazione di misure di sicurezza*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, cit., pp. 237 ss.

[125] Sui limiti cognitivi degli esseri umani, FORZA, *Le scienze comportamentali ed il loro contributo nello studio dei processi decisionali*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale,* cit., pp. 33 ss.

[126] Arrestato nel 2013 con l'accusa di ricettazione e resistenza a pubblico ufficiale, è stato condannato dalla Corte distrettuale alla pena detentiva di anni sei di reclusione, poiché ritenuto soggetto con "*a high risk of violence, high risk of recidivism, [and] high pretrial risk*", cfr., *State Vs. Loomis*, 881, N.W.2d 749 (Wis. 2016).

La valutazione compiuta dall'algoritmo, inclusa nel *Presentencing Investigation Report (PSI)*[127], ha orientato i giudici statali verso il diniego della concessione della libertà vigilata in favore del condannato.

Seppur senza esito positivo, la difesa aveva già presentato in primo grado un *post-conviction relief* per ottenere la liberazione di Loomis, dolendosi dell'impossibilità di verificare la metodologia di calcolo impiegata dall'algoritmo, coperta da *trade secret*; lamentava altresì l'acritica applicazione di statistiche generaliste al condannato, evidentemente lesive del *right to be sentence on accurate information* e del *right to an individualized sentence*, rappresentando pure l'ingiustificata incidenza del genere (maschile) nella determinazione del *quoad poenam*[128].

L'esito sfavorevole è stato poi impugnato dinanzi alla *Court of Appeal*; tra i principali motivi del ricorso, sostanzialmente riproposto negli stessi termini della precedente istanza, vi era la violazione della *due process clause* (V e XIV Emendamento della Costituzione USA): l'opacità dell'algoritmo unita all'inaccessibilità della logica impiegata dalla macchina per giungere ad un determinato risultato e la carenza di motivazione della sentenza, rendevano impossibile conoscere tutte le ragioni poste a base della condanna.

Tali circostanze, a dire del prevenuto, avrebbero comportato l'irrimediabile compressione dell'esercizio del diritto di difesa, impedendo la celebrazione del *fair trial*.

La questione è stata rinviata alla *Wisconsin Supreme Court* che, nel prendere posizione sull'uso del *tool* giudiziario, ne ha riconosciuto la legittimità.

Nella fattispecie, pur precisando i limiti entro i quali – con estrema cautela − può essere impiegato[129], ha escluso possibili lesioni del diritto di difesa, in quanto «*a*

---

[127] Dopo aver raccolto l'ammissione di *guilty* dell'imputato, la Corte ha ordinato un *PSI*, che consiste in una relazione, redatta da un *probation officer* (ausiliario del giudice con particolari competenze psico-criminologiche), nella quale sono raccolti i risultati delle indagini condotte sulla storia personale dell'imputato con la finalità di verificare la presenza di circostanze utili per la determinazione della pena. Sul procedimento seguito dalle Corti statunitensi per la determinazione della pena, si veda D'AGOSTINO, *Gli algoritmi predittivi per la commisurazione della pena,* cit., pp. 360 ss.

[128] FIORIO, *Predizione algoritmica e giurisdizione di sorveglianza*, cit., p. 252.

[129] *State Vs. Loomis*, cit., §87-88, «*Next, we address the permissible uses for a COMPAS risk assessment at sentencing. Then we set forth the limitations and cautions that a sentencing court must observe when using COMPAS. Although it cannot be determinative, a sentencing court may use a COMPAS risk assessment as a relevant factor for such matters as: (1) diverting low-risk prison-bound offenders to a non-prison alternative; (2) assessing whether an offender can be supervised*

circuit court must explain the factors in addition to a COMPAS risk assessment that independently support the sentence imposed. A COMPAS risk assessment is only one of many factors that may be considered and weighed at sentencing»[130].

Pertanto, alcun rischio vi sarebbe per le garanzie difensive qualora il responso della macchina non sia l'unico elemento sul quale il giudicante fonda la propria decisione.

In questo caso, infatti, i giudici, oltre all'*output* di COMPAS hanno valutato, altresì, la gravità del reato commesso, la pregressa storia criminosa dell'imputato e gli altri capi di accusa per cui il Loomis non aveva reso la dichiarazione di colpevolezza (*read-in charges*).

Neppure le rassicurazioni della Corte si sono, però, rivelate sufficienti a placare i timori della comunità scientifica. Detta decisione ha generato una vera e propria levata di scudi da parte degli esperti del settore, che contestavano fermamente l'impiego delle tecnologie digitali come ausilio per il giudice nella fase del *sentencing*[131].

Serie e fondate critiche sono state mosse con riguardo alle possibili distorsioni cognitive dell'algoritmo (*Bias Automation*) che condurrebbero all'accreditamento di pratiche discriminatorie[132]; ancora, l'opacità del funzionamento del sistema, unita alla non conoscibilità del codice sorgente e all'indeterminatezza del *database* utilizzato, ne rendevano impraticabile qualsivoglia impiego giudiziario.

Il tipico atteggiamento di ritrosia del giurista, da sempre smarrito al cospetto delle innovazioni tecnologiche, si è acuito quando, nel 2016, l'organizzazione *no profit ProPublica* ha condotto uno studio di attendibilità, accuratezza e *fairness*

---

safely and effectively in the community; and (3) imposing terms and conditions of probation, supervision, and responses to violation».

[130] Cfr. *State Vs. Loomis*, cit., § 53-54. Tale interpretazione è stata condivisa anche dalla Suprema Corte degli Stati Uniti – adita in *extremis* dai difensori di Loomis – che, con una *amicus brief* presentata dal *Solicitor General* per conto degli *States*, ha avallato la tesi dei giudici statali e rigettato il *write of certiorari* presentato dalla difesa.

[131] Tra tutti, si veda, NIEVA-FENOLL, *Intelligenza artificiale e processo*, cit., p. 132, ritiene che la soluzione adottata dalla Corte suprema del Wisconsin sia «del tutto inadeguata, perché di fatto consente che un elemento di prova non facilmente controllabile dalle parti venga utilizzato nel processo. L'espressione *black box* induce una grande fascinazione, tuttavia il processo non può certamente essere una scatola nera».

[132] In generale sul tema, RENDA, *Moral Machine*, in AA.VV., *The Cambridge Handbook of the Law of Algorithms*, cit., pp. 674 ss.

dell'algoritmo *COMPAS*, rivelando scenari oscuri[133]: nonostante l'algoritmo non consideri espressamente la razza quale "fattore di rischio", da un lato, soltanto il 20% dei "potenziali criminali" ha poi commesso ulteriori delitti e, dall'altro lato, il sistema si è dimostrato incline a considerare "soggetti ad alto rischio" uomini di colore in percentuale doppia rispetto ai caucasici (45% a 24%).

È affiorata, dunque, una nuova e inquietante dimensione di fallibilità degli strumenti di *AI* legata a fattori razziali[134].

Tuttavia, per fugare ogni dubbio in ordine alla potenziale attitudine discriminatoria di siffatti applicativi può certamente affermarsi che l'*AI* non dimostra *ex se* alcun *animus*. Al contrario, però, sembra corretto affermare che gli algoritmi, seppur tendenzialmente neutrali, se male impostati, potrebbero riflettere i pregiudizi tipici dei processi decisionali dell'uomo.

Pertanto, considerato che i dati di *input* sono il carburante del sistema, è necessario selezionare con cura le informazioni con cui addestrare il *software* al fine di generare un *output* privo di discriminazioni ed esente da contaminazioni esterne.

Alla luce di tali rilievi, dunque, non può certamente ammettersi un uso indiscriminato di soluzioni algoritmiche senza averne preventivamente ponderato i rischi.

Per azzerare ogni possibile pericolo i sistemi di valutazione del rischio dovrebbero rispondere ai principi di adeguatezza, validità ed equità.

Attualmente, però, pare che nessun applicativo artificiale sia in grado di farlo[135]: l'incessante progresso tecnologico ci darà, probabilmente, le risposte di cui abbiamo bisogno. Non ci resta che attendere.

---

[133] In argomento, SLOBOGIN, *Assessing the Risk of Offending through Algorithms*, cit., pp. 440 ss.

[134] BARFIELD W., *Towards a law of artificial intelligence*, in AA.VV., *Research Handbook on the Law of Artificial Intelligence*, Barfield W. - Pagallo (*edited by*), Cheltenham, 2018, pp. 29 ss.; BARFIELD W. - BARFIELD J., *An Introduction to Law and Algorithms*, in AA.VV., *The Cambridge Handbook of the Law of Algorithms*, cit., p. 3.; HEAVEN, *Predictive policing algorithms are racist. They need to be dismantled*, in *MIT Technology Review online*, 17 luglio 2020.

[135] SLOBOGIN, *Assessing the Risk of Offending through Algorithms*, cit., p. 447.

CAPITOLO III

"GIUSTIZIA PREDITTIVA" E PERICOLOSITÀ SOCIALE

SOMMARIO: 1. Una premessa metodologica. 2. Intelligenza artificiale e pericolosità sociale. 3. La giustizia preventiva. 4. Le dinamiche cautelari. 5. La fase del *sentencing*. 6. L'esecuzione della pena e il regime penitenziario. 7. L'*iter* di formazione del *dataset*: il contraddittorio *sulla* e *per* la prova.

1. Una premessa metodologica.

L'«*Artificial Intelligence (AI) is one of the most transformative forces of our time, and is bound to alter the fabric of society*»[1], *ivi* compresa la giurisdizione penale e, in particolare, la dimensione decisoria.

Con lo sguardo costantemente rivolto ai modelli di *common law* statunitense e inglese, nelle pagine che precedono si è analizzata la sperimentazione – oltre i confini nazionali e non − dei sistemi di *AI* in tutto l'arco procedimentale: dalla fase pre-investigativa, prodromica all'acquisizione della *notitia criminis*, a quella delle indagini preliminari, sino a giungere alla dinamica probatoria e al meccanismo decisorio[2].

Proprio tale ultimo profilo, però, merita un maggiore grado di approfondimento[3].

È opportuno, dunque, vagliare la tenuta "algoritmica" dei vari moduli decisori − anche interlocutori – del procedimento penale domestico, chiarendone i profili di compatibilità con le regole processuali e i punti di rottura rispetto agli *standard* di giudizio *ivi* impiegati.

La metodologia utilizzata per condurre questo studio è ancorata alla dato normativo disponibile; è, infatti, attraverso la lente del Regolamento europeo sull'intelligenza artificiale, che categorizza come "ad alto rischio" i sistemi di amministrazione della

[1] L'espressione, che si ritiene condivisibile, era contenuta nella bozza delle *Ethics Guidelines for Trustworthy AI*, pubblicata il 18 dicembre 2018, ma non è stata ripresa nella versione definitiva del documento, pubblicato l'8 aprile 2019.

[2] Vedi *supra*, Cap. II.

[3] Sulla possibile incidenza della macchina sull'*iter* decisorio penale, LORUSSO, *La sfida dell'intelligenza artificiale al processo penale nell'era digitale*, in *Sistema penale online*, 28 marzo 2024, pp. 6 ss. Da ultimo, frena gli entusiasmi, SCALFATI, *IA e processo penale: prospettive d'impiego e livelli di rischio*, in *Processo penale e giustizia*, 2024, pp. 1404 ss.

giustizia[4], che si ritiene di ipotizzare l'impiego di detti applicativi nella sfera procedimentale, chiarendone, però, l'estensione operativa e i limiti di applicabilità.
L'esigenza di introdurre «*artificial agents*»[5] nel processo penale deriva dalla consapevolezza di un significativo mutamento della figura del decisore: da «astratto concetto di genere, uomo senza volto»[6], è divenuto giudice "suggestivo", "emotivo", "sentimentale", "empatico"[7].
Del resto il magistrato giudicante è pur sempre un uomo che, in quanto tale, potrebbe essere influenzato dalle proprie esperienze personali[8]; infatti, errori cognitivi e distorsioni possono attribuirsi anche «alla sfera dei valori e dei pregiudizi, delle emozioni/passioni e degli affetti» ovvero «all'area della comunicazione del pensiero attraverso i *mass media* o i *social network*, il cui linguaggio interagisce con il funzionamento del cervello umano e con la presa di decisione»[9].
Così, molto spesso, l'assetto emotivo viene trasferito nell'attività valutativa e ne plasma, inevitabilmente, la decisione[10], provocando la profonda crisi del principio di imparzialità del giudice, costituzionalmente garantito.
Da qui, la necessità di provare a correggere le distorsioni sistematiche della decisione penale, tipiche di un giudizio umano, attraverso il contributo dell'*AI*.

---

[4] In particolare, l'All. III, § 1, n. 8), Reg. UE 2024/1689, parla di «sistemi di IA destinati a essere usati da un'autorità giudiziaria o per suo conto per assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti, o a essere utilizzati in modo analogo nella risoluzione alternativa delle controversie».
[5] Così, FLORIDI - SANDERS, *On the Morality of Artificiale Agents*, in *Minds and Machines*, 2004, p. 349.
[6] GIUNTA, *Ghiribizzi penalistici per colpevoli. Legalità, "malalegalità", dintorni*, Pisa, 2019, p. 203.
[7] FELICIONI, *L'attività valutativa del giudice tra ragione ed emozione*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, Baccari - Felicioni (a cura di), Milano, 2023, p. 12.
[8] Sulle possibili insidie del giudizio razionale, FELICIONI, *L'attività valutativa del giudice tra ragione ed emozione*, cit., pp. 15 ss.
[9] CANZIO, *Prefazione*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, cit., p. XII.
[10] Cfr., MONTAGNA, *Prognosi personologica, commisurazione della pena e applicazione di misure di sicurezza*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, cit., pp. 226-227; FORZA, *Le scienze comportamentali ed il loro contributo nello studio dei processi decisionali*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, cit., pp. 33 ss.; FORZA - MENEGONI - RUMIATI, *Il giudice emotivo. La decisione tra ragione ed emozione*, Bologna, 2017, pp. 141 ss.;

Quasi a salvaguardia dell'integrità del processo penale, si introduce, quindi, il concetto di "giustizia predittiva"[11].

Lontana da magiche premonizioni, dunque, studia la probabilità che un determinato comportamento si verifichi, senza predire alcunché[12]. Ciò in quanto «la "probabilità" è semplicemente la verosimiglianza di realizzazione di un evento di tipo antisociale, mentre la "predizione" è la verosimiglianza che un determinato evento di tipo antisociale si verifichi in un certo lasso di tempo»[13].

Tale sintagma assume due diverse accezioni: da un lato, può riferirsi a sistemi algoritmici in grado di assicurare la prevedibilità di altre decisioni giudiziarie[14] e,

[11] Deve evidenziarsi che, mentre l'*AI Act* omette di fornire una nozione precipua di "giustizia predittiva", la Carta etica europea ne parla come «l'analisi di una grande quantità di decisioni giudiziarie mediante tecnologie di intelligenza artificiale al fine di formulare previsioni sull'esito di alcune tipologie di controversie specialistiche (per esempio, quelle relative alle indennità di licenziamento o agli assegni di mantenimento). Il termine "predittivo" utilizzato dalle società di *legal tech* [N.d.T. si veda la definizione alla relativa voce] è tratto dalle branche della scienza (principalmente la statistica) che consentono di predire risultati futuri grazie all'analisi induttiva. Le decisioni giudiziarie sono trattate al fine di scoprire correlazioni tra i dati in ingresso (criteri previsti dalla legge, fatti oggetto della causa, motivazione) e i dati in uscita (decisione formale relativa, per esempio, all'importo del risarcimento). Le correlazioni che sono giudicate pertinenti consentono di creare modelli che, qualora siano utilizzati con nuovi dati in ingresso (nuovi fatti o precisazioni introdotti sotto forma di parametri, quali la durata del rapporto contrattuale), producono secondo i loro sviluppatori una previsione della decisione (per esempio, della forbice risarcitoria). Alcuni autori hanno criticato questo approccio sia formalmente che sostanzialmente, sostenendo che, in generale, la modellizzazione matematica di determinati fenomeni sociali non è un compito paragonabile ad altre attività quantificabili più facilmente (isolare i fattori realmente causativi di una decisione giudiziaria è un compito infinitamente più complesso di giocare, per esempio, una partita di Go o riconoscere un'immagine): il rischio di false correlazioni è molto più elevato. Inoltre, in dottrina, due decisioni contraddittorie possono dimostrarsi valide qualora il ragionamento giuridico sia fondato. Conseguentemente la formulazione di previsioni costituirebbe un esercizio di carattere puramente indicativo e senza alcuna pretesa prescrittiva» (cfr., Carta etica europea, All. II, Glossario, p. 47).

[12] 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, p. 117, secondo cui non può e non deve correrci il rischio di «ammantare di certezza matematica conclusioni – quelle della macchina intelligente – che vanno invece riportate nella dimensione crepuscolare della probabilità».

[13] QUATTROCOLO, *Risk assessment: sentencing o non sentencing?*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio,* cit., p. 73. Di diverso parere, NIEVA-FENOLL, *Intelligenza artificiale e processo*, Torino, 2019, trad. it. a cura di Comoglio, pp. 51-52, secondo cui «in fin dei conti si tratta di predire le tendenze di una parte nel processo; e questo chiaramente non è facile trattandosi di una valutazione che ben difficilmente può definirsi davvero giuridica».

[14] Si tratta di previsioni circa la probabile sentenza che sarà emessa dall'organo giudicante relativa ad un caso specifico. Nel sistema sono immessi, infatti, moli precedenti giurisprudenziali che, analizzati dall'algoritmo, vengono poi raggruppate in categorie di orientamenti conformi e difformi per ogni specifica questione di diritto; sulla base di tali dati la macchina genera una prognosi circa i possibili esiti del giudizio, pur con tutti i limiti del caso.

dall'altro lato, calcolare la possibilità che un determinato soggetto ponga in essere un dato comportamento che abbia rilievo penale[15].

Ai giorni nostri, il primo profilo appare quasi scontato, pur con tutte le criticità del caso legate alla profilazione del singolo magistrato; oggetto di riflessione nelle pagine che seguono è, dunque, la seconda area applicativa che suscita inevitabilmente l'interesse del giurista.

Ipotizzare un possibile connubio tra "giustizia predittiva" e processo penale imporrebbe una lettura che adotti una logica binaria. Infatti, *keywords* per risolvere l'enigmatico rapporto tra decisione penale e *AI* sono la "pericolosità sociale" e i "criteri di giudizio"[16].

Dopo aver esaminato la nozione di pericolosità sociale, si andranno ad isolare i diversi momenti decisori in cui il legislatore onera il giudice penale di compiere una "previsione" sul futuro comportamento della persona sottoposta alle indagini o dell'imputato o, ancora, del condannato; pur senza precisi strumenti d'indagine, infatti, accolla – forse impropriamente − al decisore il peso di detta scelta.

È il concetto di rischio quindi che rappresenta il *file rouge* del presente capitolo: dopo aver testato la resistenza della decisione alla macchina computazionale, si valutano tutte le variabili celate dietro la complessa attività decisoria sulla pericolosità sociale, attualmente ad esclusivo appannaggio del giudicante umano, soppesando vantaggi e svantaggi di una possibile contaminazione algoritmica.

Nel capitolo che segue (v. Cap. IV), invece, si sviluppa quel secondo filone interpretativo che vede la "giustizia predittiva" inevitabilmente legata agli *standard* decisori.

L'obiettivo è quello di determinare i margini di compatibilità tra gli *standard* di giudizio vigenti – in particolare, la "ragionevole previsione di condanna" e l'accertamento della colpevolezza "oltre ogni ragionevole dubbio" – e l'*AI*; approfondendo la concreta fattibilità di una decisione umana coadiuvata dalla

---

In dottrina sull'incapacità dell'*AI* di riprodurre il ragionamento logico umano, SIGNORATO, *Giustizia penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo*, in *Rivista di diritto processuale*, 2020, p. 609.

[15] MONTAGNA, *Prognosi personologica, commisurazione della pena e applicazione di misure di sicurezza*, cit., p. 224.

[16] Su cui *infra*, Cap. IV.

machina sapiens, si procede con l'individuazione del meccanismo di formazione del *dataset*, anche alla luce dell'incerta traducibilità del dato normativo.

Invero, soltanto precisando regole e modalità operative da poter impiegare nella prassi, è possibile tracciare un sentiero sicuro su cui il legislatore del prossimo futuro potrebbe riuscire ad orientarsi con maggiori consapevolezze e guadagnando, forse, un pizzico di audacia in più.

Del resto la galoppante diffusione di sistemi computazionali, anche nel mondo giuridico, ne fa presagire un ingresso a gamba tesa nel panorama processuale; non possiamo (e non dobbiamo), dunque, farci trovare impreparati.

2. Intelligenza artificiale e pericolosità sociale.

Come noto, la categoria della pericolosità sociale assume connotati trasversali, coinvolgendo diversi profili dello *ius dicere*[17].

Nel dettaglio, il vaglio richiesto all'organo giudicante è di carattere soggettivo e personologico. Esula, infatti, da detta valutazione la capacità criminale del reo, sussistente *a priori* per colui che ha già commesso il reato per cui si procede; al contrario, consiste in una prognosi in ordine alla possibilità che questi realizzi ancora condotte delittuose[18].

In sostanza, «il giudizio sulla possibilità che il prevenuto commetta ulteriori reati è un calcolo di probabilità di verificazione di un evento futuro e incerto»[19] che, in quanto tale, sfugge alle coordinate del ragionamento umano.

Ipotizzare l'utilizzo di sistemi di *AI* come strumento per la valutazione del rischio[20] potrebbe sembrare impresa ardua, probabilmente utopica. Ma così non è (o meglio, così non dovrebbe essere).

---

[17] Sul punto, è interessante l'analisi di BASILE, *Esiste una nozione ontologicamente unitaria di pericolosità sociale? Spunti di riflessione, con particolare riguardo alle misure di sicurezza e alle misure di prevenzione, in Rivista Italiana di Diritto e Procedura Penale*, 2018, pp. 644 ss.; si veda pure CANESCHI, *Intelligenza artificiale e sistema penitenziario*, in *Rivista Italiana di Diritto e Procedura Penale*, 2024, 1, p. 260, che ne parla come «una categoria polifunzionale, che rileva in plurime sedi dell'ordinamento».

[18] Pone l'interessante differenza tra «giudizio sulla personalità dell'imputato» e «giudizio tecnico sulla personalità», MONTAGNA, *Prognosi personologica, commisurazione della pena e applicazione di misure di sicurezza*, cit., pp. 231 ss.

[19] MONTAGNA, *Prognosi personologica, commisurazione della pena e applicazione di misure di sicurezza*, cit., p. 228.

[20] Sul concetto di "rischio", ampiamente, ASHWORTH- ZEDER, *Preventive Justice*, Oxford, 2014, p. 121.

Occorre, quindi, comprendere come disciplinare l'uso di tali applicativi ai fini della determinazione della pericolosità sociale, che costituisce la prima area dogmatica in cui poterli sperimentare. Infatti, uno studio in tal senso potrebbe costituire un valido punto di partenza per l'immissione di detti *software* nelle aule di giustizia.

Prima di ogni cosa, però, è necessario individuare i rischi insiti all'attività valutativa automatica.

Posto che il concetto di pericolosità dell'individuo risulta inevitabilmente ancorato al contesto sociale e politico in cui si evolve, tanto che la «*perception of risk vary over time and by jurisdiction*»[21], ai rischi puramente tecnici, si aggiungerebbero le questioni sociali e politiche – le quali implicano una maggiore o minore considerazione di un determinato rischio − che variano nel tempo e nello spazio, influenzando le singole scelte di politica criminale e, quindi, incidendo significativamente su detta categoria.

Considerato che la prognosi di possibili condotte violente e delittuose può essere realizzata anche attraverso soluzioni digitali, che fanno ricorso a sofisticati metodi di *machine learning*[22], resta peraltro controversa la selezione degli indici di rischio. Una scelta non ben ponderata, infatti, potrebbe condurre ad un risultato che potrebbe «essere influenzato da un pregiudizio, che può portare alla discriminazione di singoli individui o di gruppi sociali»[23].

Poste queste premesse e poiché «prevedere il futuro significa cercare di ridurre, dal primo momento possibile, il rischio legato alla pericolosità sociale dell'imputato»[24], si ipotizza una contaminazione algoritmica del processo decisionale in quattro diversi momenti procedimentali[25]: l'area della giustizia preventiva, il modello cautelare, la fase del *sentencing* e l'esecuzione della pena.

Nel contesto comunitario, ne offre una definizione anche l'art. 3, n. 2), Reg. 2024/1689 UE, secondo cui si tratta della «combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso».

[21] In questi termini si esprimono ASHWORTH- ZEDER, *Preventive Justice*, cit., p. 119, che ribadiscono «*what is perceived and targeted as hazardous at any ont time is partly a matter of social construction, susceptible to changes in public toleration and shifting perceptions of what threatens*».

[22] QUATTROCOLO, *Risk assessment*, cit., p. 69.

[23] Così, MAUGERI, *L'uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra* evidence based practies *e tutela dei diritti fondamentali*, in *Archivio penale web*, 17 maggio 2021, p. 7.

[24] Così, QUATTROCOLO, *Risk assessment*, cit., p. 71.

[25] Si tratta, a parere di chi scrive, di segmenti decisori automatizzabili entro quelli che QUATTROCOLO, *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *MediaLaws*, 3,

Si tratta, infatti, di porzioni di decisione tutte accomunate, sul piano strutturale, da valutazioni circa la pericolosità della persona sottoposta alle indagini o dell'imputato (a seconda del momento procedimentale in cui si opera) che potrebbero essere efficacemente assunte dal giudice con l'ausilio di meccanismi di *AI*.

3. La giustizia preventiva.

Nato nell'Ottocento, l'"universo parallelo" della giustizia preventiva costituisce, probabilmente, l'ossidato retaggio delle vecchie misure di polizia.

È ontologicamente ispirato da fattori di precauzione e di attenuazione del rischio di commissione di fatti illeciti, da raggiungere attraverso misure adottate dall'autorità che siano in grado di limitare le libertà fondamentali dell'individuo[26]; in sostanza, il procedimento preventivo si pone l'obiettivo di ridurre i rischi di danno in vari ambiti del diritto[27].

Sebbene, com'è noto, le manifestazioni di pericolosità più evidenti derivano da eventi delittuosi accertati con sentenze di condanna, è pur vero che «la pericolosità può sussistere anche di fronte ai casi di proscioglimento e di assoluzione stante l'autonomia del procedimento di prevenzione rispetto al procedimento penale»[28].

Insomma, la *ratio* di tali misure non è quella di «punire (o reagire ad) un illecito commesso nel passato» ma «prevenire (o ridurre) il rischio che un evento dannoso si verifichi in futuro»[29].

2020, p. 133, definisce come i «numerosi momenti in cui l'autorità giudiziaria è chiamata a svolgere valutazioni di tipo prognostico-predittivo, gravando il decisore di una prognosi estremamente complessa».

[26] In argomento, si veda FIANDACA, voce *Misure di prevenzione (profili sostanziali)*, in *Digesto delle discipline penalistiche*, VIII,1994, Torino, pp. 108 ss.

[27] In senso analogo, ASHWORTH - ZEDER, *Preventive Justice*, cit., p. 5.

[28] TESCAROLI, *Il procedimento di prevenzione patrimoniale: profili problematici e questioni aperte*, in *Questione giustizia online*, 15 febbraio 2022, p. 3.

In giurisprudenza, Cass., sez. 1, 20 febbraio 2019, n. 21735, in *CED*, n. 276400-01, nella parte motiva chiarisce che il giudice della misura di prevenzione non è vincolato a recepire l'eventuale esito assolutorio del processo celebrato a carico dell'imputato.

[29] CAIANIELLO, *Potenzialità e rischi derivanti dall'interazione tra I.A. e giustizia penale preventiva*, in AA.VV., *XXVI lezioni di diritto dell'intelligenza artificiale*, Ruffolo (a cura di), Torino, 2021, p. 271.

Nel dettaglio trattasi di provvedimenti coercitivi[30] «destinati a funzionare non già, a guisa delle "pene criminali", *post et propter delictum*, contro chi di questo si è reso autore» ma *ante o praeter delictum* «cioè prima od a prescindere dalla commissione di simile illecito, per il solo fatto che il rispettivo destinatario, in virtù di determinate circostanze, appare come "autore futuribile" di taluni fatti penalmente antigiuridici»[31].

Ebbene, il *modus operandi* che anima l'autorità competente ad adottare siffatte misure segue «un giudizio prognostico o predittivo», privo di «finalità retributive o punitive»[32].

Di conseguenza, trattandosi di misure «che hanno come componente strutturale una valutazione di pericolosità basata su dati indiziari e strutturalmente incline ad essere "integrata" da indici di carattere predittivo»[33], è in questa sede che potrebbero schiudersi concreti spazi applicativi per sistemi di artificiali governati da algoritmi. Sembrerebbe, dunque, che la propensione del soggetto a commettere futuri reati, intesa come base di partenza per l'adozione di provvedimenti applicativi di misure preventive *ante delictum* o *preater delictum*, possa essere agevolmente sottoposta alla valutazione dell'*AI*, in ragione del peculiare percorso decisionale cui è chiamata l'autorità giudicante, pur senza un preciso armamentario.

Che si tratti di "pericolosità generica"[34] o di "pericolosità qualificata"[35], infatti, il *software*, restituendo uno *score* probabilistico, potrebbe orientare in maniera efficace il giudice nella sua decisione.

---

[30] Si distinguono in personali e patrimoniali; la loro disciplina è contenuta prevalentemente nel d.lgs. 6 settembre 2011, n. 159, rubricato "Codice delle leggi antimafia e delle misure di prevenzione". In dottrina, sulle criticità legate a tale istituto che alimentano proposte abolitive, GRASSO, *Le misure di prevenzione personali e patrimoniali nel sistema costituzionale*, in *Sistema penale online*, 14 febbraio 2020. In prospettiva comparata, con riferimento al sistema giuridico di *common law* americano, si veda l'analisi condotta da ASHWORTH - ZEDER, *Preventive Justice*, cit., pp. 251 ss.

[31] MOSCARINI, *Riflessioni sul modello attuale delle misure di prevenzione personale*, in *Processo penale e giustizia*, 2023, p. 936.

[32] CAIANIELLO, *Potenzialità e rischi derivanti dall'interazione tra I.A. e giustizia penale preventiva*, cit., p. 271.

[33] MANES, *L'oracolo algoritmico e la giustizia penale: al piglio tra tecnologia e tecnocrazia*, in *Discrimen*, 15 maggio 2020, p. 10.

[34] È legata alla condotta e il tenore di vita del soggetto attenzionato, dai quali è possibile dedurre, sulla base di elementi di fatto e non meri indizi, che tali soggetti vivano abitualmente (anche soltanto in parte) con i proventi di attività delittuose.

[35] È attribuita a coloro i quali sono indiziati di reato *ex* art. 416 *bis* c.p.p. nonché ai sensi dell'art. 51, comma 3 bis, c.p.p.

Gli strumenti algoritmici, infatti, ben si presterebbero ad operare in un terreno già incerto e farraginoso, sul quale tradizionalmente si fonda la valutazione umana, che pretende di "indovinare" i potenziali e, allo stato, non determinati futuri comportamenti pericolosi o criminali di un determinato soggetto.

In effetti, come statuito dalla giurisprudenza di legittimità, tale giudizio di pericolosità è dotato di una doppia anima: vi è una prima fase di tipo "constatativo" rapportata alla importazione di dati cognitivi idonei a rappresentare l'avvenuta condotta contraria alle ordinarie regole di convivenza tenuta – in passato – dal soggetto proposto e una seconda fase di tipo essenzialmente prognostico, per sua natura alimentata dai risultati della prima, tesa a qualificare come "probabile" il ripetersi di condotte antisociali, inquadrate nelle categorie criminologiche di riferimento previste dalla legge[36].

Ebbene, proprio quest'ultimo segmento valutativo potrebbe essere deferito all'*AI* che, sulla base di calcoli statistici, potrebbe offrire una previsione oggettiva ancorata al canone della probabilità; resta, invece, ad appannaggio umano il momento iniziale di ricognizione dei dati utili per valutare la pericolosità del soggetto, che costituiscono le informazioni di partenza per l'elaborazione della prognosi algoritmica.

Alcun dubbio residuerebbe circa la possibilità che la macchina intelligente possa decidere sulla base delle conoscenze pregresse dell'individuo di cui si è in possesso (precedenti penali, eventuali procedimenti pendenti e stile di vita tenuto)[37]; del resto, già la decisione esclusivamente umana viene, in ogni caso, fondata su tali (pregiudizievoli?) parametri.

---

[36] Così, Cass., Sez. I, 11 febbraio 2014, n. 23641, in *CED*, n. 260104-01: «in tema di misure di prevenzione personali, la valutazione del requisito di attualità della pericolosità sociale deve essere effettuata per tutte le categorie dei soggetti indicati nell'art. 4 D.Lgs. n. 159 del 2011, che possono essere assoggettati a misure di prevenzione personali con la conseguenza che, non essendo ammissibile una presunzione di pericolosità derivante esclusivamente dall'esito di un procedimento penale, è onere del giudice verificare in concreto la persistenza della pericolosità del proposto, specie nel caso in cui sia decorso un apprezzabile periodo di tempo tra l'epoca dell'accertamento in sede penale e il momento della formulazione del giudizio sulla prevenzione».

[37] In materia di misure di prevenzione personali, si pensi all'art. 1, d.lgs. 6 settembre 2011, n. 159, che si riferisce a «coloro che debbano ritenersi, sulla base di elementi di fatto, abitualmente dediti a traffici delittuosi», a «coloro che per la condotta ed il tenore di vita debba ritenersi, sulla base di elementi di fatto, che vivono abitualmente, anche in parte, con i proventi di attività delittuose» nonché a «coloro che per il loro comportamento debba ritenersi, sulla base di elementi di fatto […] che sono dediti alla commissione di reati che offendono o mettono in pericolo l'integrità fisica o morale dei minorenni, la sanità, la sicurezza o la tranquillità pubblica».

In particolare, i primi dati operativi da inserire – che corrisponderebbero alle informazioni che vengono già assunte dall'autorità procedente per la decisione – sono quelli relativi al certificato dei carichi pendenti e del casellario giudiziale, alle ordinanze di custodia cautelare ovvero alle sentenze di condanna, da cui poter desumere l'esistenza di "elementi di fatto" o di "sufficienti indizi" per il riconoscimento della c.d. "pericolosità generica"; meno rigoroso, invece, è il paramento dell'"indiziato di delitto" necessario per accertare la c.d. "pericolosità specifica".

L'adozione di un provvedimento ablativo reale di tipo algoritmico richiederebbe, inoltre, un'indagine patrimoniale per individuare eventuali "sproporzioni" tra guadagni leciti e beni (mobili o immobili) "disponibili", i cui esiti potrebbero pure essere immessi nel sistema algoritmico per essere attentamente ponderati dallo stesso.

Affinché, invece, sia applicabile una misura di prevenzione personale, anche in combinato disposto con quella patrimoniale, oltre all'abitualità alla propensione criminosa, è necessario che la pericolosità sia attuale; sicché il fattore temporale gioca un ruolo fondamentale nella valutazione degli indici di cui sopra.

Il *database* del sistema dovrebbe essere dotato anche di una nutrita raccolta di sentenze: in questo modo, in ossequio ai principi dettati dalla giurisprudenza di legittimità, potrebbe analizzare cosa è accaduto in casi analoghi e, dunque consultare pure i singoli provvedimenti di merito; così, saggerebbe l'effettiva utilizzabilità dei dati immessi unilateralmente dal giudice della prevenzione, segnalando eventuali anomalie e scartandone quelli inadeguati.

Incrociando i dati di cui dispone, l'algoritmo sarebbe in grado di individuare quale sia la misura preventiva personale o patrimoniale più adeguata al caso di specie; qualora optasse per un provvedimento ablativo di tipo reale potrebbe altresì indicare quali beni sequestrare, qualora sia in possesso di informazioni relative alla condizione economica e patrimoniale del soggetto in questione.

Dunque, l'eventualità che il tribunale − per taluni provvedimenti preventivi − dovesse affidarsi alla previsione algoritmica per generare il provvedimento da adottare potrebbe non apparire poi così tanto estrema.

In prospettiva *de iure condendo*, quindi, date le note criticità esistenti nel settore della prevenzione nonché le frizioni costituzionali e sovrannazionali − già denunciate a gran voce da più fronti − si dovrebbe «saper cogliere l'opportunità presentata dai cambiamenti in atto, cercando di introdurre quelle tutele attese da tempo, favorendo anche un uso mirato di I.A. e di *machine learning* per conferire al settore maggiore prevedibilità e coerenza»[38].

Il medesimo discorso potrebbe essere esteso anche alla disciplina delle misure di sicurezza.

Del resto è lo stesso legislatore che, nel dettarne i requisiti di applicabilità, parla di "persone socialmente pericolose" (art. 202, comma 1, c.p.), specificando che sono ritenuti tali coloro i quali, pur non imputabili o non punibili, "è probabile che commetta(no) nuovi fatti preveduti dalla legge come reati" (art. 203, comma 1, c.p.).

Infatti, proprio tale pericolosità sociale, che secondo l'art. 203, comma 2, c.p. dovrebbe essere desunta *ex* art. 133 c.p., potrebbe presentarsi come naturale *sedes materiae* in cui la macchina computazionale si troverebbe ad operare, sottraendo così l'analisi probabilistica alla mera intuizione del giudicante, intesa come fattore distorsivo del giudizio umano[39].

Una prospettiva allettante, sembrerebbe; da maneggiare con cura, però, evitando inaccettabili lesioni dei diritti fondamentali dell'individuo.

4. Le dinamiche cautelari.

L'*AI* potrebbe altresì insinuarsi tra le pieghe del procedimento cautelare.

In origine, tale momento − sia nella tradizione di *civil law* che in quella di *common law* − era incentrato sulla «valutazione del rischio per lo svolgimento futuro del procedimento penale»[40]; tuttavia, negli ultimi anni si è registrato uno «slittamento

[38] CAIANIELLO, *Potenzialità e rischi derivanti dall'interazione tra I.A. e giustizia penale preventiva*, cit., pp. 279.

[39] Sul punto, FORZA, *Le scienze comportamentali ed il loro contributo nello studio dei processi decisionali*, cit., p. 34, secondo cui si tratta «non tanto, o non solo, (di) *deficit* di intelligenza o del pensiero razionale, riconducibili alla logica formale, ma scostamenti automatici del pensiero riferibili all'intuizione».

[40] QUATTROCOLO, *Risk assessment*, cit., p. 70.

della funzione cautelare verso rischi che non sono tipicamente endoprocedimentali, ma sono piuttosto ascrivibili ad una valutazione di pericolosità sociale»[41].

Nel contesto domestico, infatti, il giudice deve verificare l'esistenza delle condizioni generali di applicabilità previste *ex lege* per emettere un'ordinanza applicativa di una misura cautelare idonea a soddisfare almeno una delle esigenze di cui all'art. 274 c.p.p. Fra i pericoli che tende a scongiurare vi è il rischio di inquinamento probatorio e quello di fuga (art. 274, comma 1, n. 1 e 3, c.p.p.) nonché di reiterazione del reato (art. 274, comma 1, n. 2, c.p.p.).

In sostanza, il magistrato si ritrova a confrontarsi con la seguente domanda: un soggetto che, probabilmente, ha commesso il reato per cui si procede – magari con una fedina penale tutt'altro che limpida – potrebbe rendersi autore di un altro delitto? Ed ancora, sarebbe capace di sottarsi alla giustizia dandosi alla fuga o compromettendo l'ipotetico quadro probatorio, allo stato meramente indiziario, a suo carico?

L'oggetto dell'apprezzamento cautelare consiste in un rischio legato a «un evento incerto nell'*an* e nel *quantum*; e ciò aggiunge ulteriore disorientamento nella valutazione che deve essere compiuta»[42].

Molto spesso nella pratica giudiziaria si tenta di superare i dubbi relativi a ciò che potrebbe (o non potrebbe) accadere in futuro attraverso una serie di automatismi, suscettibili di feroci critiche poiché qui si ha a che fare con la libertà personale dell'indagato, ritenuta inviolabile dall'art. 13 Cost.

Ebbene, con l'impiego della *machina sapiens* si potrebbe valutare "con cognizione di causa"[43], l'effettiva sussistenza di tali fattori cautelari, misurandone l'intensità.

In tal modo, dunque, sarebbe altresì assicurato il rispetto dei principi di adeguatezza, proporzionalità e gradualità delle misure cautelari poiché il giudice, esaminando anche il "parere dell'algoritmo", potrebbe meglio ponderare la sua decisione, fondandola su pilastri valutativi più solidi.

---

[41] QUATTROCOLO, *Risk assessment*, cit., p. 71.

[42] NIEVA-FENOLL, *Intelligenza artificiale e processo*, cit., p. 52.

[43] Si mostra diffidente, NIEVA-FENOLL, *Intelligenza artificiale e processo*, cit., p. 53, secondo cui «si può certamente provare a registrare una statistica per calcolare le percentuali di possibilità di accadimento di un pericolo, ma la conferma dell'effettivo accadimento di tale pericolo verrà osservata solo quanto è accaduto davvero, ossia solo al momento dell'esecuzione della sentenza. Vale a dire, solo quando il rischio si è trasformato in danno».

La *machina sapiens* basandosi sulle medesime informazioni pervenute al giudice, potrebbe dunque valutare l'esistenza di concreti e «gravi indizi di colpevolezza» a carico dell'indagato nonché la sussistenza di almeno una delle esigenze cautelari previste dal codice di rito.

In particolare, nel caso in cui si trattasse del pericolo di distruzione delle prove, il sistema artificiale potrebbe essere allenato con i dati relativi alle azioni eventualmente già compiute dalla persona sottoposte a indagini preliminari, come l'aver fornito un alibi evidentemente falso o l'aver tentato di manipolare le tracce del reato, valutando in generale la pericolosità del soggetto rispetto all'accertamento giudiziario; è da tenere in considerazione anche la posizione di potere che potrebbe esercitare all'interno di una struttura criminale che gli consentirebbe, più agevolmente, di interferire nel processo.

Per calcolare, invece, il rischio di reiterazione del reato, l'algoritmo potrebbe impiegare gli esiti investigativi − seppur ad uno stadio iniziale − e il profilo criminale dell'indagato, ricostruito non solo attraverso la consultazione del casellario giudiziale e dei carichi pendenti ma anche prendendo in esame dati relativi alle sue abitudini di vita, *ivi* compresa la frequentazione con soggetti pericolosi.

Più complessa è la decisione in ordine al rischio di fuga poiché «appartiene alle idee più intime di un soggetto»[44]; ad ogni buon conto, potrebbero essere prese in considerazioni più variabili al fine di ottenere un riscontro basato su dati più o meno certi: l'imminente esecuzione di una pena detentiva significativa, l'esistenza di precedenti penali per evasione, gli eventuali episodi di resistenza all'autorità pubblica durante l'esecuzione di provvedimenti cautelari o definitivi, l'appartenenza ad un sodalizio criminale che potrebbe agevolarne la latitanza nonché la concreta disponibilità di mezzi finanziari necessari per la fuga.

Ciò detto, è il caso di comprendere in base a quale meccanismo giuridico potrebbero trovare ingresso i sistemi di *AI* nella parentesi cautelare.

Riconoscere validità alla teoria secondo cui tali applicativi si basano su valutazioni psico-criminogene significherebbe vietarne l'accesso nel nostro sistema

[44] NIEVA-FENOLL, *Intelligenza artificiale e processo*, cit., p. 66.

processuale ai sensi dell'art. 220, comma 2, c.p.p., che proibisce l'ingresso nel processo di perizie psicologiche[45].

Macroscopiche sono, però, le differenze tra il *modus operandi* proprio del sistema algoritmico e quello tipico della perizia: il primo si basa su dati oggettivi e documentali; il secondo su valutazioni psicologiche che, pur compiute da esperti del settore, ricostruiscono la personalità del soggetto sulla base di elementi aleatori ed incerti, tanto che la "diagnosi" potrebbe mutare, di volta in volta, se si cambiasse tecnico.

L'esistenza di una palese asimmetria valutativa tra l'operato delle macchine intelligenti e quello di esperti come psicologi, psichiatri e criminologi, indurrebbe a collocare l'*AI* al di fuori del recinto ostativo di cui all'art. 220, comma 2, c.p.p., rendendone l'ingresso nelle aule di giustizia del tutto legittimo, atteso che l'algoritmo non è finalizzato a scandagliare il foro interiore della persona sottoposta alle indagini preliminari[46].

Tuttavia se, da un lato, è chiaro che giammai potrebbe essere concesso al *software* di decidere in autonomia circa l'eventuale compressione del diritto alla libertà personale di un soggetto, dall'altro, il suo compito potrebbe essere quello di corroborare la decisione del g.i.p., formulando prognosi fondate su basi statistiche e non lasciando la scelta a meri presentimenti.

L'utilizzo di strumenti predittivi nella fase cautelare sarebbe, però, ipotizzabile assegnando all'*output* prodotto dall'*AI* il valore di semplice indizio, bisognoso di essere sempre avvalorato da ulteriori elementi probatori, e in quanto tale è suscettibile di interpretazione ad opera del giudice.

In tal modo, probabilmente, si eviterebbe di incorrere in macroscopici errori – celati dietro oscure motivazioni − cui i "presagi" del giudicante possono condurre.

---

[45] In tal senso, QUATTROCOLO, *Risk assessment*, cit., p. 80. Si veda, altresì, LA REGINA, *I.A. e ragionamento giuridico: la giustizia prevedibile*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, cit., p. 178, avverte che «in assenza di ostacoli all'ingresso della "previsione" nel patrimonio conoscitivo del giudice, sarebbe più che concreto il rischio di immettere valutazioni concernenti la personalità dell'imputato nell'itinerario che conduce all'apprezzamento delle sue responsabilità».

[46] 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 online*, 28 maggio 2019, p. 20.

L'impiego di sistemi intelligenti dovrebbe, comunque, sempre risultare dall'ordinanza applicativa della misura cautelare, sebbene la motivazione resti a cura del giudicante umano; in tal modo, la difesa verrebbe a conoscenza dell'utilizzo della macchina computazionale e potrebbe esercitare il proprio diritto di acceso allo strumento per attingere ai dati di partenza utilizzati dal *software*: l'obiettivo sarebbe quello di riuscire a comprendere come si sia addivenuti ad un determinato risultato, verificando pure – magari con l'ausilio di un tecnico – la correttezza del processo algoritmico che si trova alla base della scelta automatica presa in considerazione dal magistrato.

In questo modo, le eventuali falle dell'*iter* decisorio potrebbero essere facilmente individuate e, nell'ipotesi in cui si ravvisi una lesione dei diritti fondamentali della persona sottoposta alle indagini preliminari, costituire un legittimo motivo di gravame cautelare.

5. La fase del *sentencing*.

Accertata la colpevolezza del soggetto imputato − segmento della decisione che, come si vedrà, deve necessariamente restare ad esclusivo appannaggio umano[47] − il giudice deve irrogare la sanzione prevista dalla norma incriminatrice, individuandone la specie e il *quantum*, barcamenandosi tra minimi e massimi edittali[48].

Non solo. Dovrà poi fornire idonea motivazione in ordine alla sua scelta: quale pena base per il calcolo del trattamento sanzionatorio, quali aumenti di pena (dovuti, ad esempio, a ipotesi di reato continuato)[49] e quali ragioni sono sottese a tali scelte.

---

[47] Si veda *infra*, Cap. IV.

[48] Sul dibattito tra natura e limiti della c.d. discrezionalità sanzionatoria, COPPOLA, *Commisurazione della pena e intelligenza artificiale: una ipotesi di lavoro con l'algoritmo Ex-Aequo*, in *Archivio penale web*, 2023, 2, pp. 8 ss.

[49] È quanto stabilito dalla giurisprudenza di legittimità, Cass., Sez. Un., 24 dicembre 2021, n. 47127, in *CED*, n. 282269 con nota di SILVA, *La continuazione di reati torna alle Sezioni Unite: la conferma - prevedibile - della necessità di indicare e motivare ciascun aumento di pena per i reati satellite*, in *Giurisprudenza italiana*, 2022, pp. 1719 ss.: «in tema di reato continuato, il giudice, nel determinare la pena complessiva, oltre ad individuare il reato più grave e stabilire la pena base, deve anche calcolare e motivare l'aumento di pena in modo distinto per ciascuno dei reati satellite. (La Corte ha precisato che il grado di impegno motivazionale richiesto in ordine ai singoli aumenti di pena è correlato all'entità degli stessi e tale da consentire di verificare che sia stato rispettato il rapporto di proporzione tra le pene, anche in relazione agli altri illeciti accertati, che risultino rispettati i limiti previsti dall'art. 81 cod. pen. e che non si sia operato surrettiziamente un cumulo materiale di pene). In argomento, si veda, altresì BATTISTONI, *Reato continuato: l'obbligo di*

Il legislatore nazionale, a garanzia della proporzionalità della pena, ha costruito il sistema sanzionatorio attraverso limiti edittali massimi e minimi, in grado di riflettere la gravità del reato e la diversa scala di disvalore di ogni fattispecie incriminatrice.

Resta, però, al giudice un ampio margine di discrezionalità (art. 132 c.p.): pur rimanendo entro il *range* di pena previsto, potrà collocarsi ove meglio crede, atteso che gli unici indicatori contemplati a livello codicistico sono la capacità a delinquere del colpevole e la gravità del reato (art. 133 c.p.).

Tuttavia, nonostante le raccomandazioni della Corte di legittimità, troppo spesso la motivazione in ordine alla scelta del trattamento sanzionatorio, sia nell'*an* che nel *quantum*, si riduce a formule di stile come "correttezza" e "adeguatezza" della pena comminata. Tali espressioni, perlopiù ripetitive, denotano un certo torpore argomentativo, che presta il fianco a legittimi atti di gravame, con conseguente ed inevitabile netto allungamento dei tempi della giustizia.

Dunque, nel poco tempo a disposizione in camera di consiglio prima della lettura del dispositivo in aula, il magistrato molto spesso finisce per rifarsi alla propria esperienza o alla mera intuizione per determinare la pena che gli sembra più giusta; d'altronde studi sull'euristica della decisione hanno appurato che «*animals, including humans, shape their behavior on the basis of experience*»[50].

Queste le pecche del modello commisurativo italiano che potrebbero essere attenuate – se non risolte – da una possibile interazione tra *AI* e giudice nella fase della determinazione della pena.

I sistemi algoritmici, infatti, potrebbero agevolmente affiancare il giudicante in tale delicato momento, al fine di ponderare il *quantum* di sanzione da irrogare e di valutare la concessione di benefici premiali, come la sospensione condizionale della pena *ex* artt. 163 ss. c.p.

---

indicazione e motivazione degli aumenti per i reati satellite, in *Diritto penale e processo*, 2022, pp. 638 ss.; CONZ, *La discrezionalità vincolata del giudice nella commisurazione del cumulo giuridico delle pene*, in *Cassazione penale*, 2022, pp. 1369 ss.; CONZ, *La sentenza delle Sezioni unite sull'onere per il giudice di calcolare e motivare l'aumento di pena per ciascuno dei reati uniti dal vincolo della continuazione*, in *Sistema penale online*, 20 gennaio 2021; ROMANELLI, *Aumenti di pena per la continuazione e obblighi motivazionali: le Sezioni unite tra novità e conservazione*, in *Processo penale e giustizia*, 2022, pp. 932 ss.

[50] SEYMOUR - SINGER - DOLAN, *The neurobiology of punishment*, in *Nature*, 2007, 8, p. 300.

I dati su cui riposerebbe la decisione algoritmica appartengono a due diverse tipologie: la prima risponde alla norma, la seconda all'orientamento giurisprudenziale.

Da un lato, infatti, è necessario che l'algoritmo si rifaccia ai medesimi indicatori forniti al giudice dall'art. 133 c.p.p. Dovranno, dunque, essere inseriti nell'applicativo, con riferimento alla gravità del reato (comma 1), informazioni circa la natura, la specie, i mezzi, l'oggetto, il tempo, il luogo e ogni altra modalità dell'azione, così come accertata nel corso del processo; la gravità del danno o del pericolo cagionato alla persona offesa dal reato; l'intensità del dolo o il grado della colpa stabilito dal giudice persona fisica. Gli elementi utili a desumere la capacità a delinquere (comma 2) sono, invece, i motivi a delinquere e il carattere del reo; i precedenti penali e giudiziari e, in genere, la condotta e la vita del reo, antecedenti al reato; la condotta contemporanea o susseguente al reato; le condizioni di vita individuale, familiare e sociale del reo.

Dall'altro lato, invece, è necessario estrarre informazioni dalla prassi sanzionatoria, al fine di garantire un equo trattamento punitivo tra i soggetti condannati per i medesimi reati, in presenza delle stesse circostanze aggravanti e attenuanti[51].

La fase di selezione di questi dati di *input* è certamente fondamentale per un buon esito della dosimetria della pena: il giudice attraverso l'individuazione di parole chiave riuscirebbe a restringere il campo dei precedenti giurisprudenziali, impartendo alla macchina delle linee guida attraverso le quali poter decidere.

A tale operazione dovrebbero poter partecipare anche le parti; in alternativa, ammettendo la possibilità di veder riconosciuto un mero contraddittorio postumo, la procedura seguita dovrebbe essere documentata e resa nota agli interessati per verificarne la linearità e la correttezza del percorso decisionale algoritmico.

Sarebbe, quindi, salvo il principio di individualizzazione del trattamento sanzionatorio[52], garantito dalla costante ed irrinunciabile presenza del giudice,

[51] Un interessante studio in materia, di cui si condivide l'impostazione, è stato condotto da COPPOLA, *Commisurazione della pena e intelligenza artificiale*, cit., 1 ss., che prospetta l'adozione di un modello algoritmico, che prende in nome di *Ex-Aequo*, capace di consentire una più agevole e trasparente valutazione dei precedenti al fine di assicurare uniformità sanzionatoria e di azzerare le discriminazioni o gli errori giudiziari causati da *bias* cognitivi o da propensioni personali del giudicante.

[52] Critico sul punto, MANES, *Intelligenza artificiale e giustizia penale*, cit., p. 282; GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., p. 3, secondo cui l'impiego di sistemi di

perno fondamentale intorno al quale deve continuare ad orbitare tale momento processuale; è il magistrato a ricevere il risultato algoritmico necessario per orientare la «commisurazione (della pena) umana»[53], assicurando così *empátheia* e *synthesis* alla decisione.

Oltre ad una miglior ponderazione della sanzione, pur senza rallentare i ritmi della camera di consiglio, altro innegabile vantaggio è rappresentato dalla maggiore uniformità e proporzionalità sanzionatoria che ne deriverebbe su tutto il territorio nazionale.

Dunque, in tale settore – in verità, come detto, privo di idonee garanzie capaci di regolare l'operato dell'uomo − i benefici legati all'*AI* supererebbero i rischi; la *machina sapiens* potrebbe essere impiegata nelle dinamiche decisorie unicamente quale ausilio alla deliberazione[54], che resta opportunamente nelle mani del giudice[55], unico soggetto capace di bilanciare le circostanze e gli interessi in gioco, la cui discrezionalità è orientata dall'algoritmo ma, allo stesso tempo, preservata da eventuali compromissioni.

6. L'esecuzione della pena e il regime penitenziario.

Di compatibilità tra *AI* e pericolosità sociale può parlarsi anche con riguardo al momento esecutivo: è qui, infatti, che la valutazione del rischio assume valore centrale per la differenziazione del regime sanzionatorio applicabile.

Preso atto delle criticità del sistema penitenziario italiano – fra tutte, quella relativa al sovraffollamento carcerario[56] − si ipotizzano soluzioni algoritmiche al fine di promuoverne l'efficientamento; il tutto avendo, però, cura di ponderare le possibili ricadute sui diritti fondamentali dei detenuti.

AI nel momento decisorio potrebbe determinare un pericoloso cambio di paradigma da "diritto penale del fatto" a "diritto penale dell'autore".

[53] COPPOLA, *Commisurazione della pena e intelligenza artificiale*, cit., p. 20.

[54] KOSTORIS, *Predizione decisoria e* diversion *processuale*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, cit., p. 110, afferma che bisognerebbe riconoscere all'intelligenza artificiale «una funzione esclusivamente ausiliaria e complementare della giustizia amministrata dagli uomini, volta a rafforzarne e ad amplificarne l'efficacia e le potenzialità».

[55] Come stabilito dal cons. 61), Reg. UE 2024/1689, «l'utilizzo di strumenti di IA può fornire sostegno al potere decisionale dei giudici o all'indipendenza del potere giudiziario, ma non dovrebbe sostituirlo: il processo decisionale finale deve rimanere un'attività a guida umana».

[56] Sul punto, CANESCHI, *Intelligenza artificiale e sistema penitenziario*, cit., p. 253.

Oltre all'implementazione di applicativi tecnologici capaci di migliorare il sistema di controllo inframurario[57] e di garantire uno *standard* di vita adeguato ai soggetti reclusi, si potrebbero introdurre modelli di riconoscimento biometrico per agevolare la procedura di accesso ai colloqui[58].

L'*AI*, poi, potrebbe operare nella giurisdizione di sorveglianza, pur senza provocarne un inutile ingessamento[59], intervenendo su aspetti puramente giurisdizionali: si pensi, ad esempio, alla decisione in ordine all'accesso a misure alternative alla detenzione[60] ovvero alle richieste di concessione di benefici penitenziari[61].

In tali casi, il magistrato dell'esecuzione deve verificare la sussistenza dei determinati presupposti: il residuo di pena (non superiore a diciotto mesi per l'esecuzione presso il domicilio della pena detentiva o non superiore a due anni per la concessione della detenzione domiciliare biennale generica); l'imminente pericolo di vita di un familiare o di un convivente; la sussistenza di una «regolare condotta» *ex* art. 30 *ter*, comma 1, l. 354/1975; l'assenza di pericolosità sociale; la prognosi positiva che il provvedimento di affidamento in prova al servizio sociale contribuisca alla rieducazione del condannato; la verifica dell'assenza di un «concreto pericolo di commissione di ulteriori delitti» *ex* art. 47 *quinquies*, l. 354/1975, per la detenzione domiciliare speciale; i «progressi compiuti nel corso del trattamento, quando vi sono le condizioni per un graduale reinserimento del

[57] Il riferimento è a sistemi anti-drone, *metal detector* fissi o di *body scanner* per impedire l'accesso di oggetto vietati nel luogo di detenzione. Sulle forme avanzate di controllo e sorveglianza con strumenti di *AI*, CANESCHI, *Intelligenza artificiale e sistema penitenziario*, cit., p. 264.

[58] Ne parla CANESCHI, *Intelligenza artificiale e sistema penitenziario*, cit., p. 255, secondo la quale l'uso di sistemi di *AI* biometrica semplificherebbe le operazioni di identificazione, atteso che «la ricognizione automatica del dato permetterebbe infatti alle persone già registrate nel sistema di entrare e di uscire dall'istituto nella giornata del colloquio senza l'articolata procedura di registrazione cartacea, con un evidente risparmio di tempo e di risorse in termini organizzativi».

[59] Ricorda FIORIO, *Predizione algoritmica e giurisdizione di sorveglianza*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, cit., p. 259, che il magistrato di sorveglianza, dopo il suo inserimento nella l. 26 luglio 1975, n. 354, svolgeva funzioni puramente amministrative e quasi prive di spessore giurisdizionale; soltanto con la l. 10 ottobre 1986, n. 354, con il potenziamento delle misure alternative alla detenzione sono state riviste le funzioni del magistrato di sorveglianza, aumentandone i poteri, destinati a subire una notevole estensione nel corso del tempo (si veda, l. 27 maggio 1988, n. 165, con la quale si è intervenuto sul meccanismi di cui all'art. 656, comma 5, c.p.p., consentendo al giudicante di esprimersi sull'effettività dell'ordine amministrativo di esecuzione, sancendo la priorità della rieducazione sulla forza del giudicato).

[60] Le misure alternative alla detenzione sono disciplinate dagli artt. 47, 47 *ter*, 47 *quater*, 47 *quinquies* e 50, l. 354/1975 nonché dall'art. 94 d.P.R. 9 ottobre 1990, n. 309.

[61] I benefici penitenziari sono contemplati dagli artt. 21, 30, 33 *ter* e 54, l. 354/1970.

soggetto» (art. 50, l. 354/1975) per la concessione della semilibertà; la documentazione rilasciata da una struttura sanitaria attestante lo stato di tossicodipendenza ai sensi dell'art. 94, d.P.R. 309/1990 e l'accertamento di precarie condizioni economiche[62].

Nel dettaglio, nel procedimento di sorveglianza "ordinario" – per differenziarlo dal regime del c.d. "doppio binario" di cui all'art. 4 *bis*, l. 354/1975 –, attraverso il quale si valuta l'efficacia rieducativa del percorso ai sensi dell'art. 27, comma 3, Cost., il giudice può fondare l'istruzione su prove documentali, a cui riconoscere un «ruolo di assoluta preminenza»[63]: l'art. 678, comma 2, c.p.p., ad esempio, impone di acquisire la documentazione relativa all'osservazione scientifica condotta sulla personalità del soggetto interessato, avvalendosi pure della collaborazione dei tecnici del trattamento.

Sulla base di tale materiale raccolto, però, al magistrato viene poi richiesto un complesso sforzo d'immaginazione: per l'affidamento in prova al servizio sociale deve valutare che la misura «assicuri la prevenzione del pericolo che egli commetta altri reati» (art. 47, l. 354/1975); la detenzione domiciliare può essere concessa quando è reputata «idonea ad evitare il pericolo che il condannato commetta altri reati» (art. 47 *ter*, comma 1 *bis*, l. 354/1975), mentre quella speciale solo «se non sussiste un concreto pericolo di commissione di ulteriori delitti» (art. 47 *quinquies*, l. 354/1975); il regime di semilibertà è, invece, riconosciuto quando «vi sono le condizioni per un graduale reinserimento» del soggetto nella compagine sociale (art. 50, l. 354/1975); anche i c.d. premessi premio (art. 30 *ter*, l. 354/1975) sono subordinati all'assenza di pericolosità, oltre che al requisito della buona condotta.

Non solo. Per la verifica del superamento della c.d. ostatività penitenziaria *ex* art. 4 *bis*, l. 354/1975 l'attività di valutazione è ancora più complessa.

Infatti, per l'accesso ai benefici o alle misure alternative per i delitti menzionati in detta norma è necessario verificare la sussistenza di una serie di elementi: il *tempus commissi delicti*; la collaborazione *omnibus* (c.d. pentismo); la collaborazione con la giustizia *ex* artt. 4 *bis* e 58 *ter*, l. 354/1975 nonché di cui all'art. 323 *bis* c.p.; per i soggetti non collaboranti, invece, è necessario accertare la oggettiva irrilevanza,

[62] Sull'indicizzazione dei presupposti per benefici penitenziari e misure alternative, FIORIO, *Predizione algoritmica e giurisdizione di sorveglianza*, cit., p. 271

[63] FIORIO, *Predizione algoritmica e giurisdizione di sorveglianza*, cit., p. 261.

impossibilità o inesigibilità di una utile collaborazione con la giustizia o, in alternativa, l'adempimento alle obbligazioni civili ovvero la dimostrazione dell'assoluta impossibilità di tale adempimento; i risultati dell'osservazione scientifica della personalità; la positiva partecipazione al programma psicologico ai sensi dell'art. 13 *bis*, l. 354/1975[64].

A ciò si aggiunga che l'*iter* di valutazione delle istanze di accesso a benefici premiali è mutato a seguito della recente riforma dell'ordinamento penitenziario[65]: per i delitti di cui all'art. 4 *bis*, comma 1, vi è un sistema fondato su condizioni e presupposti che il richiedente, non collaborante, deve necessariamente allegare e documentare per escludere l'attualità del pericolo che ripristini collegamenti con l'associazione criminale di appartenenza; per i reati di cui all'art. 4 *bis*, comma 1 *bis*, è opportuno che il non collaborante provi l'inesistenza dell'attualità dei collegamenti (e non la possibilità di rispristino dei medesimi) con il contesto criminale in cui l'azione criminosa è stata consumata.

Ebbene, la complessità di questo grappolo di condizioni da valutare suggerisce la necessità di un ripensamento globale della normativa, orientato alla semplificazione, magari proprio in prospettiva algoritmica.

Da un lato, l'*AI* potrebbe restituire una corretta prognosi di pericolosità sociale, decretandone l'assenza – o, al contrario, la sussistenza − ai fini della concessione di un beneficio penitenziario.

Dall'altro lato, a voler pensare in grande, la macchina computazionale potrebbe contenere tutti i dati da analizzare riferiti al singolo soggetto, per decidere se ammettere o meno il condannato ad una misura alternativa alla detenzione; tale prospettiva, ovviamente, non vorrebbe condurre ad una sostituzione della magistratura con i sistemi artificiali. Semplicemente, si ritiene che una decisione basata sulla logica della probabilità e non sull'immaginazione del giudicante potrebbe, forse, offrire più certezze e garanzie.

La decisione della magistratura di sorveglianza deve, altresì, tenere conto delle informazioni dettagliate rese dal Comitato provinciale per l'ordine e la sicurezza pubblica territorialmente competente (comma 2) e, qualora trattasi di fattispecie

[64] Sull'indicizzazione degli elementi relativi al superamento della c.d. ostatività penitenziaria, FIORIO, *Predizione algoritmica e giurisdizione di sorveglianza*, cit., pp. 266 ss.

[65] Si tratta del d.l. 31 ottobre 2022, n. 162, conv. dalla l. 30 dicembre 2022, n. 199.

incriminatrici comprese nell'art. 51, commi 3 *bis* e 3 *quater*, c.p.p., del parere del pubblico ministero presso il giudice che ha emesso la condanna in primo grado e del Procuratore nazionale antimafia e antiterrorismo; essenziali pure le informazioni fornite dalla Direzione dell'istituto di pena, gli esiti degli accertamenti reddituali e patrimoniali disposti sull'istante e sul suo nucleo familiare nonché eventuali elementi di prova contraria quando dall'istruttoria emergono indizi che farebbero supporre l'attualità dei collegamenti con la criminalità organizzata.

Allo scopo di favorire la formazione e la condivisione di dette informazioni, necessarie per la decisione, è già stata istituita una "Area sicura di condivisione informativa" (chiamata "Procedure 4 *bis* ord. pen."), all'interno del "Sistema Informativo Direzione Nazionale Antimafia" (SIDNA), che raccoglie una cospicua mole di dati, organizzati in cartelle personali, che diventano così immediatamente fruibili dal giudice[66].

L'immediata evoluzione di un sistema di raccolta dei dati come questo potrebbe essere la messa a punto di un applicativo capace di analizzare le informazioni già raccolte e catalogate; incrociando i dati disponibili il *software* sarebbe così in grado di proporre al magistrato una possibile soluzione.

Questo richiederebbe, certamente, una riscrittura degli indici di riferimento che, talvolta, assumono connotati «metagiuridici»[67] e una decriptizzazione del *legal writing* affinché sia comprensibile dal sistema artificiale.

Al fine di evitare inaccettabili discriminazioni e di ottenere un risultato quanto più "giusto" possibile, si potrebbero pensare di bandire dall'istruttoria algoritmica «le informative datate che si limitano ad una mera declinazione dei precedenti penali o dei precedenti titoli custodiali della pena per cui il condannato si trova in esecuzione»[68].

Orizzonte certamente affascinante è, dunque, quello che vedrebbe coinvolta l'*AI* nella fase esecutiva della pena, al netto di una sostanziale revisione della normativa di riferimento in un'ottica di semplificazione.

Quello riconosciuto alla macchina sarebbe, però, un ruolo meramente subalterno, atteso che, in accordo con le disposizioni europee e, in particolare, con la

[66] In argomento, CANESCHI, *Intelligenza artificiale e sistema penitenziario*, cit., p. 259.
[67] FIORIO, *Predizione algoritmica e giurisdizione di sorveglianza*, cit., p. 274.
[68] Sul punto, ancora, FIORIO, *Predizione algoritmica e giurisdizione di sorveglianza*, cit., p. 274

raccomandazione del *Council for Penological Co-operation* (*PC-CP*), affidare in via esclusiva alle macchine le valutazioni in ordine al pericolo di recidiva del condannato sarebbe imprudente; tale scelta non terrebbe conto delle problematiche legate all'attuale incertezza del loro funzionamento e al rischio di fallibilità.

7. L'*iter* di formazione del *dataset*: il contraddittorio *sulla* e *per* la prova.

È ormai innegabile che «la scienza e la tecnologia irrompono nel crogiuolo dell'esperienza giuridica»[69]. In tempi non troppo lontani, infatti, l'«oracolo algoritmo»[70] potrà integrare il patrimonio conoscitivo del giudice, a patto che − come ci insegna l'esperienza nordamericana − non sia l'unico elemento sulla base del quale decidere.

A tal fine, occorre qualche precisazione sul valore da riconoscere all'*output*.

L'approccio muta in base alla differente catalogazione dei sistemi artificiali cui si vuole far riferimento: se si inquadrasse l'applicativo come "strumento di predizione a fini decisori" il giudice si troverebbe a disattendere un dato probatorio di tipo scientifico[71], con conseguente obbligo di darne conto nella motivazione del provvedimento da adottare ai sensi degli artt. 192, comma 1, e 546, comma 1, lett. e), c.p.p. Al contrario, qualora si considerasse come "predizione decisoria", porrebbe in essere un comportamento sostanzialmente equiparabile alla mancata adesione ad un precedente orientamento giurisprudenziale[72].

A prescindere da ogni catalogazione, sembrerebbe che l'operazione condotta dalla macchina debba assumere i caratteri della scientificità e, dunque, essere «*subject to the restraints self-imposed by scientific method*»[73] affinché il risultato sia spendibile processualmente.

---

[69] Così, CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, cit., p. 130.

[70] MANES, *L'oracolo algoritmico e la giustizia penale*, cit., p. 1.

[71] KARNOW, *The Opinion of Machine*, in AA.VV., *The Cambridge Handbook of the Law of Algorithms*, Barfield (*edited by*), Cambridge, 2021, p. 17, secondo il quale «*judges must have sufficient knowledge to handle the technical issues. Furthermore, appreciating the risks involved, judges must also have the legal authority to decide whether the software is scientifically reliable*».

[72] Detta *summa divisio* è tracciata da KOSTORIS, *Predizione decisoria e* diversion *processuale*, cit., p. 96.

[73] È quanto affermato da ASHWORTH - ZEDER, *Preventive Justice*, cit., p. 133, le quali riprendono il pensiero di SIMON, *Reversal of Fortune: The Resurgence of Individual Risk assessment in Criminal Justice*, in *Annual Review of Law and Social Science*, 2005, pp. 397 ss.; in tal senso pure BACCARI

Il riferimento è al c.d. *Dauber test*, coniato dalla giurisprudenza statunitense[74], che potrebbe costituire la prima necessaria verifica cui sottoporre i modelli computazionali.

Tali criteri sono stati importati pure nel contesto processuale italiano e reinterpretati dai giudici di legittimità: ai consueti requisiti di verificabilità, falsificabilità, sottoposizione al controllo della comunità scientifica, conoscenza del tasso di errore e generale accettazione da parte della comunità di esperti, si aggiungono i nuovi criteri di affidabilità e indipendenza della teoria, della considerazione delle finalità, della possibilità di individuare indici di scelta tra le contrapposte tesi scientifiche[75]. Ponendosi in questo angolo visuale, si ammetterebbe, quindi, un contraddittorio soltanto postumo *sulla* prova "scientifica", lasciando all'autonomia del giudice la scelta in ordine all'inserimento dei dati di *input*. In tal caso, la contrapposizione dialettica tra le parti potrebbe essere assicurata esclusivamente dall'impiego, da parte della difesa, delle «istruzioni per l'uso» del *software*[76], attraverso cui poter verificare, in primo luogo, se la macchina sia stata impiegata in maniera conforme alle finalità previste dal fornitore e, in secondo luogo, se la qualità dei dati immessi sia sufficiente a produrre un riscontro privo (o meno) di *bias*.

- PECCHIOLI, *I.A. e giudizio sul fatto: gli strumenti di* e-evidence *per la cognizione*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, cit., pp. 125 ss.

[74] Il riferimento è alla sentenza *Daubert v. Merrel Dow Pharmaceuticals*, Inc., 509 U.S. 579, 113 S. Ct. 2786 (1993).

[75] Cfr., Cass., sez. IV, 13 settembre 2010, n. 43786, con nota di TONINI, *La Cassazione accoglie i criteri Daubert sulla prova scientifica. Riflessi sulla verifica delle massime di esperienza*, in *Diritto penale e processo*, 2011, pp. 1341 ss.

In dottrina, per una più ampia analisi del concetto di prova scientifica si veda, tra i tanti, CANZIO - LUPARIA DONATI (a cura di), *Prova scientifica e processo penale*, Milano, 2022, II ed.; CANZIO, *La valutazione della prova scientifica fra verità processuale e ragionevole dubbio*, in *Archivio penale*, 2011, 3, p. 1 ss.; CANZIO, *Prova scientifica, ricerca della "verità" e decisione giudiziaria nel processo penale*, in AA. VV., *Scienza e causalità*, Di Maglie - Seminara (a cura di), Padova, 2006, pp. 143 ss.; CAPRIOLI, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cassazione penale*, 2008, pp. 3520 ss.; CATALANO - CURTOTTI NAPPI - DELLA MONICA - LORUSSO - MONTAGNA – PROCACCINO (a cura di), *Prova penale e metodo scientifico*, Torino, 2009; CECCHI, *Il giudice dinanzi alla prova scientifica*, in *Archivio penale web*, 2022, 1, pp. 1 ss.; CONTI, *La prova scientifica alle soglie dei vent'anni dalla sentenza Franzese: vette e vertigini in epoca di pandemia*, in *Sistema penale online*, 9 febbraio 2021; CUPELLI, *Prova scientifica, regole cautelari e responsabilità medica*, in *Sistema penale online*, 14 marzo 2023; DE CATALDO, *L'operazione decisoria da emanazione divina alla prova scientifica*, Padova, 2014; DOMINIONI, *La prova penale scientifica*, Milano, 2005; LORUSSO, *Prova scientifica*, in AA. VV., *La prova penale*, Gaito (diretto da), II, Torino, 2008, pp. 319 ss.

[76] Cfr. art. 3, n. 15), Reg. UE 2024/1689.

In tal modo, però, si rischia di rievocare l'antica diatriba sulla effettiva scientificità del metodo da applicare, amplificata dalle problematiche ontologiche ai sistemi di *AI*, quali i *deficit* strutturali di trasparenza e l'impenetrabilità della c.d. *black box*[77]. Per risolvere l'*impasse*, sarebbe più corretto se la scelta dei dati da immettere nel sistema per generare l'*output* avvenisse nel contraddittorio anticipato tra le parti.

Dunque, potrebbe essere utile costruire un filtro di accesso preventivo al *software* per escludere che prove inadeguate entrino nel patrimonio conoscitivo del giudice[78]. Si tratterebbe di un contraddittorio *per* la prova, analogo a quello previsto in materia di prova atipica *ex* art. 189 c.p.p.[79]; tale cornice normativa risponde, infatti, all'esigenza di garantire che il processo sia aperto alle innovazioni tecnologiche[80], assicurando un accertamento sull'attendibilità del risultato *ex ante*[81].

Probabilmente sarebbe, però, complicato parlare di contraddittorio anticipato in momenti come quello cautelare o preventivo che, per loro stessa natura, vietano di svelare al destinatario il provvedimento che si sta per adottare; in questa parentesi procedimentale, il contraddittorio, pur sempre garantito, non può che essere soltanto postumo, consentendo alle parti di offrire il proprio punto di vista dopo aver analizzato la documentazione relativa all'impiego dell'algoritmo per evidenziare eventuali falle attraverso gli strumenti impugnatori.

---

[77] Sul punto, BACCARI - PECCHIOLI, *I.A. e giudizio sul fatto: gli strumenti di* e-evidence *per la cognizione*, cit., pp. 132-133; GABBRIELLI, *Dalla logica al* deep learning: *una breve riflessione sull'intelligenza artificiale*, in AA.VV., *XXVI lezioni di diritto dell'intelligenza artificiale*, cit., p. 30.

[78] In tal senso pure CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, cit. p. 130.

[79] Considera troppo semplicistico il rinvio all'art. 189 c.p.p., BACCARI - PECCHIOLI, *I.A. e giudizio sul fatto: gli strumenti di* e-evidence *per la cognizione*, cit., pp. 121-122: «vi è una chiara tendenza, in una parte della dottrina e della giurisprudenza, di classificare i nuovi ritrovamenti del progresso scientifico-tecnologico come prova atipica. Ebbene, a nostro modo di vedere, siffatta lettura rappresenta una sorta di "richiamo abusivo" dell'istituto tratteggiato dall'art. 189 del codice di rito: abuso fondato sul fraintendimento per cui la novità del metodo scientifico implicherebbe di necessità l'atipicità del mezzo di prova da esperirsi per la formazione dell'elemento conoscitivo».

[80] Cfr., Reazione al Progetto preliminare al codice di procedura penale del 1988, p. 60, che, nel chiarire la *ratio* dell'art. 189 c.p.p., precisa «è sembrato che una norma così articolata possa evitare eccessive restrizioni ai fini dell'accertamento della verità, tenuto conto del continuo sviluppo tecnologico che estende le frontiere dell'investigazione, senza mettere in pericolo le garanzie difensive».

[81] CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, cit. p. 130, secondo il quale, attraverso il meccanismo di cui all'art. 189 c.p.p., «allo scopo di garantire l'anticipata conoscenza delle parti circa le metodologie che saranno applicate nell'accertamento, il giudice, dopo aver sentito le parti sulle modalità di assunzione della prova, provvede all'ammissione con ordinanza, fissando le regole per la corretta applicazione dei metodi e delle procedure tecniche di acquisizione della stessa».

Tuttavia, alla luce della recente introduzione dell'inedita figura del c.d. interrogatorio cautelare preventivo, probabilmente si aprirebbe un varco per il l'impiego di sistemi algoritmici; ciò in quanto, in occasione di detto momento partecipativo, si potrebbe procedere alla selezione delle informazioni da inserire nel *dataset* del sistema di *AI*, assicurando alle parti proprio quell'irrinunciabile contraddittorio *per* la prova.

Più agevole è, invece, il discorso relativo alla fase della determinazione della pena o dell'esecuzione della medesima atteso che, qui, può certamente ritagliarsi un momento in cui le parti, in contraddittorio, siano abilitate ad intervenire nell'*iter* di formazione del *dataset* che la macchina deve utilizzare per la decisione.

Il medesimo discorso deve essere esteso anche al possibile rapporto tra *AI* e *standard* di giudizio[82], atteso che l'utilizzabilità processuale del dato algoritmico deve necessariamente essere subordinata alla garanzia del contraddittorio, meglio se anticipato.

Pertanto, pur ammettendo che debba comunque esserci una rispondenza scientifica del metodo algoritmico utilizzato dal sistema, questa teoria, da sola, potrebbe non trovare un effettivo sbocco applicativo in ragione della necessità di garantire alle parti una partecipazione dialettica attiva nelle fasi preparatorie e prodromiche all'utilizzo dell'*AI*; la selezione dei dati di *input* costituisce, infatti, il delicato momento in cui si stabiliscono le sorti della risposta artificiale.

Pertanto, tale momento deve necessariamente svolgersi nel contraddittorio (se possibile, anticipato) tra le parti e in condizioni di parità, dinanzi ad un giudice terzo ed imparziale, in ossequio ai dettami del *fair trial*.

[82] Su cui *infra*, Cap. IV.

CAPITOLO IV

DECISIONE ALGORITMICA E *STANDARD* DI GIUDIZIO

SOMMARIO: 1. L'incerta traducibilità del dato normativo e il valore del precedente. 2. *AI* e regole decisorie. 3. La "ragionevole previsione di condanna": dall'archiviazione …; 4. … alla sentenza di non luogo al procedere; 5. L'accertamento della responsabilità oltre ogni ragionevole dubbio. 6. L'imprescindibile centralità del giudice.

1. L'incerta traducibilità del dato normativo e il valore del precedente.

Lo «tsunami digitale»[83] che ha colpito la società contemporanea e il mondo giuridico ci incoraggia a prospettare l'ingresso dell'*AI* nel processo penale, in un'ottica in cui i modelli computazionali sarebbero in grado di favorire un livello elevato di certezza del diritto[84] e di prevedibilità della decisione, al fine di assicurare una maggiore efficienza dell'intero sistema giustizia.

L'algoritmo si compone di una sequela finita di istruzioni ripetibili e univoche, che indicano una combinazione di azioni da compiere per risolvere un determinato problema; affinché sia possibile offrire una specifica soluzione, si avvale di comandi espressi con un linguaggio formale di programmazione – evidentemente diverso da quello umano – in grado di essere compreso dal calcolatore per trasformare i dati di *input* in *output*.

Questioni controverse sorgono, però, nel momento in cui si deve addestrare la macchina per fornirle i parametri di funzionamento[85], mediante il c.d. *natural language processing*[86] che mira al trattamento informatico del linguaggio umano.

---

[83] L'espressione è di GALGANI, *Considerazioni sui "precedenti" dell'imputato e del giudice al cospetto dell'IA nel processo penale*, in *Sistema penale*, 2020, 4, p. 82.

[84] Analizza il rapporto tra certezza del diritto e intelligenza artificiale, BARONE, *Giustizia Predittiva e Certezza del Diritto*, Pisa, 2024, pp. 99 ss.

[85] Sulle tre tipologie di apprendimento automatico (supervisionato, non supervisionato e per rinforzo), MOSCATO, Calculemus? *Da Leibniz all'intelligenza artificiale*, in *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, pp. 30 ss.

[86] Quest'approccio utilizza tecniche di apprendimento automatico che estrapolano le regole grammaticali tipiche del linguaggio comune attraverso l'analisi di una moltitudine di testi.
In passato, invece, per "tradurre" il linguaggio umano e renderlo comprensibile all'algoritmo, ci si avvaleva di linguisti che coadiuvavano i programmatori nel processo di trasposizione delle regole di sintassi e di grammatica nel *software*.

Infatti, pur riuscendo a raggiungere ottime prestazioni dal punto di vista linguistico, non è ancora in grado di processare i dati in funzione semantica e di capirne il reale significato; le problematiche connesse alla traducibilità della lingua comune[87] aumentano in maniera esponenziale quando si tratta di parametri giuridici.

Operando in base a calcoli matematici, sarebbe opportuno decodificare il linguaggio utilizzato nelle controversie, *ivi* comprese le regole probatorie e quelle decisorie, affinché l'apparato digitale possa comprendere dette informazioni e applicarle nei suoi percorsi di "scelta".

Ogni tentativo di trovare una perfetta sintesi tra *AI* e processo penale si scontra, però, con un ostacolo, ad oggi, quasi insormontabile: l'oscurità della eccessiva – e, probabilmente, inutile – complessità delle leggi.

Soltanto realizzando la tanto auspicata disambiguazione del linguaggio giuridico sarebbe, quindi, possibile individuare un punto di equilibrio: l'obiettivo da raggiungere è costruire un diritto certo nella sua formulazione linguistica, che non dia spazio a stravaganti interpretazioni e che sia capace di soddisfare le esigenze di chiarezza della norma.

Ciò in quanto, se negli ordinamenti di *common law* la macchina viene allenata con dati relativi alle precedenti pronunce giurisprudenziali, nei sistemi di *civil law* sarebbe necessario fornire al *software* parametri diversi.

Al fine di scongiurare il reale pericolo di commistione tra due opposti sistemi giuridici[88] (probabilmente già in atto), infatti, sarebbe il dato normativo a dover essere decifrato, atteso che nei sistemi di *civil law* «decidere significa soprattutto motivare, in chiave dialettica e confutativa e non può risolversi in un'applicazione di precedenti giurisprudenziali secondo una logica puramente binaria»[89].

Secondo parte della dottrina, ammettere che il giudice possa conformarsi soltanto ai precedenti giurisprudenziali significherebbe anche essere disposti a delle

[87] MOSCATO, Calculemus? *Da Leibniz all'intelligenza artificiale*, cit., pp. 25 ss.

[88] In termini più moderati, PALAZZO, *Considerazioni minime sulla prevedibilità della decisione giudiziale (tra miti, illusioni e pragmatismi)*, in *Cassazione penale*, 2022, p. 943, secondo cui il principio di prevedibilità, che nasce sul terreno del diritto giurisprudenziale, è il segno «di quell'avvicinamento, unanimemente riconosciuto, tra sistemi di *civil law* e sistemi di *common law*: un fenomeno davvero radicato in tendenze "globalizzanti" che paiono capaci di vincere qualunque resistenza nazionalistica e segnare piuttosto l'attuale direzione della storia».

[89] CATERINI, *Il giudice penale* robot, in *La legislazione penale*, 19 dicembre 2020, p. 15.

importanti rinunce[90]: da un lato, verrebbe meno il possibile *overrulling* della risoluzione di una questione controversa[91] e, dall'altro lato, vi sarebbe l'abdicazione del giudice al fondamentale compito di interpretare la legge – e non un precedente giurisprudenziale − in chiave evolutiva.

Tale prospettiva non è, però, condivisibile in quanto evidentemente estrema.

In primo luogo, l'*AI* non sostituirebbe mai il giudice nella sua decisione, limitandosi ad offrire competenze di cui l'uomo, oggettivamente, non potrà mai disporre, se non affidandosi al suo intuito; il riferimento è chiaramente alla previsione relativa al futuro comportamento dell'indagato/imputato o alla sorte di un processo[92].

In secondo luogo, qui si prospetta l'idea di una giustizia predittiva limitata a porzioni di segmenti decisori, escludendo che la valutazione sia interamente affidata all'algoritmo; la critica, dunque, non attecchisce.

Last but not least, il giudice che resta «saldato sul sacro scranno decisionale»[93], potrà sempre discostarsi dall'*output* reso dalla macchina computazionale, dandone conto nella motivazione del provvedimento da adottare[94].

Per cui, coscienti dell'esistenza di limiti, attualmente insuperabili, legati all'incerta traducibilità del dato normativo, non si vedono profili di incompatibilità sistematica assoluta all'inserimento dei precedenti giurisprudenziali quali parametri "legali" utili per la risposta algoritmica.

Tra l'altro, è lo stesso art. 628, comma 1 *bis*, c.p.p. a legittimare «un sistema di vincolo relativo al precedente emesso dalle Sezioni Unite, senza peraltro indurre

---

[90] LUCIANI, *La decisone giudiziaria robotica*, in AA.VV., *Decisione robotica*, Carleo (a cura di), Bologna, 2019, p. 86, afferma che «vincolare il *robot* alla giurisprudenza pregressa impedisce l'evoluzione degli indirizzi giurisprudenziali e preclude al diritto di esercitare la sua funzione primaria (rispondere a bisogni umani regolando umani rapporti corrispondentemente alle esigenze sociali del momento storico)».

[91] Al contrario, evidenzia l'esigenza di stabilizzazione della giurisprudenza, DI GIOVINE, *Il* judge-bot *e le sequenze giuridiche in materia penale*, in *Cassazione penale*, 2020, p. 952, precisando che «poiché al consolidamento della giurisprudenza osta (tra le altre cose) un carico giudiziario così gravoso da impedire un ottimale impiego delle risorse umane e da sottrarre ai giudici il tempo necessario ad approfondire le questioni più controverse, va da sé che un contributo allo smaltimento di tale carico e quindi al consolidamento della giurisprudenza potrebbe venire dall'intelligenza artificiale (di seguito, AI)».

[92] Vedi *infra*, § 4.

[93] LUPARIA DONATI, *Notazioni controintuitive su intelligenza artificiale e libero convincimento*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, cit., p. 116.

[94] Sul punto, infra, § 6.

automatismi o rigidità tali da rischiare di ingessare l'evoluzione del diritto giurisprudenziale»[95].

Dunque, ammettere che il *software* possa decidere anche in base al consolidato orientamento della giurisprudenza di legittimità – salvaguardando il mutamento giurisprudenziale favorevole al reo[96] − e riconoscendone una sorta di vincolatività in *bonam partem* del precedente[97], non parrebbe essere una cattiva soluzione[98].

Pure le sentenze di merito potrebbero rientrare in questo *panel*[99]: avrebbero, infatti, un ruolo determinante in quanto offrirebbero dati concreti, riferibili a casi simili, attraverso i quali la macchina può gestire la sua "decisione"[100].

Si potrà ritornare sulla faccenda quando, in futuro, nuovi sviluppi tecnologici renderanno praticabile l'immissione del dato normativo, seppur ancora spurio e da perfezionare, nella macchina computazionale.

In tale prospettiva, «il ruolo ancillare ma istituzionalizzato dell'algoritmo predittivo nel processo servirebbe da filtro idoneo a contrastare la giurisprudenza gratuitamente creativa, senza scoraggiare quella meritoriamente evolutiva»[101],

---

[95] Così, PALAZZO, *Considerazioni minime sulla prevedibilità della decisione giudiziale*, cit., pp. 951 ss.; in argomento, si veda, altresì, CADOPPI, *Il valore del precedente nel diritto penale*, Torino, 1999, pp. 109 ss.; FIDELBO, *Verso il sistema del precedente? Sezioni Unite e principio di diritto*, in AA.VV., *La riforma delle impugnazioni tra carenze sistematiche e incertezze applicative*, Bargis - Belluta (a cura di), Torino, 2018, pp. 115 ss.

[96] CATERINI, *Il giudice penale robot*, cit., p. 4, secondo cui se «l'apertura dei "cancelli delle parole" sospinge verso esiti interpretativi più favorevoli all'imputato, l'atteggiamento del giudice potrà essere meno rigido, secondo il modello delle direttive ermeneutiche, perciò aperto anche a soluzioni metatestuali purché in attuazione sistematica dei princìpi costituzionali. Consentire, viceversa, al Türhüter di aprire i "cancelli delle parole" verso esiti più sfavorevoli, implica la delega di compiti d'indirizzo sociale che trasforma i giudici nei principali attori della politica criminale, spesso più influenti dello stesso legislatore».

[97] Di questa opinione è CATERINI, *Il giudice penale robot*, cit., p. 21, per cui «il funzionamento di un sistema esperto sulla base dei precedenti giurisprudenziali, infatti, potrebbe operare calcolando una serie di opzioni interpretative tra le quali dovrebbe scegliere non quella statisticamente più frequente, ma quella più favorevole all'imputato».

[98] *Contra*, FRONZA - CARUSO, *Ti faresti giudicare da un algoritmo? Intervista a Antoine Garapon*, in *Questione giustizia*, 2018, 4, p. 196, in cui Garapon, afferma che la giustizia predittiva si basa sulla «sostituzione della capacità di ragionamento (giuridico) con la capacità computazionale» e «non si nutre di conoscenze giuridiche ma di dati (ossia le informazioni su casi simili) in cui tali conoscenze siano state già digerite e applicate»; palesa, dunque, il rischio di commistione tra diritto e fatto atteso che «nel momento in cui il diritto viene limitato dalle regolarità osservate dai pratici, l'idea stessa di una causalità giuridica scompare e restano solo dei collegamenti fra parentesi».

[99] Evidenzia i rischi legati alla valorizzazione di precedenti giurisprudenziali dell'imputato o del singolo magistrato giudicante, GALGANI, *Considerazioni sui "precedenti" dell'imputato e del giudice al cospetto dell'IA nel processo penale*, cit., pp. 81 ss.

[100] Sul punto, *infra*, § 4.

[101] RUFFOLO, *La* macchina sapiens *come "avvocato generale" ed il primato del giudice umano*, in AA.VV., *XXVI lezioni di diritto dell'intelligenza artificiale*, Ruffolo (a cura di), Torino, 2021, pp. 217.

assumendo una funzione correttiva e dissuasiva rispetto a decisioni potenzialmente devianti.

2. *AI* e regole decisorie.

Il processo penale s'innerva «intorno ai concetti di ipotesi e fatti, indizi e prove, contraddittorio, verità e dubbio, conferma e falsificazione dell'ipotesi, giustificazione razionale della decisione, controllo impugnatorio della motivazione»[102].

Per giungere ad una corretta ricostruzione della verità processuale, intesa come naturale prodotto dell'ordinario svolgimento dell'*iter* procedimentale, il legislatore ha dettato precise regole che stabiliscono tempi e modalità dell'accertamento.

L'obiettivo della "sfida adattiva" che qui si propone di compiere è quello di comprendere se e in quali termini sia possibile l'ingresso di modelli computazionali tra gli snodi della decisione penale, compatibilmente con le regole decisorie *ivi* previste.

Protagonisti saranno, dunque, lo *standard* della ragionevole previsione di condanna e quello dell'oltre ogni ragionevole dubbio; l'uno è il criterio di giudizio adottato per il provvedimento di archiviazione e per la sentenza di non luogo a procedere, l'altro il canone da seguire nella decisione dibattimentale sul fatto.

Quanto al primo, introdotto dalla c.d. riforma Cartabia, avviata con il d.lgs. 10 ottobre 2022, n. 150 − che ha adottato un approccio quasi "ingegneristico" nel tentativo di incrementare l'efficienza del processo penale[103] −, propone una nuova tipologia di accertamento giurisdizionale pressoché "automatizzata"[104].

---

[102] CANZIO, *Intelligenza artificiale e processo penale*, in AA.VV., *Prova scientifica e processo penale*, Canzio - Luparia Donati (a cura di), ed. II, Milano, 2022, p. 904.

[103] Ciò in quanto l'inadeguatezza dell'udienza preliminare di assolvere alla propria funzione di filtro avverso le imputazioni azzardate rendeva necessario un intervento riformatore (cfr. DANIELE, *La riforma Cartabia del processo penale: pretese algoritmiche ed entropia sistemica*, in *Sistema penale*, 2023, 7-8, p. 21; DELLA MONICA, *Il filtro della ragionevole previsione di condanna*, in *Archivio penale*, 2023, 2, p. 9). Tale criticità, infatti, aveva persino indotto la dottrina a dubitare della sua effettività utilità, prospettandone addirittura l'abrogazione (La proposta è di DANIELE, *L'abolizione dell'udienza preliminare per rilanciare il sistema accusatorio*, in *Sistema penale*, 2020, 1, pp. 131 ss.).

[104] In questo senso, DANIELE, *La riforma Cartabia del processo penale: pretese algoritmiche ed entropia sistemica*, cit., p. 20: «mi sembra, nondimeno, che un aspetto di novità stia nel modo in cui la riforma Cartabia prova ad ottenere l'efficienza: la quale viene rincorsa attraverso una mentalità ingegneristica e meccanismi che non esiterei a definire "algoritmici", che hanno come tratto caratterizzante la volontà di governare l'accertamento giurisdizionale mediante criteri decisori e

Infatti, i *conditores* optando per un potenziamento della «capacità "drenante" dell'udienza preliminare»[105], hanno introdotto la nuova regola *ex* art. 425, comma 3, c.p.p.[106]; l'hanno poi estesa sia all'inedita udienza predibattimentale (art. 554 *ter*, comma 1, c.p.p.)[107] che all'archiviazione (art. 408, comma 1, c.p.p.)[108], abrogando così l'art. 125 disp. att. c.p.p.

La costruzione del filtro giurisdizionale di nuovo conio è proiettata sui possibili esiti del giudizio di responsabilità dell'indagato/imputato; mira, dunque, a favorire un risultato anticipato, con conseguente riduzione del numero di dibattimenti considerati "inutili", precludendone dunque l'accesso. Da qui, l'opportunità di parlare di criterio "preclusivo" più che "propulsivo"[109]: non consente di transitare al successivo *step*, arrestando la progressione processuale alla fase delle indagini o a quella dell'udienza preliminare.

Tale formula porta con sé un criterio di valutazione necessariamente probabilistico, che potrebbe idealmente collocarsi in una posizione intermedia tra lo *standard* di derivazione nordamericana dell'"oltre ogni ragionevole dubbio"[110] e quello di origine processualcivilistica del "più probabile che non"[111].

---

tempistiche procedimentali di tipo "automatizzato", appositamente costruiti per ottenere determinati risultati».

[105] DELLA TORRE, *La ragionevole previsione di condanna*, in *La legislazione penale*, 19 luglio 2024, p. 4.

[106] CANESCHI, *Le modifiche relative all'udienza preliminare*, in AA.VV., *Riforma Cartabia. Le modifiche al sistema penale*, *Commentario diretto da Gian Luigi Gatta e Mitja Gialuz*, *Nuove dinamiche del procedimento penale*, Bene - Bontempelli - Luparia Donati (a cura di), II, Torino, 2024, pp. 135 ss.; GIALUZ, *Per un processo penale più efficiente e giusto. Guida alla lettura della riforma Cartabia. Profili processuali*, in *Sistema penale*, 28 ottobre 2022, pp. 51 ss.

[107] Sul tema si veda DELLA MONICA, *Il filtro della ragionevole previsione di condanna*, cit., 23; RENZETTI, *L'udienza preliminare ridisegnata e la nuova udienza di comparizione predibattimentale*, in AA. VV., *Commenti alla legge n. 134 del 2021. Riassetti della penalità, razionalizzazione del procedimento di primo grado, giustizia riparativa*, Catalano - Kostoris - Orlandi (a cura di), II, Torino, 2023, pp. 113 ss.

[108] In argomento, GIALUZ, *Per un processo penale più efficiente e giusto*, cit., pp. 44 ss.; LEO, *La regola di giudizio dell'archiviazione e la riapertura delle indagini*, in AA.VV., *Riforma Cartabia*. *Le modifiche al sistema penale. Commentario diretto da Gian Luigi Gatta e Mitja Gialuz*, *Nuove dinamiche del procedimento penale*, cit., pp. 81 ss.; VICOLI, *Nuovi equilibri delle indagini preliminari*, in AA.VV., *Commenti alla legge n. 134 del 2021*, cit., pp. 100 ss.

[109] Contrariamente alla tesi qui sostenuta, parla della ragionevole previsione di condanna come criterio propulsivo, DELLA TORRE, *La ragionevole previsione di condanna*, cit., pp. 2 ss.

[110] Su cui *infra*.

[111] Di diversa opinione, INTRIERI - VIOLA, *Ragionevole previsione di condanna e giustizia predittiva: una modesta proposta per la riforma dell'art. 425 c.p.p.*, in www.giustiziainsieme.it, 1 febbraio 2022, secondo i quali sarebbe ontologicamente legata «al criterio del "più probabile che non" come parametro di giudizio preliminare a fronte dell'"oltre ogni ragionevole dubbio" del giudizio propriamente definitivo del merito»; in tal senso pure FANUELE, *I nuovi criteri per la decisione di non luogo a procedere*, in *Processo penale e giustizia*, 2023, pp. 963 ss.

Tuttavia, tra gli operatori del diritto si è diffusa la sensazione che la riforma Cartabia non sia riuscita ad attuare i suoi propositi in modo sufficientemente netto[112], tralasciando le conseguenze che gli innesti normativi legati alla nuova regola di giudizio avrebbero prodotto nella prassi operativa, anche alla luce delle evidenti resistenze della magistratura nel recepire il cambio di passo realizzato dal legislatore[113].

Infatti, la neo-introdotta formula sembra lasciare uno spazio eccessivo alla componente valutativa in ordine al futuro esito del dibattimento, con conseguente dilatazione dei margini di discrezionalità del giudicante a cui è richiesta la formulazione di una «ragionevole previsione di *probabile* condanna»[114] anche a fronte di una prova della colpevolezza soltanto "in ipotesi".

Per tale ragione ci si deve interrogare sui possibili correttivi funzionali a ripristinare quel *quantum* di efficienza ed efficacia solo abbozzato dalla novella legislativa, pur senza arretrare sul piano della ragionevole durata del processo e su quello delle garanzie difensive.

E se la risposta fosse l'impiego di sistemi algoritmici?

L'idea sarebbe quella di coniugare la realtà giudiziaria con le innovazioni tecnologiche e, in particolare, con sistemi di *AI*, ipotizzandone un possibile coinvolgimento per risolvere le criticità della regola di giudizio *de qua*.

Altro canone decisorio coinvolto in questa "impresa avanguardista" è quello dell'oltre ogni ragionevole dubbio.

---

[112] Sull'acceso dibattito dottrinale si veda, tra i tanti, CIVITA, *Udienza preliminare: la nuova regola di giudizio per la sentenza di non luogo a procedere*, in AA.VV., *La Riforma Cartabia*, Spangher (a cura di), Pisa, 2022, pp. 317 ss.; FERRUA, *Regole di giudizio e udienza preliminare*, in *Processo penale e giustizia*, 2023, 4, p. 966; LA REGINA, *L'archiviazione nel vortice efficientista*, in AA.VV., *La Riforma Cartabia*, cit., pp. 276 ss.; MARZADURI, *Il declino del paradigma accusatorio ed il ritorno all'istruzione sommaria*, in *La legislazione penale*, 3 agosto 2023, p. 1; MENNA, *L'inquadramento della regola di giudizio del non luogo a procedere tra passato e presente dell'udienza preliminare*, *Archivio penale web*, 1 febbraio 2023, p. 4.; TONDIN, *La nuova regola di giudizio della ragionevole previsione di condanna*, in *Cassazione penale*, 2023, pp. 404 ss.

[113] Il riferimento è, ad esempio, alla prima pronuncia di merito del Trib. Patti, G.u.p., 27 gennaio 2023, n. 10, in *Giurisprudenza penale web*, p. 2, che evidenzia come «quella introdotta dalla riforma Cartabia non è una formula nuova e neppure originale perché una locuzione assai simile era già stata fatta propria e utilizzata dalle Sezioni Unite, nel lontano 1955» che parla di «concreta prevedibilità di condanna» (cfr. Cass., Sez. Un., 25 ottobre 1995, n. 38, in *Cassazione penale*, 1996, pp. 776 ss.).

[114] L'espressione è di FERRUA, *Tre temi corderiani: modelli di giustizia procedurale, prove critico-indiziarie, regole di giudizio*, in AA. VV., *Corderiana. Sulle orme di un maestro del rito penale*, Catalano - Ferrua (a cura di), Torino, 2023, p. 83.

Detto *standard* trae la sua origine nell'esperienza processuale di *common law*[115]; pensato come regola probatoria[116] e di giudizio[117] sulla cui base la giuria emana un verdetto immotivato di *not guilty*[118], viene poi introdotto nel nostro sistema giuridico con una nuova veste: da baluardo a tutela della presunzione di innocenza a regola per l'affermazione della colpevolezza dell'imputato.

Tanto è sintomatico dell'inesatta – e, probabilmente, distratta − opera di importazione di siffatto canone processuale nel sistema giuridico di *civil law* italiano ad opera della l. 20 febbraio 2006, n. 46 (c.d. legge Pecorella) che, nell'interpolare l'art. 533, comma 1, c.p.p., ne ha mutato significativamente i tratti caratteristici[119].

---

[115] La paternità del principio tende ad attribuirsi agli Stati Unite, atteso che è in un processo celebrato in Massachusettes nel 1770 che si è parlato per la prima volta di "ragionevole dubbio". Tuttavia, non mancano voci discordanti come quella di FANCHIOTTI, voce *Processo penale statunitense*, in *Enciclopedia del diritto*, *Annali*, II, I, Milano, 2008, p. 827, *sub* nota 121, secondo cui la formula è comparsa per la prima volta nel *common law*, quasi contemporaneamente, alla fine del XVIII secolo in alcuni processi svolti in Irlanda (1796) e nel Regno Unito (Trial of lyon, 1798). Per una ricostruzione approfondita alla genesi del canone, si veda, WHITMAN, *The Origins of Reasonable Doubt. Theological Roots of the Criminal Trial*, New Haven, 2008.

[116] Per un'analisi degli aspetti legali agli *standard* di prova vigenti in ogni fase del procedimento penale, si veda, UBERTIS, *Verso una teoria degli* standard *di prova*, in *Cassazione penale*, 2021, pp. 2214 ss.

[117] Intendono la regola quale probatoria e decisoria, CANZIO - TARUFFO - UBERTIS, *Opinioni a confronto. Fatto, prova e verità (alla luce del principio dell'oltre ogni ragionevole dubbio),* in *Criminalia,* 2009, p. 305; CANZIO, *L'oltre ogni ragionevole dubbio come regola probatoria e di giudizio nel processo penale*, in *Rivista Italiana di Diritto e Procedura Penale*, 2004, pp. 303 ss.; COLAMUSSI, *"Oltre il ragionevole dubbio": il principio e la Costituzione,* in AA.VV., *Giudizio penale e ragionevole dubbio,* Incampo - Scalfati (a cura di), Bari, 2017, p. 182; CONTI, *Il* BARD *paradigma di metodo: legalizzare il convincimento senza riduzionismi aritmetici*, in *Diritto penale e processo*, 2020, pp. 829 ss.; DELL'ANNO, *Obbligo di motivazione e ragionevole dubbio,* in *Processo penale e giustizia,* 2017, p. 524; ILLUMINATI, *La presunzione d'innocenza dell'imputato,* Bologna, 1979, p. 93; STELLA, *Giustizia e modernità: la protezione dell'innocente e la tutela delle vittime,* Milano, 2001, p. 134 ss.

A conferma di questa tesi, cfr. altresì, Cass., Sez. Un., 12 luglio 2005, n. 33748, in *Cassazione penale,* 2005, p. 3752 ss.; Cass., Sez. Un., 11 settembre 2002, n. 30328, in *Rivista Italiana di Diritto e Procedura Penale,* 2002, p. 1133 ss.

Per la tesi opposta, secondo la quale può essere inteso solo come regola di giudizio si veda Ubertis in CANZIO - TARUFFO - UBERTIS, *Opinioni a confronto. Fatto, prova e verità (alla luce del principio dell'oltre ogni ragionevole dubbio),* cit., p. 328; VIGONI, *Giudizi prognostici e ragionevole dubbio,* in AA.VV., *Giudizio penale e ragionevole dubbio*, cit., p. 379.

Tale tesi è sostenuta pure da una copiosa giurisprudenza, per cui si veda per tutti, Cass., sez. V, 28 gennaio 2013, n. 10411, in *CED*, n. 254579.

[118] Sebbene la letteratura d'oltralpe sul tema sia davvero molto ampia, si veda, tra i tanti, DERSHOWITZ, *Dubbi ragionevoli. Il sistema della giustizia penale nel caso O.J. Simpson*, Milano, 2007; SHAPIRO,*"Beyond Reasonable Doubt" and "Probable Cause". Historical Prospectives on the Anglo-American Law of Evidence*, Oakland, 1991.

[119] Sulla fisionomia dello *standard* nel sistema processuale italiano, *ex multis*, CANZIO, *La motivazione della sentenza e la prova scientifica: "reasoning by probabilities"*, in AA.VV., *Prova scientifica e processo penale*, cit., pp. 13 ss.; CATALANO, *Ragionevole dubbio e logica della decisione. Alle radici del giusnaturalismo processuale*, Milano, 2016.

Ciò posto, si proverà a verificare la compatibilità tra il momento di accertamento della responsabilità penale dell'imputato e i sistemi di *AI*.

Lo "studio di fattibilità algoritmica" che si vuole condurre, stante la difficile traducibilità di tali parametri[120], propone di mettere a confronto i due *standard* di giudizio, evidenziandone luci e ombre al cospetto della macchina computazionale.

Per ragioni sistematiche, si partirà dall'analisi del criterio "preclusivo" introdotto dalla riforma Cartabia che opera, in maniera quasi speculare, sia nel momento conclusivo delle indagini preliminari che in quello terminativo dell'udienza preliminare, dando vita a decisioni di tipo processuale; poi, si passerà a scandagliare la tenuta del ragionevole dubbio e, dunque, del provvedimento giurisdizionale di merito rispetto al coinvolgimento dei sistemi di *AI*.

3. La "ragionevole previsione di condanna": dall'archiviazione …

Sebbene già il dato testuale − ragionevole previsione di condanna − suggerisca una certa sintonia tra la regola *de qua* e il *modus operandi* proprio di sistemi predittivi, è necessario spingersi oltre, anche al fine di evitare equivoci.

Compito del giurista, infatti, è quello di andare a fondo, sino a giungere alla struttura di base degli ingranaggi di funzionamento dei momenti decisori, provando a prospettarne un «mutamento di paradigma»[121].

Il punto di partenza è costituito dai termini del binomio "ragionevole-previsione": il primo, pur affetto da una notevole dose di indeterminatezza[122], richiede quella componente di razionalità umana capace di condurre ad una decisione logica e, pertanto, spiegabile; il secondo, invece, per definizione, si basa sull'analisi

[120] Sul tema, si veda *supra*, § 1.

[121] Così, CANZIO, *Il dubbio e la legge*, in *Diritto penale contemporaneo online*, 20 luglio 2018, p. 4, secondo cui «si è forse agli inizi di uno sconvolgente (e però non auspicabile) mutamento di paradigma della struttura e della funzione della giurisdizione»; l'espressione è riproposta in CANZIO, *Prefazione*, in AA.VV., Baccari - Felicioni (a cura di), *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, 2023, Milano, p. XIII, allorquando afferma che «non può seriamente dubitarsi che la forza espansiva di un tale sistema comporti il rischio di un mutamento di paradigma del dire e del fare diritto nel XXI secolo, incidendo pesantemente anche sull'etica del giudizio penale».

[122] DELLA TORRE, *La ragionevole previsione di condanna*, cit., p. 26.

essenzialmente matematica di serie storiche ed è ispirata a canoni statistici, sul presupposto che ciò che è accaduto in passato potrebbe accadere in futuro[123].

È proprio con riferimento a tale ultimo fattore che potrebbe trovare uno spazio applicativo l'*AI* c.d. "debole"[124] che, sulla falsariga dei sistemi di *e-discovery*[125], sarebbe in grado di offrire in tempi rapidissimi un'analisi degli atti che compongono la piattaforma conoscitiva del magistrato, evidenziandone i passaggi che farebbero propendere o meno per una prognosi di futura condanna, offrendo così anche una sorta di "motivazione algoritmica".

Da qui il sistema, calibrato per seguire un ragionamento di tipo induttivo[126], esaminerebbe gli atti contenuti nel fascicolo e i precedenti giurisprudenziali generando un *output* capace di rivelare se, in presenza di un tale compendio probatorio, si possa successivamente giungere (in dibattimento) ad affermare la responsabilità penale dell'imputato.

Giova ricordare che i dati probatori in base ai quali il sistema articolerebbe la propria decisione sono stati raccolti prevalentemente nella fase delle indagini preliminari e, solo in taluni casi, arricchiti da eventuali investigazioni difensive, per cui non consentirebbero il raggiungimento della piena prova della colpevolezza dell'imputato.

In questa prospettiva, pare fondamentale la scelta del *dataset* da immettere nella macchina intelligente. Dovrebbe, dunque, essere garantito *ex ante* il contraddittorio tra le parti circa gli *input* da inserire nel sistema[127], consentendo ai soggetti coinvolti di partecipare al procedimento di selezioni dei dati e delle informazioni di partenza, al fine di generare un *output* privo di *bias*.

Tuttavia, questo non può fisiologicamente accadere nel momento investigativo.

Per tale ragione, nonché alla luce dei chiaroscuri legati al neo-introdotto *standard* di giudizio, sarei portata a escludere la possibilità di impiegare sistemi artificiali

---

[123] Più in generale sul concetto di prevedibilità delle decisioni, PALAZZO, *Considerazioni minime sulla prevedibilità della decisione giudiziale*, cit., p. 941 ss.

[124] Sulla distinzione tra sistemi intelligenti "forti" e "deboli", cfr. *supra*, Cap. I, § 2.

[125] Di tale tecnologia si è già trattato *supra*, Cap. II, § 1.

[126] *Contra*, INTRIERI - VIOLA, *Ragionevole previsione di condanna e giustizia predittiva*, cit., ritengono, invece, che «per correttamente utilizzare l'art. 425 comma 3 c.p.p., come novellato − sarà necessario utilizzare modelli di giustizia predittiva, cercando una sintesi tra quello deduttivo e quello induttivo».

[127] *Supra*, Cap. III, § 7.

nella fase delle indagini per coadiuvare la pubblica accusa nell'assumere determinazioni in ordine all'esercizio dell'azione penale, atteso che tale momento assume movenze talvolta "inquisitorie" per via del segreto investigativo; ed ancora, in virtù della sua funzione, è certamente privo di contrapposizione dialettica, garantita solo nello stadio conclusivo.

Infatti, nelle indagini preliminari, ancor più che in ogni altra scansione processuale, l'accertamento del fatto è soltanto abbozzato e il pubblico ministero valuta unilateralmente il teorema accusatorio di cui è egli stesso autore, in totale assenza di contraddittorio, neppure di quello certamente monco e imperfetto tipico dell'udienza preliminare, con inevitabile compressione del diritto di difesa.

Pure il ruolo della persona offesa verrebbe irreparabilmente compresso, stante il gravoso onere probatorio che incomberebbe sulla stessa, in caso di opposizione alla richiesta dell'accusa adottata con strumenti di *AI*, atteso che tali modalità renderebbero, di fatto, indiscutibile la decisione[128].

Pertanto, si ritiene preferibile che alcun meccanismo artificiale possa insinuarsi tra le pieghe del congegno dell'archiviazione, che «discende dall'idea di non iniziarlo neppure (il processo), in ragione della sua 'inutilità'»[129], senza inaccettabili compromissioni dei diritti dei soggetti coinvolti che meritano di essere protetti dalla deriva tecnologica.

4. … alla sentenza di non luogo a procedere.

Al contrario, concreti spiragli applicativi per i sistemi di *AI* s'intravedono nel momento conclusivo dell'udienza preliminare, in cui il giudicante deve valutare se adottare una sentenza di non luogo a procedere o disporre il giudizio.

Il parametro decisorio impiegato, anche qui, è quello della ragionevole previsione di condanna.

Stando al dato normativo, la formula di nuovo conio, soprattutto in questa fase, assume caratteri dinamici: letta *a contrario*, consente di transitare al dibattimento

[128] In questo senso pure MALINO, *Esercizio dell'azione penale e prognosi di condanna mediante* software *predittivi. Verso la creazione di un PM-robo*t, in *La legislazione penale*, 19 giugno 2024, p. 20, che tende ad escludere categoricamente l'impiego di sistemi algoritmici nella fase conclusiva delle indagini preliminare per decidere tra archiviazione e rinvio a giudizio.

[129] KOSTORIS, *Predizione decisoria e* diversion *processuale*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, cit., p. 107.

solo dopo aver preso in «considerazione la plausibile sorte che il materiale raccolto nelle fasi preliminari potrebbe avere […] anche in termini di eccezioni che potranno ivi essere sollevate sul piano della sua utilizzabilità o su quello dell'applicazione dei criteri di valutazione della prova previsti dalla legge […] oppure circa l'affidabilità o la credibilità dei dichiaranti»[130].

A valle di tale articolato *iter* decisionale si pongono le penetranti valutazioni del g.u.p., chiamato ad esprimersi sulla eventuale responsabilità dell'imputato e tenuto a verificare non solo la correttezza del capo di imputazione e la sua corrispondenza alle risultanze dell'attività investigativa ma anche la completezza del materiale probatorio posto a sostegno della tesi accusatoria. Tutti compiti, questi, deferibili in prima battuta all'*AI* e che opererebbe sotto la lente attenta del magistrato giudicante.

Insomma, sembrerebbe che la contraddizione in termini intrinseca alla (im)prevedibilità della futura condanna dell'imputato, a fronte di una prova della colpevolezza ad uno stadio embrionale, potrebbe essere in qualche modo sanata proprio dall'apporto di strumenti predittivi.

Consapevoli, dunque, che "ragionevolezza" e "prevedibilità" (di condanna) coesisterebbero con qualche difficoltà se il momento decisorio dovesse restare ad esclusivo appannaggio del giudicante umano, la proposta di coinvolgere l'*AI* potrebbe rivelarsi risolutiva.

In particolare, si tratterebbe di un algoritmo che, oltre a verificare la correttezza e la completezza del capo d'imputazione, sarebbe capace di filtrare le informazioni contenute negli atti di cui al fascicolo della pubblica accusa, eventualmente integrati con attività svolta in sede di udienza preliminare, evidenziandone i passaggi che farebbero propendere per una concreta previsione di condanna (o meno). Dall'analisi computazionale potrebbero, altresì, emergere eventuali lacune probatorie, sollecitando il giudice ad attivare i poteri istruttori *ex officio* ai sensi degli artt. 421 *bis* e 422 c.p.p.

Tale scelta sarebbe basata su una valutazione algoritmica compiuta *rebus sic stantibus* ovvero orientata unicamente dalle risultanze probatorie sino a quel

[130] DELLA TORRE, *La ragionevole previsione di condanna*, cit., p. 34.

momento raccolte, senza poter ipotizzare eventuali future evoluzioni dibattimentali del materiale disponibile.

Affinché l'*output* sia corretto, però, è necessario che il sistema sia allenato con dati precisi[131].

Si rende, dunque, opportuno l'impiego di un *dataset* ricco di precedenti giurisprudenziali[132], sia di merito che di legittimità, che potrebbero indicare in quanti casi, in passato, un determinato compendio probatorio sia stato ritenuto idoneo a soddisfare tale *standard* "preclusivo"[133].

Quindi a quali pronunce fare, in concreto, riferimento[134]? Alle sentenze di non luogo a procedere per carenza di ragionevole previsione di condanna oppure a quelle dibattimentali di condanna oltre ogni ragionevole dubbio?

Quello a cui sarebbe chiamata la macchina – e a cui, per il momento, è chiamato il solo giudice − è un giudizio prognostico, basato su ciò che potrebbe accadere in futuro. Pertanto, si ritiene opportuno che i precedenti di merito a cui fare riferimento siano, inevitabilmente, quelli dibattimentali; infatti, nonostante l'incerta traducibilità algoritmica del criterio di giudizio di cui all'art. 533, comma 1, c.p.p., immettere nel sistema un *set* di pregresse sentenze di condanna (o di assoluzione), offrirebbe alla macchina un parametro effettivo per meglio calibrare le proprie scelte. Conveniente sarebbe altresì arricchire le "conoscenze" dell'applicativo

---

[131] DE FELICE, *Intelligenza artificiale e processi decisionali automatizzati: GDPR ed* ethics by design *come avamposto per la tutela dei diritti umani*, in AA.VV., *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, D'Aloia (a cura di), Milano, 2020, p. 416, sostiene che «dall'esattezza dei dati utilizzati e dalla logica del trattamento alla base della configurazione degli algoritmi dipende l'"intelligenza" delle loro scelte».

[132] Sul ruolo del precedente quale strumento di prevedibilità del diritto, DE FELICE, *Su probabilità, «precedente» e calcolabilità giuridica,* in *Rivista di diritto processuale*, 2017, pp. 1546 ss.

[133] Secondo DELLA TORRE, *La ragionevole previsione di condanna*, cit., p. 40 ss., pur ritenendo che «i *tools* potrebbero essere […] idealmente sfruttati, non solo per rendere più spedita l'attività dei pubblici ministeri e dei giudici, ma anche più informata», poiché «grazie alla loro grande potenza di calcolo, i *software* potrebbero fornire una base esperienziale molto più ampia rispetto a quella di una persona fisica, indicando in quale percentuale di fattispecie, data la presenza di determinati elementi istruttori, la condanna del prevenuto sia stata ritenuta, in precedenza, idonea a raggiungere il criterio decisorio di cui agli artt. 408, 425 e 554-*ter* c.p.p.»; tuttavia, considera non particolarmente agevole l'ingresso di sistemi di *AI* sia nel fondamentale snodo tra "azione" e "inazione" che in quello tra "giudizio" e "non luogo a procedere".

[134] Sull'utilizzabilità delle sentenze giudiziarie, alla luce della frizione con il diritto alla *privacy* e alla riservatezza dei dati personali, PALMIRANI - PODDA, *Anonimizzazione e pseudonimizzazione di sentenze giudiziarie*, in AA.VV., *La trasformazione digitale della giustizia nel dialogo tra discipline*, Palmirani - Sapienza (a cura di), Milano, 2022, p. 38, secondo le quali «le sentenze giudiziarie sono, di fatto, foriere di dettagli sulla vita delle persone, nonché sul loro contesto di appartenenza».

artificiale con gli orientamenti della giurisprudenza di legittimità, che tenta di limare eventuali sbavature interpretative legate al neo-introdotto *standard* di giudizio.

Insomma, l'uso di un *software* programmato secondo *input* ben determinati, selezionati nel contraddittorio (anticipato) tra le parti[135], sarebbe probabilmente in grado di assicurare stabilità operativa alla nuova regola di giudizio, consentendo così al giudicante di compiere un'adeguata sintesi tra ragionevolezza e prevedibilità della decisione, in linea con le richieste del legislatore.

Neppure può dirsi che la valutazione del g.u.p., supportata dall'*AI*, possa in qualche modo contaminare la genuinità della decisione del giudice dibattimentale. Tale prospettazione, infatti, potrebbe verificarsi anche se non fosse contemplato l'utilizzo di sistemi artificiali, in considerazione del complesso sforzo richiesto al magistrato che, comunque, dovrebbe pronosticare i possibili esiti del giudizio di responsabilità; ed ancora, vigerebbe in dibattimento, in ogni caso, quello sbarramento costituito dalla inutilizzabilità fisiologica degli atti compiuti nelle precedenti fasi.

Ad ogni buon conto, una strada percorribile per superare tale obiezione potrebbe essere quella di inibire al decisore finale l'accesso all'eventuale responso algoritmico, soprattutto nel caso in cui il sistema avesse valutato il materiale probatorio disponibile come adeguato a prevedere la futura condanna dell'imputato, oltre ogni ragionevole dubbio, ai sensi dell'art. 533 c.p.p.

Inoltre, presta il fianco a soluzioni algoritmiche pure la neonata udienza predibattimentale, che funziona sul modello dell'udienza preliminare, ed è pensata per garantire un vaglio a maglie strette anche per quei reati rispetto ai quali l'esercizio dell'azione penale avviene mediante il decreto di citazione diretta a giudizio.

L'accertamento giudiziario tipico di questo modulo procedimentale diversificato richiede, al pari di quello ordinario, la prosecuzione del giudizio soltanto in presenza dei presupposti per formulare una ragionevole previsione di condanna, senza però consentire al giudice, in caso contrario, di colmare eventuali vuoti probatori.

---

[135] Cfr. *supra*, Cap. III, § 7.

Pertanto, anche in questa sede, potrebbero ravvisarsi concreti spazi operativi riservabili a sistemi algoritmici.

5. L'accertamento della responsabilità oltre ogni ragionevole dubbio.

Il tema più controverso[136] resta, invece, quello che prevede il riconoscimento alla macchina di un qualche ruolo determinante nella fase della decisione[137] dibattimentale.

La questione è molto discussa in quanto, «l'accertamento dei fatti raggiunto nel ragionamento giudiziario, grazie al metodo induttivo, all'apporto del sapere scientifico, oltre che del "buon senso", pare […] l'unico metodo per verificare o smentire l'ipotesi relativa alla responsabilità penale»[138].

Tuttavia, è innegabile che «ai fini dell'accertamento del fatto, la prova scientifica, digitale o informatica, e l'impiego di un modello matematico-statistico nell'esercizio di quella che viene definita giustizia "algoritmica" o "predittiva" sono destinati a svolgere un ruolo di straordinario rilievo nel ragionamento giudiziale»[139].

È il caso, però, di ricordare che «l'intelligenza artificiale non emette sentenze. Non condanna. Può sembrare che lo faccia, ma non lo fa, e non può farlo, e quindi non dovrebbe farlo»[140].

L'attività processuale di ricostruzione della verità è orientata a comprendere cosa sia accaduto in passato, tentando così di mettere insieme i tasselli di un mosaico ancora da comporre; l'obiettivo è quello di arrivare alla decisione dibattimentale con una immagine nitida di ciò che sarebbe accaduto.

---

[136] NIEVA-FENOLL, *Intelligenza artificiale e processo*, Torino, 2019, trad. it. a cura di Comoglio, p. 89, lo considera come l'argomento che incute più paura sia ai giuristi che ai cittadini: il vero timore consisterebbe nell'affidare il destino dell'imputato ad una macchina che decide solo in funzione di variabili statistiche, senza alcuna componente "umana".

[137] RUFFOLO, *La* machina sapiens *come "avvocato generale" ed il primato del giudice umano*, cit., pp. 206, per spiegare l'attività decisoria rievoca il concetto *weberiano* di *factis species* ovvero la dottrina della fattispecie, secondo cui il giudizio consiste nella «riconduzione di un fatto specifico a un caso particolare dello schema astratto (fattispecie) preveduto dalla norma».

[138] In tal senso, CAIANIELLO, *Potenzialità e rischi derivanti dall'interazione tra I.A. e giustizia penale preventiva*, in AA.VV., *XXVI lezioni di diritto dell'intelligenza artificiale*, cit., p. 269.

[139] In tal senso, CANZIO, *Prefazione*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, cit., p. XIII.

[140] Così, NIEVA-FENOLL, *Intelligenza artificiale e processo*, cit., p. 5.

Si tratta, infatti, di *lost facts* che vanno ricostruiti nel presente «poiché, quando le cause non sono riproducibili nell'esperienza attuale, non rimane che inferirle dagli effetti, (per cui) l'itinerario del processo è caratterizzato dalla retrospezione»[141].

Com'è stato autorevolmente sostenuto «il processo assolve una funzione cognitiva e di accertamento della verità in ordine al fatto prospettato nell'imputazione elevata dall'organo dell'accusa». Tuttavia, ciò avviene «nell'ormai acquista consapevolezza della valenza solo probabilistica del giudizio di conferma dell'enunciato di partenza, in termini di verosimiglianza, plausibilità, corrispondenza rispetto al fatto realmente accaduto in passato»[142].

In buona sostanza, pur ammettendo che «il codice di rito penale accusatorio è imperniato su inferenze logiche strutturalmente probabilistiche»[143], si ritiene più corretto – almeno per il momento − che tale attività decisoria deputata all'accertamento del fatto spetti solo ed unicamente al giudicante umano, escludendo, dunque, il possibile apporto di strumenti di *AI*.

D'altronde, sino ad ora, si è tentato di ricavare spazi applicativi per detti sistemi sempre in chiave prognostica; è questo quello che fanno i modelli computazionali e che, al contrario, l'uomo non è in grado di fare: elaborare velocemente una enorme mole di dati per restituire previsioni, ancorate a basi statistiche, circa futuri possibili accadimenti.

All'opposto, invece, si colloca l'accertamento della responsabilità penale in dibattimento; dominato da dati riferibili al passato, utili per comprendere se l'imputazione sia fondata o meno e, dunque, se il fatto storico di reato sia stato commesso dall'imputato con quelle precise modalità, non richiede momenti "predittivi".

Pertanto, è indispensabile che tale accertamento sia guidato dall'uomo che, analizzate le prove assunte in contraddittorio tra le parti e forgiate dal "fuoco

---

[141] CANZIO, *La motivazione della sentenza e la prova scientifica: "reasoning by probabilities"*, in AA.VV., *Prova scientifica e processo penale*, cit., p. 4.

[142] CANZIO, *Prefazione*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, cit., p. IX, che prosegue affermando che si tratta di «*trial by probabilities*», benché citando SHAFER, *A Matematichal Theory of Evidence*, Princerton, 1979, avverte che «*probability is not about number, is about reasoning*».

[143] FELICIONI, *L'attività valutativa del giudice tra ragione ed emozione*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, cit., p. 6.

incrociato" della *cross examination*, deve valutare se queste siano sufficienti a fugare ogni ragionevole dubbio in ordine alla colpevolezza del *reo*[144].

Ancora, la stessa struttura normativa dello *standard* di giudizio chiude le porte ai sistemi artificiali: nessuna compatibilità sembrerebbe scorgersi tra l'oltre ogni ragionevole dubbio e i caratteri tipici, tendenzialmente prognostici, propri degli applicativi artificiali[145].

Pertanto, si ritiene che la giustizia predittiva, a cui potrebbe essere riservato un ruolo in altri intervalli della decisione penale, non possa soccorrere il giudice nell'accertamento della *questio facti*.

6. L'imprescindibile centralità del giudice.

Così delineati i profili del possibile rapporto tra algoritmi e decisione ed escluso *a priori* − almeno per il momento – il coinvolgimento dell'*AI* nel giudizio sul fatto, pare opportuna qualche riflessione conclusiva, seppur non definitiva, evidenziando, sempre con le dovute cautele, i vantaggi legati all'impiego della tecnologia in termini di efficienza, efficacia e celerità dei tempi della giustizia[146].

Coscienti delle problematiche emerse oltreoceano − tra opacità dell'algoritmo[147] e *bias* cognitivi −, pare giunto il momento di soffermarsi sui correttivi necessari per sopperire alle possibili distorsioni applicative legate all'impiego dell'*AI* nel settore penale.

Affinché sia anche solo ipotizzabile uno scenario come quello sino ad ora prospettato è necessario regolamentare due aspetti fondamentali: il controllo umano e la vincolatività della risposta algoritmica.

---

[144] BLAIOTTA, *Giustizia, errore, intelligenza artificiale*, in *Sistema penale online*, 23 ottobre 2023, p. 1, secondo cui «il codice di procedura penale esprime una chiara epistemologia giudiziaria: la colpevolezza oltre ogni ragionevole dubbio, l'esplicazione delle ragioni della decisione e del mancato accoglimento della tesi contraria, il contraddittorio, il confronto tra l'ipotesi ed i fatti e tra ipotesi in conflitto, l'affidabilità e la coerenza degli indizi» che, in quanto tale, non può essere per nessuna ragione rovesciata.

[145] Al contrario, analizza gli eventuali profili prognostici del criterio dell'oltre ogni ragionevole dubbio, VIGONI, *Giudizi prognostici e ragionevole dubbio*, cit., pp. 373 ss.

[146] LUPARIA DONATI, *Artificial Intelligence in Criminal Courts. Opportunity or Threat?*, in AA.VV., *Legal Challenges in the New Digital Age*, Lopez Rodriguez - Green - Kubica (*edited by*), Leiden, 2021, pp. 160 ss.

[147] Sull'opacità dell'*AI*, UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, cit., pp. 12 ss.

Infatti, consapevoli della ineluttabile catarsi digitale che ha travolto (e che travolgerà ancora) la giustizia penale, è necessario tracciare precisi punti fermi, indispensabili ad evitare il crollo delle fondamenta del "giusto processo"; del resto, «la distopia delle macchine al potere è non solo un'ipotesi da fantascienza ma anche una possibilità da tenere in considerazione»[148].

Pertanto, è necessario riflettere sul ruolo del giudice rispetto alle novità che l'*AI* propone nel campo del diritto processuale penale: quale custode degli equilibri processuali, vede la sua centralità riconfermata e protetta anche in un mondo di "giustizia algoritmica". Tali valori, infatti, seguendo le coordinate fin qui tracciate, sarebbero solo apparentemente alterati dall'ingresso di strumenti di *AI* nei tribunali. A livello europeo, infatti, la *human supervision* di cui all'art. 14[149] dell'*AI Act* è considerata strumento indispensabile per ammettere l'impiego di sistemi "ad alto rischio". Tra i requisiti di garanzia richiesti, infatti, vi è quello di assicurare una

[148] Così, DI SALVO, *Noi e i robot. Intervista a Jerry Kaplan*, in *Wired online*, settembre 2017, e riprodotto nella monografia di KAPLAN, *Intelligenza artificiale*, *Guida al futuro prossimo*, Roma, 2108, p. 217.

[149] Data la centralità del tema, pare opportuno riportare le parti dell'art. 14, Reg. UE 2024/1689, che si ritengono fondamentali ai fini della presente analisi: «1. I sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso. 2. La sorveglianza umana mira a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere quando un sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, in particolare qualora tali rischi persistano nonostante l'applicazione di altri requisiti di cui alla presente sezione. 3. Le misure di sorveglianza sono commisurate ai rischi, al livello di autonomia e al contesto di utilizzo del sistema di IA ad alto rischio e sono garantite mediante almeno uno dei tipi di misure seguenti: a) misure individuate e integrate nel sistema di IA ad alto rischio dal fornitore prima della sua immissione sul mercato o messa in servizio, ove tecnicamente possibile; b) misure individuate dal fornitore prima dell'immissione sul mercato o della messa in servizio del sistema di IA ad alto rischio, adatte ad essere attuate dal *deployer*. 4. Ai fini dell'attuazione dei paragrafi 1, 2 e 3, il sistema di IA ad alto rischio è fornito al *deployer* in modo tale che le persone fisiche alle quali è affidata la sorveglianza umana abbiano la possibilità, ove opportuno e proporzionato, di: a) comprendere correttamente le capacità e i limiti pertinenti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, anche al fine di individuare e affrontare anomalie, disfunzioni e prestazioni inattese; b) restare consapevole della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'output prodotto da un sistema di IA ad alto rischio ("distorsione dell'automazione"), in particolare in relazione ai sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche; c) interpretare correttamente l'output del sistema di IA ad alto rischio, tenendo conto ad esempio degli strumenti e dei metodi di interpretazione disponibili; d) decidere, in qualsiasi situazione particolare, di non usare il sistema di IA ad alto rischio o altrimenti di ignorare, annullare o ribaltare l'output del sistema di IA ad alto rischio; e) intervenire sul funzionamento del sistema di IA ad alto rischio o interrompere il sistema mediante un pulsante di "arresto" o una procedura analoga che consenta al sistema di arrestarsi in condizioni di sicurezza […]».

dimensione antropocentrica della tecnologia[150], attribuendo all'uomo il ruolo di "guardiano della macchina".

In primis, dunque, dev'essere assicurata una modalità d'uso di tali *software* che non affievolisca la funzione giudiziaria: il processo penale non può (e non deve) fare a meno di essere «un giudizio dell'uomo sull'uomo»[151].

In altre parole, dev'essere salvaguardato quel «controllo umano significativo»[152] necessario nel momento decisorio, consentendo al giudicante di interpretare il dato (non vincolante) generato dalla macchina su cui poggerà, seppur non in via esclusiva, la sua decisione.

Tale *modus operandi* presuppone l'impiego di algoritmi neutrali e intelligibili, il cui potenziale tasso d'errore dev'essere reso noto e che operino con modalità di funzionamento pubbliche ed accessibili agli operatori del diritto, garantendo il contraddittorio tra le parti circa gli *input* da immettere nel sistema al fine di generare un *output* privo di *bias*.

Dev'essere, insomma, consentito sia all'utilizzatore che al destinatario della decisione di comprendere quale sia l'*iter* seguito per giungere ad una determinata conclusione[153]: il primo, se in possesso di strumenti utili per contestarla, è legittimato a discostarsi dalla scelta operata della macchina, preservando il proprio libero convincimento[154] e assolvendo all'obbligo di motivazione[155]; il secondo, nell'esercizio del diritto di difesa, è abilitato a criticare l'operato del giudice (e dell'algoritmo) in sede d'impugnazione.

---

[150] PAJNO - BASSINI - DE GREGORIO - MACCHIA - PATTI - POLLICINO - QUATTROCOLO - SIMEOLI - SIRENA, *AI: profili giuridici. Intelligenza Artficiale: criticità emergenti e sfide per il giurista,* in *BioLaw Journal - Rivista di BioDiritto*, 2019, 3, p. 206, secondo i quali «si impone, altresì, la necessità di assicurare che il progresso tecnologico si svolga in armonia con le esigenze di tutela individuali e collettive, nel rispetto di una dimensione antropocentrica».

[151] Così, LUPARIA DONATI, *Notazioni controintuitive su intelligenza artificiale e libero convincimento*, cit., p. 115.

[152] L'espressione è di UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, cit., pp. 22 ss.

[153] In argomento, KOSTORIS, *Predizione decisoria e* diversion *processuale*, cit., p. 95.

[154] Sul tema del libero convincimento, ampiamente, NOBILI, *Il principio del libero convincimento del giudice*, 1974, Milano.

[155] Più in generale, sulla motivazione delle sentenze, si veda, IACOVIELLO, voce *Motivazione della sentenza penale (controllo della)*, in *Enciclopedia del Diritto*, Aggiornamento IV, Milano, 2000, p. 750, che la intende non come atto processuale ma come «frammento di un atto processuale».

Anche nel perimetro della c.d. «giustizia 2.0»[156], ove l'algoritmo potrebbe attualizzare e rendere praticabile la regola della ragionevole previsione di condanna e spingersi a valutare su basi probabilistiche anche la pericolosità sociale della persona sottoposta alle indagini, dell'imputato o del condannato, al giudicante resterebbero riconosciuti ampi margini di discrezionalità.

Il compito del giudice sarebbe, dunque, quello di garantire, in ossequio alla *voluntas legis* e a tutela dei principi cardine del processo penale, quella irrinunciabile componente razionale del momento valutativo, impiegando utilmente il responso analitico fornito dalla "macchina intelligente"; dopo aver ottenuto il risultato adattato al caso di specie, avrebbe gli strumenti utili per decidere, non propendendo unicamente per la soluzione che sembrerebbe essere la più convincente ma assestandosi su di una posizione che risponda anche al canone della probabilità[157].

Dunque, la macchina avrebbe un ruolo meramente ausiliario, che non comporterebbe l'esclusione del giudicante dal processo decisionale; l'influenza dell'algoritmo assumerebbe il valore di «previsione ipotetica non vincolante per il giudice, la cui pronuncia non sarebbe pertanto preconfezionata»[158], né esposta al rischio di divenire una "meta-motivazione" o "motivazione di secondo grado".

Si tratterebbe quindi di una vera e propria collaborazione, «una sorta di tecno-umanesimo, una contaminazione tra *humanitas* e *techne*» che rivela la sua utilità sia per «ridurre i tempi di risposta dell'autorità giudiziaria, sia per la maggiore prevedibilità nell'applicazione della legge e uniformità degli orientamenti giurisprudenziali»[159].

---

[156] LORUSSO, Digital evidence*,* cybercrime *e giustizia penale 2.0*, in *Processo penale e giustizia*, 2019, pp. 821 ss.

[157] Sull'inevitabile incertezza che permea il processo penale nel momento dell'accertamento del fatto e, dunque, sulla necessità di far riferimento alla probabilità, TARONI - BOZZA - VUILLE, *La probabilità come strumento per una coerente valutazione della prova scientifica*, in AA.VV., *Prova scientifica e processo penale*, cit., pp. 21 ss.

[158] Così, UBERTIS, *Intelligenza artificiale e giustizia predittiva,* in *Sistema penale online*, 16 ottobre 2023, p. 10.

[159] Così, CATERINI, *Il giudice penale robot*, cit., pp. 21-22.

Pertanto, pur mantenendo ben saldo il carattere umano della *iurisdictio*[160], verrebbe assicurata una «interazione feconda tra uomo e *robot*»[161]; senza mai intaccare la libertà di giudizio dell'organo decidente, il sistema potrebbe restituire un parere non vincolante, «una sorta di "*second opinion* algoritmica"»[162], che il decisore resterebbe libero di disattendere con motivazione rafforzata sul punto[163].

Insomma, da un lato, con l'utilizzo di sistemi di *AI* sarebbe nettamente agevolato il compito del giudice, che resterebbe indiscusso *dominus* del momento decisorio, a cui si affiancherebbe l'operato del sistema predittivo, con le opportune cautele e senza "minaccia" di sostituzione alcuna; dall'altro lato, dev'essere dotato di un antidoto contro lo strapotere dell'esperto artificiale per preservare la sua capacità di discernimento ed evitare di appiattirsi sul responso dell'*AI*[164], abdicando alle sue funzioni.

Giammai ci si dovrebbe ritrovare dinanzi a un «giudice imbambolato dalla seduzione dell'intelligenza artificiale»[165]; *ex adverso*, nonostante l'*appeal* sprigionato della tecnologia, il magistrato dovrebbe essere in grado di dominarla, dosandone la potenza e non piegandosi acriticamente alla sua volontà[166].

Pertanto, qualora dovesse essere in disaccordo con le risultanze algoritmiche potrebbe propendere per una soluzione diversa da quella proposta dall'*AI*.

Sarebbe infondato, dunque, il timore di una validazione acritica del risultato algoritmico, atteso che il giudicante, avvalendosi della cooperazione di esperti del

---

[160] LEGNINI, *Introduzione*, in AA.VV., *Decisione robotica*, cit., p. 14, afferma che «nel continuare a pretendere che questa componente di *humanitas* esista, noi non possiamo tagliare fuori le applicazioni e gli sviluppi del progresso tecnologico e della robotica in particolare».

[161] PUNZI, Judge in the machine. *E se fossero le macchine a restituirci l'umanità del giudicare?*, in AA.VV., *Decisione robotica*, cit., p. 328.

[162] Così, MANES, *Intelligenza artificiale e giustizia penale*, in AA.VV., *XXVI lezioni di diritto dell'intelligenza artificiale*, cit., p. 283; un interessante approfondimento sull'opinione della macchina è stato condotto da KARNOW, *The Opinion of Machine*, in AA.VV., *The Cambridge Handbook of the Law of Algorithms*, Barfield (*edited by*), Cambridge, 2021, pp. 16 ss.

[163] Configura l'ipotesi della macchina come una sorta di Avvocato Generale, le cui "conclusioni" restando parere obbligatorio ma non vincolante, RUFFOLO, *La* machina sapiens *come "avvocato generale" ed il primato del giudice umano*, cit., pp. 209 ss.

[164] CECCHI, *Sfogliando* Justice Machines: *evocazioni antesignane su diritto e intelligenza artificiale*, in *Cassazione Penale*, 2021, p. 4174, attraverso la trama del breve racconto filosofico-giuridico di Jacques Charpentier, intitolato *Justice Machines*, afferma che «la giustizia, affinché possa dirsi umanamente soddisfacente, non può darsi unilateralmente ma deve essere partecipata, senza appiattimenti su meccanismi e risposte automatiche».

[165] Così, LA REGINA, *I.A. e ragionamento giuridico: la giustizia prevedibile*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, cit., p. 179.

[166] Al contrario, DE KERCKHOVE, *La decisione datacratica*, in AA.VV., *Decisione robotica*, cit., p. 104, sostiene che la vera vittima dell'*AI* è l'autonomia dell'uomo.

settore, potrebbe essere in grado di comprendere il funzionamento della macchina e di individuare eventuali errori che ne inficerebbero il responso algoritmico, decretandone così l'utilizzabilità o meno nel contesto processuale.

Affinché ciò sia possibile è, però, necessario assicurare agli operatori del diritto un buon livello di alfabetizzazione in materia di *AI*, in ossequio a quanto disposto dalla regolamentazione comunitaria[167], creando, dunque, una strutturata catena di conoscenza del meccanismo che sta alla base di tali applicativi.

In tal senso, all'*AI* potrebbe essere riconosciuto il merito di «sostituire a questo disordine (processuale) – o, se si preferisce, a quest'ordine complesso e precario – un passaggio lineare, riproponendo l'idea tipicamente illuministico-positivista di un diritto "calcolabile"»[168].

In definitiva, adottando tutti gli accorgimenti suggeriti dal già menzionato *AI Act* − che classifica i modelli predittivi nella categoria dei sistemi ad alto rischio – e idonei a correggere eventuali *bias* o malfunzionamenti, non può negarsi, che il contributo delle macchine intelligenti potrebbe tradursi in una riduzione consistente dei tempi della giustizia, *fil rouge* dei recenti pacchetti di riforma.

Al contrario, inibire totalmente l'accesso ai *software* predittivi nel processo penale significherebbe voler rinunciare ad un certo livello di qualità ed efficienza della giustizia, depurata da personalismi e decisioni emotive, abdicando così ancora una volta all'obiettivo di ridurre la – talora ancora irragionevole − durata dei tempi processuali.

In tal modo, l'ingresso dell'*AI* nelle dinamiche decisorie potrebbe altresì costituire il giusto contrappeso per ridurre l'arbitrio del giudice e l'inevitabile errore giudiziario, insinuandosi negli interstizi del sistema probatorio per fungere da elemento di controllo in grado di irrobustire la decisione del giudice.

L'introduzione di modelli computazionali potrebbe favorire «la conoscenza del giudice del *probabilistic reasoning* in generale e di quello *bayesian* in particolare, facendo guadagnare agli operatori della giustizia *skills* che da anni, a livello internazionale, si vuole che il decisore penale acquisisca»; questo poiché il

[167] Cfr., art. 4 e 13, nonché cons. 20), Reg. UE 2024/1689.

[168] In tal senso, KOSTORIS, *Predizione decisoria e* diversion *processuale*, cit., p. 97; sulla calcolabilità giuridica, si veda, altresì, LEGNINI, *Introduzione*, in AA.VV., *Decisione robotica*, cit., pp. 9 ss.

magistrato «si occupa di una gemma preziosa nel forziere dei valori, la libertà delle persone, (e) deve possedere un bagaglio metodologico, comprensivo dei meccanismi logici probabilistici, uguale, se non superiore, a quello di altri professionisti che si muovono nella complessa società contemporanea»[169].

Non è pensabile, infatti, che la giurisdizione penale sia privata di tali conoscenze tecnologiche che, beninteso, non sottraggono al giudice la sua individualità di apprezzamento ma ne agevolano il buon uso e il successivo esame, in ossequio alla logica del controllo della decisione.

Del resto sarebbe sciocco non ammettere l'utilizzabilità di tali *software* solo perché, proprio come accade quotidianamente al giudicante, mossi da una logica *fuzzy*: nel processo, infatti, è sempre necessario orientarsi tra una serie di condizioni incerte e di dati frammentati da ricostruire e cui dare un senso, che dovrà essere esplicitato nella motivazione del provvedimento da adottare.

Pertanto, alla luce dei *diktat* europei, si auspica un ampio (e coraggioso) intervento del legislatore nazionale, che apra le porte della giustizia ai nuovi sistemi algoritmici.

Sulla falsa riga delle considerazioni sin qui esposte, infatti, si potrebbe avviare la sperimentazione di sistemi di *AI*, da un lato, per la valutazione della pericolosità sociale e, dall'altro, per soddisfare la prevedibilità "processuale" di una ragionevole previsione di condanna, così come richiesto dal legislatore.

L'urgente obiettivo da raggiungere resta, dunque, quello di mettere a punto una normativa dettagliata, che tenga conto sia delle problematiche intrinseche ai sistemi tecnologici che di quelle ontologicamente legate al processo penale e che consenta ai modelli computazionali di intervenire come possibile correttivo all'attuale condizione di inadeguatezza della giurisdizione.

[169] È quanto affermato da LUPARIA DONATI, *Notazioni controintuitive su intelligenza artificiale e libero convincimento*, cit., p. 118.

BIBLIOGRAFIA

ADINOLFI, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, in AA.VV., *Intelligenza artificiale e diritto: una rivoluzione?*, Pajno - Donati - Perrucci (a cura di), Bologna, 2022, 1, pp. 127 ss.;

ALGERI, *Intelligenza artificiale e polizia predittiva*, in *Diritto penale e processo*, 2021, pp. 724 ss.;

ASHWORTH- ZEDER, Preventive Justice, OUP, Oxford, 2014;

ATERNO, Alexa *testimone in tribunale: i vantaggi per gli investigatori e le garanzie per la difesa*, in *Agenda digitale online*, 20 marzo 2020;

AVITABILE, *Il diritto davanti all'algoritmo*, in *Rivista italiana per le scienze Giuridiche*, 2017, 8, pp. 327 ss.;

BACCARI - PECCHIOLI, *I.A. e giudizio sul fatto: gli strumenti di* e-evidence *per la cognizione*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, Baccari - Felicioni (a cura di), Milano, 2023, pp. 109 ss.;

BACCARI - MARRAFFINO, *Le prospettive di utilizzo delle* chatbot *nel procedimento penale*, in *Diritto penale e processo*, 2021, p. 1008 ss.;

BALKIN, *The Three Laws of Robotics in the Age of Big Data*, in *Ohio State Law Journal*, 2017, p. 1219;

BARBARO, *Lo studio di fattibilità di un nuovo quadro normativo sulla concezione, lo sviluppo e l'applicazione dei sistemi di Intelligenza Artificiale sulla base delle norme del Consiglio d'Europa. Il lavoro del Comitato ad hoc sull'intelligenza artificiale del CdE*, in *Questione giustizia online*, 28 aprile 2021;

BARBARO, *Cepej, adottata la prima Carta etica europea sull'uso dell'intelligenza artificiale (AI) nei sistemi giudiziari*, in *Questione giustizia online*, 7 dicembre 2018;

BARBARO, *Uso dell'intelligenza artificiale nei sistemi giudiziari: verso la definizione di principi etici condivisi a livello europeo?*, in *Questione giustizia*, 2018, 4, pp. 189 ss.;

BARFIELD W. - BARFIELD J., *An Introduction to Law and Algorithms*, in AA.VV., *The Cambridge Handbook of the Law of Algorithms*, Barfield (*edited by*), Cambridge, 2021, pp. 3 ss.;

BARFIELD W., *Towards a law of artificial intelligence*, in AA.VV., *Research Handbook on the Law of Artificial Intelligence*, Barfield W. - Pagallo (*edited by*), Cheltenham, 2018, pp. 29 ss.;

BARONE, *Giustizia Predittiva e Certezza del Diritto*, Pisa, 2024;

BARONE, *La regolamentazione dell'Intelligenza Artificiale: è "corsa agli armamenti"*, in *Diritto penale e processo*, 2024, 8, pp. 991 ss.;

BARONE, *Intelligenza artificiale e processo penale: la linea dura del Parlamento europeo. Considerazioni a margine della risoluzione del Parlamento europeo del 6 ottobre 2021*, in *Cassazione Penale*, 2022, pp. 1180 ss.;

BASILE, *Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione*, in AA.VV., *Diritto penale e intelligenza artificiale. Nuovi scenari*, Balbi - De Simone - Esposito - Manacorda (a cura di), Torino, 2022, pp. 1 ss.

BASILE, *Intelligenza artificiale e responsabilità penale: un'intelligenza tanto "umana" da poter essere punita?*, 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, pp. 85 ss.;

BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Diritto Penale e Uomo*, 2019, 10, pp. 1 ss.;

BASILE, *Esiste una nozione ontologicamente unitaria di pericolosità sociale? Spunti di riflessione, con particolare riguardo alle misure di sicurezza e alle misure di prevenzione,* in *Rivista Italiana di Diritto e Procedura Penale*, 2018, pp. 644 ss.;

BATTISTONI, *Reato continuato: l'obbligo di indicazione e motivazione degli aumenti per i reati satellite*, in *Diritto penale e processo*, 2022, pp. 638 ss.;

BIARELLA, *Polizia Predittiva: al via la sperimentazione a Caorle*, in *Altalex online*, 24 maggio 2021;

BLAIOTTA, *Giustizia, errore, intelligenza artificiale*, in *Sistema penale online*, 23 ottobre 2023;

BODEN, *L'intelligenza artificiale*, Bologna, 2019;

BOMPREZZI - SAPIENZA, Algorithmic justice *e classificazione di rischio nella proposta* AI Act, in AA.VV., *La trasformazione digitale della giustizia nel dialogo tra discipline*, Palmirani - Sapienza (a cura di), Milano, 2022, pp. 65 ss.;

BORRUSO, voce *Informatica Giuridica*, in *Enciclopedia del diritto*, Aggiornamento I, Milano, 1997, pp. 640 ss.;

BURCHARD, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *Rivista Italiana di Diritto e Procedura Penale*, 2019, pp. 1909 ss.;

CADOPPI, *Il valore del precedente nel diritto penale*, Torino, 1999;

CAIANIELLO - PUGLIESE, *Manifesto per la giustizia penale digitale: il processo penale telematico*, in AA.VV., *Riforma Cartabia. Le modifiche al sistema penale*, *Commentario diretto da Gian Luigi Gatta e Mitja Gialuz*, *Il procedimento penale*

tra efficienza, digitalizzazione e garanzie partecipative, Caianiello - Gialuz - Quattrocolo (a cura di), I, Torino, 2024, pp. 165 ss.;

CAIANIELLO, *Dangerous Liaisons. Potentialities and Risks Deriving from the Interaction between Artificial Intelligence and Preventive Justice*, in *European journal of crime, criminal law and criminal justice*, 2021, pp. 1 ss.;

CAIANIELLO, *Potenzialità e rischi derivanti dall'interazione tra I.A. e giustizia penale preventiva*, in AA.VV., *XXVI lezioni di diritto dell'intelligenza artificiale*, Ruffolo (a cura di), Torino, 2021, pp. 265 ss.;

CALABRESI, *Scienza e diritto: alcune notazioni preliminari*, in AA.VV., *Scienza e diritto nel prisma del diritto comparato. Atti del convegno tenutosi a Pisa il 22-24 maggio 2003*, Comandè - Ponzanelli (a cura di), Torino, 2004, pp. 3 ss.;

CAMALDO, *Intelligenza artificiale e investigazione penale predittiva*, in *Rivista Italiana di Diritto e Procedura Penale*, 2024, 1, pp. 233 ss.;

CANALINI, *L'algoritmo come "atto amministrativo informatico" e il sindacato del giudice*, in *Giornale di diritto amministrativo*, 2019, pp. 781 ss.

CANESCHI, *Le modifiche relative all'udienza preliminare*, in AA.VV., *Riforma Cartabia. Le modifiche al sistema penale*, *Commentario diretto da Gian Luigi Gatta e Mitja Gialuz*, *Nuove dinamiche del procedimento penale*, Bene - Bontempelli - Luparia Donati (a cura di), II, Torino, 2024, pp. 135 ss.;

CANESCHI, *Intelligenza artificiale e sistema penitenziario*, in *Rivista Italiana di Diritto e Procedura Penale*, 2024, 1, pp. 251 ss.;

CANZIO, *AI Act e processo penale: sfide e opportunità*, in *Sistema penale online*, 14 ottobre 2024;

CANZIO, *Prefazione*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, Baccari - Felicioni (a cura di), 2023, Milano, pp. IX ss.;

CANZIO, *La motivazione della sentenza e la prova scientifica: "reasoning by probabilities"*, in AA.VV., *Prova scientifica e processo penale*, Canzio - Luparia Donati (a cura di), 2022, ed. II, Milano, pp. 3 ss.;

CANZIO, *Intelligenza artificiale e processo penale*, in AA.VV., *Prova scientifica e processo penale*, Canzio - Luparia Donati (a cura di), 2022, Milano, ed. II, pp. 903;

CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale*, 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, pp. 129 ss.;

CANZIO, *Il dubbio e la legge*, in *Diritto penale contemporaneo online*, 20 luglio 2018;

CANZIO, *La valutazione della prova scientifica fra verità processuale e ragionevole dubbio*, in *Archivio penale*, 2011, 3, pp. 1 ss.;

CANZIO - TARUFFO - UBERTIS, *Opinioni a confronto. Fatto, prova e verità (alla luce del principio dell'oltre ogni ragionevole dubbio),* in *Criminalia*, 2009, pp. 305 ss.;

CANZIO, *Prova scientifica, ricerca della "verità" e decisione giudiziaria nel processo penale*, in AA. VV., *Scienza e causalità*, Di Maglie - Seminara (a cura di), Padova, 2006, pp. 143 ss.;

CANZIO, *L'oltre ogni ragionevole dubbio come regola probatoria e di giudizio nel processo penale*, in *Rivista Italiana di Diritto e Procedura Penale*, 2004, pp. 303 ss.;

CAPRIOLI, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cassazione penale*, 2008, pp. 3520 ss.;

CARRATTA, *Decisione robotica e valori del processo*, in *Rivista di diritto processuale*, 2020, pp. 491 ss.;

CASONATO - MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal - Rivista di BioDiritto*, 2021, pp. 415 ss.;

CASTELLI - PIANA, *Giusto processo e intelligenza artificiale*, Santarcangelo di Romagna, 2019;

CASTETS - RENARD, *Human Rights and Algorithmic Impact Assessment for Predictive Policing*, in AA.VV., *Constitutional Challenges in the Algorithmic Society*, Micklitz - Pollicino - Reichman - Simoncini - Sartor - De Gregorio (*edited by*), Cambridge, 2022, pp. 93 ss.;

CATALANO, *Ragionevole dubbio e logica della decisione. Alle radici del giusnaturalismo processuale*, Milano, 2016;

CATALANO - CURTOTTI NAPPI - DELLA MONICA - LORUSSO - MONTAGNA – PROCACCINO (a cura di), *Prova penale e metodo scientifico*, Torino, 2009;

CATERINI, *Il giudice penale robot*, in *La legislazione penale*, 19 dicembre 2020, pp. 1 ss.;

CECCHI, *Il giudice dinanzi alla prova scientifica*, in *Archivio Penale web*, 2022, 1, pp. 1 ss.;

CECCHI, *Sfogliando* Justice Machines: *evocazioni antesignane su diritto e intelligenza artificiale*, in *Cassazione Penale*, 2021, pp. 4172 ss.;

CENTRORAME, *Le indagini tecnologiche ad alto potere intrusivo fra esigenze di accertamento e sacrale inviolabilità dei diritti della persona*, in *Rivista Italiana di Diritto e Procedura Penale*, 2021, pp. 499 ss.;

CIVITA, *Udienza preliminare: la nuova regola di giudizio per la sentenza di non luogo a procedere*, in AA.VV., *La Riforma Cartabia*, Spangher (a cura di), Pisa, 2022, pp. 317 ss.;

COLAMUSSI, *"Oltre il ragionevole dubbio": il principio e la Costituzione,* in AA. VV., Incampo - Scalfati (a cura di), *Giudizio penale e ragionevole dubbio,* Bari, 2017, pp. 173 ss.;

CONTI, *La prova scientifica alle soglie dei vent'anni dalla sentenza Franzese: vette e vertigini in epoca di pandemia*, in *Sistema penale online*, 9 febbraio 2021;

CONTI, *Il BARD paradigma di metodo: legalizzare il convincimento senza riduzionismi aritmetici*, in *Diritto penale e processo*, 2020, pp. 829 ss.;

CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Diritto penale e processo*, 2018, pp. 1210 ss.;

CONTISSA - GALLI - GODANO - SARTOR, *La nuova Proposta di Regolamento europeo sull'intelligenza artificiale: questioni giuridiche e approcci regolatori*, in AA.VV., *Nuove questioni di informatica forense*, Brighi (a cura di), Roma, 2022, pp. 387 ss.;

CONTISSA - LASAGNI, *When it is (also) Algorithms and AI that decide on Criminal Matters: In Search of an Effective Remedy*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2020, pp. 280 ss.;

CONZ, *La discrezionalità vincolata del giudice nella commisurazione del cumulo giuridico delle pene*, in *Cassazione penale*, 2022, pp. 1369 ss.;

CONZ, *La sentenza delle Sezioni unite sull'onere per il giudice di calcolare e motivare l'aumento di pena per ciascuno dei reati uniti dal vincolo della continuazione*, in *Sistema penale online*, 20 gennaio 2021;

COPPOLA, *Commisurazione della pena e intelligenza artificiale: una ipotesi di lavoro con l'algoritmo Ex-Aequo*, in *Archivio penale web*, 2023, 2, pp. 1 ss.;

COSIMI, *Jerry Kaplan sull'AI generativa: "Non preoccupiamoci di cosa farà a noi ma guardiamo a quel che farà per noi"*, in *Wired online*, 31 ottobre 2024;

COVELLI, *Dall'informatizzazione della giustizia alla «decisione robotica»? Il giudice del merito*, in AA.VV., *Decisione robotica*, Carleo (a cura di), Bologna, 2019, pp. 125 ss.;

CUPELLI, *Prova scientifica, regole cautelari e responsabilità medica*, in *Sistema penale online*, 14 marzo 2023;

D'AGOSTINO, *Gli algoritmi predittivi per la commisurazione della pena. A proposito dell'esperienza statunitense nel c.d.* evidence-based sentencing, in *Diritto penale contemporaneo - Rivista trimestrale*, 2019, 2, pp. 354 ss.;

D'ALOIA, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in AA.VV., *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, D'Aloia (a cura di), Milano, 2020, pp. 7 ss.;

DALY - HAGENDORFF - MANN - MARDA - WAGNER - WEI WANG, *AI, Governance and Ethics. Global Perspective*, in AA.VV., *Constitutional Challenges in the Algorithmic Society*, Micklitz - Pollicino - Reichman - Simoncini - Sartor - De Gregorio (*edited by*), Cambridge, 2022, pp. 182 ss.;

DANIELE, *La riforma Cartabia del processo penale: pretese algoritmiche ed entropia sistemica*, in *Sistema penale*, 2023, 7-8, pp. 19 ss.;

DANIELE, *L'abolizione dell'udienza preliminare per rilanciare il sistema accusatorio*, in *Sistema penale*, 2020, 1, pp. 131 ss.;

DE CATALDO, *L'operazione decisoria da emanazione divina alla prova scientifica*, Padova, 2014;

DE FELICE, *Intelligenza artificiale e processi decisionali automatizzati: GDPR ed* ethics by design *come avamposto per la tutela dei diritti umani*, in AA.VV., *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, D'Aloia (a cura di), Milano, 2020, pp. 415 ss.;

DE FELICE, *Su probabilità, «precedente» e calcolabilità giuridica,* in *Rivista di diritto processuale*, 2017, pp. 1546 ss.;

DE KERCKHOVE, *La decisione datacratica*, in AA.VV., *Decisione robotica*, Carleo (a cura di), Bologna, 2019, pp. 97 ss.;

DE RENZIS, *Primi passi nel mondo della giustizia «high tech»: la decisione in un corpo a corpo virtuale tra tecnologia e umanità*, in AA.VV., *Decisione robotica*, Carleo (a cura di), Bologna, 2019, pp. 139 ss.;

DELL'ANNO, *Obbligo di motivazione e ragionevole dubbio,* in *Processo penale e giustizia,* 2017, n. 3, pp. 522 ss.;

DELLA MONICA, *Il filtro della ragionevole previsione di condanna*, in *Archivio penale*, 2023, 2, pp. 1 ss.;

DELLA TORRE, *La ragionevole previsione di condanna*, in *La legislazione penale*, 19 luglio 2024, pp. 1 ss.;

DELLA TORRE, *Quale spazio per i* tools *di riconoscimento facciale nella giustizia penale?*, in AA.VV., *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, Di Paolo - Presacco (a cura di), Napoli, 2022, pp. 7 ss.;

DELLA TORRE, *Le decisioni algoritmiche all'esame del Consiglio di Stato*, in *Rivista di diritto processuale*, 2021, pp. 713 ss.;

DELLERBA, *La giustizia predittiva come possibile antidoto all'inadeguatezza della giurisdizione*, in *Sistema penale online*, 28 marzo 2024;

DELVECCHIO, *Prospettive e tempi della digitalizzazione del processo*, in *Processo penale e giustizia*, 2022, pp. 8 ss.;

DERSHOWITZ, *Dubbi ragionevoli. Il sistema della giustizia penale nel caso O.J. Simpson*, Milano, 2007;

DI GIOVINE, *Il* judge-bot *e le sequenze giuridiche in materia penale*, in *Cassazione penale*, 2020, pp. 951 ss.;

DI NICOLA, *La semplificazione delle attività di deposito di atti, documenti e istanze*, in *Processo penale e giustizia*, fasc. straord., *Giustizia penale: la disciplina transitoria della c.d. riforma Cartabia*, Cimadomo (a cura di), 2023, pp. 25 ss.;

DICK, *Rapporto di minoranza e altri racconti*, trad. it a cura di Prezzavento, 2002, Roma;

DI SALVO, *Noi e i robot. Intervista a Jerry Kaplan*, in *Wired online*, settembre 2017;

DIXON, *Artificial Intelligence: Benefits and Unknown Risks*, in www.americanbar.org, 15 gennaio 2021;

DOMINIONI, *La prova penale scientifica*, Milano, 2005;

DONATI, *Diritti fondamentali e algoritmi nella proposta di regolamento sull'intelligenza artificiale*, in AA.VV., *Intelligenza artificiale e diritto: una rivoluzione?*, Pajno - Donati - Perrucci (a cura di), *Diritti fondamentali, dati personali e regolazione*, Bologna, 2022, 1, pp. 111 ss.;

DONATI, *Intelligenza artificiale e giustizia*, in AA.VV., *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, D'Aloia (a cura di), Milano, 2020, pp. 237 ss.;

DORIGO (a cura di), *Il Ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020;

ERCOLE, *Contro la "giustizia predittiva". Per una lettura conservativa del principio di certezza del diritto*, Torino, 2024;

FANCHIOTTI, voce *Processo penale statunitense*, in *Enciclopedia del diritto*, *Annali*, II, I, Milano, 2008, pp. 808 ss.;

FANUELE, *I nuovi criteri per la decisione di non luogo a procedere*, in *Processo penale e giustizia*, 2023, pp. 958 ss.;

FELICIONI, *L'attività valutativa del giudice tra ragione ed emozione*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, Baccari - Felicioni (a cura di), Milano, 2023, pp. 3 ss.;

FERRUA, *Regole di giudizio e udienza preliminare*, in *Processo penale e giustizia*, 2023, pp. 966 ss.;

FERRUA, *Tre temi corderiani: modelli di giustizia procedurale, prove critico-indiziarie, regole di giudizio*, in AA. VV., *Corderiana. Sulle orme di un maestro del rito penale*, Catalano - Ferrua (a cura di), Torino, 2023, pp. 83 ss.;

FERRUA, *Un giardino proibito per il legislatore: la valutazione delle prove*, in *Questione giustizia*, 1988, pp. 587 ss.;

FIANDACA, voce *Misure di prevenzione (profili sostanziali)*, in *Digesto delle discipline penalistiche*, VIII, Torino, 1994, pp. 108 ss.;

FIDELBO, *Verso il sistema del precedente? Sezioni Unite e principio di diritto*, in AA.VV., *La riforma delle impugnazioni tra carenze sistematiche e incertezze applicative*, BARGIS - BELLUTA (a cura di), Torino, 2018, pp. 115 ss.;

FINOCCHIARO, *La Proposta di Regolamento sull'intelligenza artificiale: il modello europeo bastato sulla gestione del rischio*, in *Diritto dell'Informazione e dell'Informatica (II)*, 2, 1 aprile 2022, pp. 303 ss.;

FIORIO, *Predizione algoritmica e giurisdizione di sorveglianza*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, Baccari - Felicioni (a cura di), Milano, 2023, pp. 247 ss.;

FLORIDI, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Milano, 2022;

FLORIDI - SANDERS, *On the Morality of Artificial Agents*, in *Minds and Machines*, 2004, pp. 349 ss.;

FORZA, *Le scienze comportamentali ed il loro contributo nello studio dei processi decisionali*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale,* Baccari - Felicioni (a cura di), Milano, 2023, pp. 33 ss.;

FORZA - MENEGONI - RUMIATI, *Il giudice emotivo. La decisione tra ragione ed emozione*, Bologna, 2017;

FRONZA - CARUSO, *Ti faresti giudicare da un algoritmo? Intervista a Antoine Garapon*, in *Questione giustizia*, 2018, 4, pp. 196 ss.;

FROSINI, *L'orizzonte giuridico dell'intelligenza artificiale*, in *Diritto dell'Informazione e dell'Informatica (II)*, I, 1 febbraio 2022, pp. 5 ss.;

GABBRIELLI, *Dalla logica al* deep learning: *una breve riflessione sull'intelligenza artificiale*, in AA.VV., *XXVI lezioni di diritto dell'intelligenza artificiale*, Ruffolo (a cura di), Bologna, 2019, pp. 21 ss.;

GALGANI - AGOSTINO, *L'impiego dei collegamenti audiovisivi ai fini della partecipazione e dell'assunzione probatoria*, in AA.VV., *Riforma Cartabia. Le*

modifiche al sistema penale, *Commentario diretto da Gian Luigi Gatta e Mitja Gialuz*, *Il procedimento penale tra efficienza, digitalizzazione e garanzie partecipative*, Caianiello - Gialuz - Quattrocolo (a cura di), I, Torino, 2024, pp. 213 ss.;

GALGANI, *Forma e garanzie nel prisma dell'innovazione tecnologica. Alla ricerca di un processo penale "virtuoso"*, Milano, 2022;

GALGANI, *Considerazioni sui "precedenti" dell'imputato e del giudice al cospetto dell'IA nel processo penale*, in *Sistema penale*, 2020, 4, pp. 81 ss.;

GALGANI, *Il processo penale in "ambiente" digitale: ragioni e (ragionevoli) speranze*, in *Questione giustizia*, 2021, 4, pp. 181 ss.;

GALLI, *Law Enforcement and Data-Driven Predictions at the National and EU Level. A Challenge to the Presumption of Innocence and Reasonable Suspicion?*, in AA. VV., *Constitutional Challenges in the Algorithmic Society*, Micklitz - Pollicino - Reichman - Simoncini - Sartor - De Gregorio (*edited by*), Cambridge, 2022, pp. 111 ss.;

GARAPON - LASSÈGUE, *La giustizia digitale. Determinismo tecnologico e libertà*, ed. it. a cura di Ferrarese, Bologna, 2021;

GIALUZ - DELLA TORRE, *Giustizia per nessuno. L'inefficienza del sistema penale italiano tra crisi cronica e riforma Cartabia*, Torino, 2022;

GIALUZ, *Per un processo penale più efficiente e giusto. Guida alla lettura della riforma Cartabia. Profili processuali*, in *Sistema penale*, 28 ottobre 2022;

GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, 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, pp. 52 ss.;

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 online*, 28 maggio 2019;

GILLESPIE, *The relevance of Algorithms*, in AA.VV., *Media Technologies. Essays on Communication, Materiality, and Society,* Gillespie - Boczkowski - Foot (*edited by*), Cambridge, 2014, pp. 167 ss.;

GIUNTA, *Ghiribizzi penalistici per colpevoli. Legalità, "malalegalità", dintorni*, Pisa, 2019.

GRASSO, *Le misure di prevenzione personali e patrimoniali nel sistema costituzionale*, in *Sistema penale online*, 14 febbraio 2020;

HEAVEN, *Predictive policing algorithms are racist. They need to be dismantled*, in *MIT Technology Review online*, 17 luglio 2020;

HEAVEN, *Macchine che pensano. La nuova era dell'intelligenza artificiale*, Bari, 2018;

HEIDEGGER, *L'abbandono*, trad. it. a cura di Fabris, Genova, 1995;

HEIKKILA, *The White House just unveiled a new Bill of Rights*, in *MIT Technology Review online*, 4 ottobre 2024;

IACOVIELLO, voce *Motivazione della sentenza penale (controllo della)*, in *Enciclopedia del Diritto*, Aggiornamento IV, Milano, 2000, pp. 750 ss.;

ILLUMINATI, *La presunzione d'innocenza dell'imputato,* Bologna, 1979;

INTRIERI - VIOLA, *Ragionevole previsione di condanna e giustizia predittiva: una modesta proposta per la riforma dell'art. 425 c.p.p.*, in www.giustiziainsieme.it, 1 febbraio 2022;

ITALIANO, *Intelligenza Artificiale, che errore lasciarla agli informatici*, in *Agenda digitale online*, 11 giugno 2019;

KAPLAN, *Intelligenza artificiale. Guida al futuro prossimo*, Roma, 2018;

KARNOW, *The Opinion of Machine*, in AA.VV., *The Cambridge Handbook of the Law of Algorithms*, Barfield (*edited by*), Cambridge, 2021, pp. 16 ss.;

KOSTORIS, *Predizione decisoria e* diversion *processuale*, 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, pp. 93 ss.;

KOULU - SANKARI - HIRVONEN - HEIKKINEN, *Artificial intelligence and the law: can we and should we regulate Ai system?*, in AA.VV., *The Cambridge Handbook of the Law of Algorithms*, Barfield (*edited by*), Cambridge, 2021, pp. 427 ss.;

KUGLER, *AI Judges and Juries*, in *Communications of the ACM*, 2018, 61, 12, pp. 19 ss.;

LA REGINA, *I.A. e ragionamento giuridico: la giustizia prevedibile*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, Baccari - Felicioni (a cura di), Milano, 2023, pp. 168 ss.;

LA REGINA, *L'archiviazione nel vortice efficientista*, in AA.VV., Spangher (a cura di), *La Riforma Cartabia*, Pisa, 2022, pp. 276 ss.;

LA VATTIATA, *Brevi note «a caldo» sulla recente Proposta di Regolamento Ue in tema di intelligenza artificiale*, in *Diritto penale e uomo online*, 2021, pp. 1 ss.;

LAGIOIA - SARTOR, *Il sistema compas: algoritmi, previsioni, iniquità*, in AA.VV., *XXVI lezioni di diritto dell'intelligenza artificiale*, Ruffolo (a cura di), Bologna, 2019, pp. 226 ss.;

LEGNINI, *Introduzione*, in AA.VV., *Decisione robotica*, Carleo (a cura di), Bologna, 2019, pp. 9 ss.;

LEO, *La regola di giudizio dell'archiviazione e la riapertura delle indagini*, in AA.VV., *Riforma Cartabia. Le modifiche al sistema penale*, *Commentario diretto da Gian Luigi Gatta e Mitja Gialuz*, *Nuove dinamiche del procedimento penale*, Bene - Bontempelli - Luparia Donati (a cura di), II, Torino, 2024, pp. 81 ss.;

LETTIERI, *Law in Turing's Cathedral*, in AA.VV., *The Cambridge Handbook of the Law of Algorithms*, Barfield (*edited by*), Cambridge, 2021, pp. 691 ss.;

LIPTAK, *Sent to Prison by a Software Program's Secret Algorithms*, in *New York Times*, 1 maggio 2017;

LIVNI, *Nei tribunali del New Jersey è un algoritmo a decidere chi esce su cauzione*, in www.internazionale.it, 2017;

LORUSSO, *La sfida dell'intelligenza artificiale al processo penale nell'era digitale*, in *Sistema penale*, 28 marzo 2024;

LORUSSO, Digital evidence, cybercrime *e giustizia penale 2.0*, in *Processo penale e giustizia*, 2019, pp. 821 ss.

LORUSSO, *Il diritto alla motivazione*, in *Diritto penale contemporaneo online,* 8 novembre 2018;

LORUSSO, *Il contributo degli esperti alla formazione del convincimento giudiziale*, in *Archivio Penale*, 2011, pp. 809 ss.;

LORUSSO, *Prova scientifica*, in AA.VV., *La prova penale*, Gaito (diretto da), II, Torino, 2008, pp. 319 ss.;

LUCIANI, *La decisone giudiziaria robotica*, in AA.VV., *Decisione robotica*, Carleo (a cura di), Bologna, 2019, p. 86;

LUPARIA DONATI, *La promessa della giustizia tecnologica*, in *Sistema penale online*, 1 agosto 2024;

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, pp. 113 ss.;

LUPARIA DONATI, *Artificial Intelligence in Criminal Courts. Opportunity or Threat?*, in AA.VV., *Legal Challenges in the New Digital Age*, Lopez Rodriguez – Green - Kubica (*edited by*), Leiden, 2021, pp. 160 ss.;

LUPARIA DONATI, Privacy, *diritti della persona e processo penale*, in *Rivista di diritto processuale*, 2019, pp. 1488 ss.;

MAFFEO, *Giustizia predittiva e principi costituzionali*, in i-lex. *Scienze Giuridiche, Scienze Cognitive e Intelligenza Artificiale-Rivista quadrimestrale online*, 2019, 12, pp. 277 ss.;

MAGLIULO, *L'Intelligenza Artificiale nel processo penale: progresso o rischio per la tutela dei diritti costituzionali?*, in *Il Processo*, 2022, pp. 559 ss.;

MALINO, *Esercizio dell'azione penale e prognosi di condanna mediante* software *predittivi. Verso la creazione di un PM-robo*t, in *La Legislazione penale*, 19 giugno 2024;

MANES - SANTANGELO, Mechanical judgement: *un processo* in action *di automazione della decisione penale?*, in AA.VV., *La trasformazione digitale della giustizia nel dialogo tra discipline*, Palmirani - Sapienza (a cura di), Milano, 2022, pp. 139 ss.;

MANES, *Intelligenza artificiale e giustizia penale*, in AA.VV., *XXVI lezioni di diritto dell'intelligenza artificiale*, Ruffolo (a cura di), Torino, 2021, pp. 280 ss.;

MANES, *L'oracolo algoritmico e la giustizia penale: al piglio tra tecnologia e tecnocrazia*, in *Discrimen*, 15 maggio 2020;

MARINI BALESTRA, *L'intensità della regolazione: la necessità di graduare le regole in funzione di parametri di difformità*, in AA.VV., *Intelligenza artificiale e diritto: una rivoluzione?*, *Diritti fondamentali, dati personali e regolazione*, Pajno - Donati - Perrucci (a cura di), Bologna, 2022, 1, pp. 533 ss.;

MARZADURI, *Il declino del paradigma accusatorio ed il ritorno all'istruzione sommaria*, in *La Legislazione penale*, 3 agosto 2023;

MASCOLO, *Gli algoritmi amministrativi: la sfida della comprensibilità*, in *Giurisprudenza italiana*, 2020, pp. 1190 ss.;

MAUGERI, *L'uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra* evidence based practies *e tutela dei diritti fondamentali*, in *Archivio penale web*, 17 maggio 2021;

MCCARTHY - MINSKY - ROCHESTER - SHANNON, *A proposal for the Dartmouth Summer Research Project on Artificial Intelligent*, *August 31*, 1995, in 27 *AI Magazine*, 2006;

MENNA, *L'inquadramento della regola di giudizio del non luogo a procedere tra passato e presente dell'udienza preliminare*, *Archivio penale web*, 1 febbraio 2023;

METZ, *AI Is Transforming Google Search. The Rest of the Web Is next*, in *Wired online*, 4 febbraio 2016;

MILIZIA, *Carta etica europea sull'uso dell'intelligenza artificiale nei sistemi giudiziari e loro sviluppo*, in *Il Processo Telematico*, 20 marzo 2019;

MONTAGNA, *Prognosi personologica, commisurazione della pena e applicazione di misure di sicurezza*, in AA.VV., *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, Baccari - Felicioni (a cura di), Milano, 2023, pp. 223 ss.;

MOSCARINI, *Riflessioni sul modello attuale delle misure di prevenzione personale*, in *Processo penale e giustizia*, 2023, pp. 936 ss.;

MOSCATO, Calculemus? *Da Leibniz all'intelligenza artificiale*, 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, pp. 25 ss.;

NARDO, *La progressiva digitalizzazione del processo*, in *Processo Penale e Giustizia*, fasc. straord., *La disciplina transitoria della c.d. riforma Cartabia*, cit., 2023, pp. 21 ss.;

NICOLÌ, *La predizione nell'attività di polizia*, 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, pp. 45 ss.;

NIEVA-FENOLL, *Intelligenza artificiale e processo*, Torino, 2019, trad. it. a cura di Comoglio;

NIOLA, *IA, ecco il primo trattato internazionale: la Convenzione del Consiglio d'Europa*, in *Agenda digitale online*, 6 settembre 2024;

NOBILI, *Il principio del libero convincimento del giudice*, 1974, Milano;

ODDENINO, *Intelligenza artificiale e tutela dei diritti fondamentali: alcune notazioni critiche sulla recente Proposta di Regolamento della UE, con particolare riferimento all'approccio basato sul rischio e al pericolo di discriminazione algoritmica*, in AA.VV., *Intelligenza artificiale e diritto: una rivoluzione?*, *Diritti fondamentali, dati personali e regolazione*, Pajno - Donati - Perrucci, Bologna, 2022, 1, pp. 165 ss.;

PAJNO - BASSINI - DE GREGORIO - MACCHIA - PATTI - POLLICINO - QUATTROCOLO - SIMEOLI - SIRENA, *AI: profili giuridici. Intelligenza Artificiale: criticità emergenti e sfide per il giurista,* in *BioLaw Journal - Rivista di BioDiritto*, 2019, 3, pp. 205 ss.;

PALAZZO, *Considerazioni minime sulla prevedibilità della decisione giudiziale (tra miti, illusioni e pragmatismi)*, in *Cassazione penale*, 2022, 3, pp. 941 ss.;

PALESU, *Intelligenza artificiale e giustizia penale. Una lettura attraverso i principi*, in *Archivio penale web*, 9 maggio 2022;

PALMIOTTO, *The Black box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, in AA.VV., *Algorithmic governance and governance of algorithmic*, Ebers - Cantero Gamito (*edited by*), Cham, pp. 49 ss.

PALMIRANI - SAPIENZA - BOMPREZZI, *Il ruolo dell'intelligenza artificiale nel sistema giustizia: funzionalità, metodologie, principi*, in AA.VV., Palmirani - Sapienza (a cura di), *La trasformazione digitale della giustizia nel dialogo tra discipline*, Milano, 2022, pp. 1 ss.;

PALMIRANI - PODDA, *Anonimizzazione e pseudonimizzazione di sentenze giudiziarie*, in AA.VV., *La trasformazione digitale della giustizia nel dialogo tra discipline*, Palmirani - Sapienza (a cura di*),* Milano, 2022, pp. 37 ss.;

PALMIRANI, *Interpretabilità, conoscibilità, spiegabilità dei processi decisionali automatizzati*, in AA.VV., *XXVI lezioni di diritto dell'intelligenza artificiale*, Ruffolo (a cura di), Torino, 2021, pp. 68 ss.;

PARISE, *"Alexa, chi è l'assassino?": anche in Italia gli smartspeaker potrebbero essere testimoni*, in *Agenda Digitale online*, 22 novembre 2019;

PERRY - MCINNIS - PRICE - SMITH - HOLLYWOOD, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, Santa Monica, 2013;

PICOTTI, *Diritto penale, tecnologie informatiche e intelligenza artificiale: una visione d'insieme*, in AA.VV., *Cybercrime*, Cadoppi - Canestrari - Manna - Papa (diretto da), Milano, 2023, pp. 3 ss.;

PIERGALLINI, *Intelligenza artificiale: da "mezzo" a "autore" del reato*, in *Rivista Italiana di Diritto e Procedura Penale*, 2020, pp. 1745 ss.;

PUNZI, Judge in the machine. *E se fossero le macchine a restituirci l'umanità del giudicare?*, in AA.VV., *Decisione robotica*, Carleo (a cura di), Bologna, 2019, pp. 319 ss.;

PRESACCO, *Intelligenza artificiale e ragionamento probatorio nel processo penale*, in AA.VV., *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, Di Paolo - Presacco (a cura di), Napoli, 2022, pp. 91 ss.;

QUATTROCOLO, *Risk assessment: sentencing o non sentencing?*, 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, pp. 69 ss.;

QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Springer, 2020;

QUATTROCOLO, *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *MediaLaws*, 3, 2020, pp. 121 ss.;

QUATTROCOLO, *Quesiti nuovi e soluzioni antiche*, in *Cassazione penale*, 2019, pp. 1748 ss.;

QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *La legislazione penale*, 18 dicembre 2018;

REICHMAN - SARTOR, *Algorithms and Regulation*, in AA.VV., *Constituional Challenges in the Algorithmic Society*, Micklitz - Pollicino - Reichman - Simoncini - Sartor - De Gregorio (*edited by*), Cambridge, 2022, pp. 131 ss.;

RENDA, *Moral Machine*, in AA.VV., *The Cambridge Handbook of the Law of Algorithms*, Barfield (*edited by*), Cambridge, 2021, pp. 667 ss.;

RENZETTI, *L'udienza preliminare ridisegnata e la nuova udienza di comparizione predibattimentale*, in AA. VV., *Commenti alla legge n. 134 del 2021. Riassetti della penalità, razionalizzazione del procedimento di primo grado, giustizia riparativa*, Catalano - Kostoris - Orlandi (a cura di), Torino, 2023, II, pp. 113 ss.;

RICCIO, *Ragionando su intelligenza artificiale e processo penale*, in *Archivio penale web*, 21 novembre 2019;

ROMANELLI, *Aumenti di pena per la continuazione e obblighi motivazionali: le Sezioni unite tra novità e conservazione*, in *Processo penale e giustizia*, 2022, pp. 932 ss.;

ROMANO, *Diritto, robotica e teoria dei giochi: riflessioni su una sinergia*, in AA.VV., *Diritto e intelligenza artificiale*, Alpa (a cura di), Pisa, 2020, pp. 103 ss.;

ROTH, *The Use of Algorithms in Criminal Adjudication*, in AA.VV., *The Cambridge Handbook of the Law of Algorithms*, Barfield (*edited by*), Cambridge, 2021, pp. 407 ss.;

ROVATTI, *Il processo di apprendimento algoritmico e le applicazioni nel settore legale*, in AA.VV., *XXVI lezioni di diritto dell'intelligenza artificiale*, Ruffolo (a cura di), Bologna, 2019, pp. 31 ss.;

ROYER - VANLEEUW, *Criminal law and tecnology*, in AA.VV., *Research Handbook on the Law of Artificial Intelligence*, Barfield - Pagallo (*edited by*), Cheltenham, 2018, pp. 190 ss;

RUFFOLO, *La* machina sapiens *come "avvocato generale" ed il primato del giudice umano*, in AA.VV., *XXVI lezioni di diritto dell'intelligenza artificiale*, Ruffolo (a cura di), Torino, 2021, pp. 205 ss.;

RUSSEL - NORVIG, *Intelligenza artificiale. Un approccio moderno*, 1, Milano, 2005,;

SACCOMANI, *L'impatto della giustizia algoritmica sul diritto all'equo processo*, in *Cassazione Penale*, 2023, pp. 628 ss.;

SALLANTIN - SZCZECINIARZ (a cura di), *Il concetto di prova alla luce dell'intelligenza artificiale*, Milano, 2005;

SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Rivista Italiana di Diritto e Procedura Penale*, 2021, pp. 83 ss.;

SCACCIANOCE, *Notificazioni al difensore dirette all'imputato*, in *Processo Penale e Giustizia*, 2022, pp. 25 ss.;

SCALFATI, *IA e processo penale: prospettive d'impiego e livelli di rischio*, in *Processo penale e giustizia*, 2024, pp. 1404 ss.;

SCALFATI (a cura di), *Le indagini atipiche*, II ed., Torino, 2019;

SEYMOUR - SINGER - DOLAN, *The neurobiology of punishment*, in *Nature*, 2007, 8, pp. 300 ss.;

SHAFER, *A Mathematical Theory of Evidence*, Princerton, 1979;

SHAPIRO,*"Beyond Reasonable Doubt" and "Probable Cause". Historical Prospectives on the Anglo-American Law of Evidence*, Oakland, 1991;

SIGNORATO, *Il diritto a decisioni penali non basate esclusivamente su trattamenti automatizzati: un nuovo diritto derivante dal rispetto della dignità umana*, in *Rivista di diritto processuale*, 2021, pp. 101 ss.;

SIGNORATO, *Giustizia penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo*, in *Rivista di diritto processuale*, 2020, pp. 605 ss.;

SILVA, *La continuazione di reati torna alle Sezioni Unite: la conferma - prevedibile - della necessità di indicare e motivare ciascun aumento di pena per i reati satellite*, in *Giurisprudenza italiana*, 2022, pp. 1719 ss.;

SIMON, *Reversal of Fortune: The Resurgence of Individual Risk assessment in Criminal Justice*, in *Annual Review of Law and Social Science*, 2005, pp. 397 ss.;

SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal-Rivista di Biodiritto*, 2019, 1, pp. 63 ss.;

SLOBOGIN, *Assessing the Risk of Offending through Algorithms*, in AA.VV., *The Cambridge Handbook of the Law of Algorithms*, Barfield (*edited by*), Cambridge, 2021, pp. 432 ss.;

SPANGHER, *Questioni in tema di investigazioni nella giustizia italiana*, in *Studium Iuris*, 2021, pp. 1039 ss.;

STELLA, *Giustizia e modernità: la protezione dell'innocente e la tutela delle vittime,* Milano, 2001;

STONE - ALTMAN - BRYNJOLFSSON - CONITZER - GRAY - GROSZ - HOWARD - LIANG - LIN - MANYIKA - MCLLRAITH - SONENBERG - WAJCMAN, *Gathering Strenght,*

Gathering Storms, in *One hundred year study on Artificial Intelligence*, Stanford University, settembre 2021;

STONE - BROOKS - BRYNJOLFSSON - CALO - ETZIONI - HAGER - HIRSCHBERG - KALYANAKRISHNAN - KAMAR - KRAUS - LEYTON-BROWN - PARKES PRESS - SAXENIAN - SHAH - TAMBE - TELLER, *Artificial Intelligence and life in 2030*, in *One hundred year study on Artificial Intelligence*, Stanford University, 16 settembre 2016;

TARONI - BOZZA - VUILLE, *La probabilità come strumento per una coerente valutazione della prova scientifica*, in AA.VV., *Prova scientifica e processo penale*, Canzio - Luparia Donati (a cura di), Milano, 2022, II ed., pp. 21 ss.;

TESCAROLI, *Il procedimento di prevenzione patrimoniale: profili problematici e questioni aperte*, in *Questione giustizia online*, 15 febbraio 2022;

TONDIN, *La nuova regola di giudizio della ragionevole previsione di condanna*, in *Cassazione penale*, 2023, pp. 404 ss.;

TONINI, *La Cassazione accoglie i criteri Daubert sulla prova scientifica. Riflessi sulla verifica delle massime di esperienza*, in *Diritto penale e processo*, 2011, pp. 1341 ss.;

TORRE, *Intelligenza artificiale e indagini penali: prospettive future e garanzie di sistema. Il sistema automatico di riconoscimento immagini*, in AA.VV., *Cybercrime*, Cadoppi - Canestrari - Manna - Papa (diretto da), Milano, 2023, pp. 1731 ss.;

TORRE, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Diritto penale e processo*, 2021, pp. 1042 ss.;

TURING, *Computing Machinery and Intelligence*, in *Mind*, LIX, 236, 1 ottobre 1950, p. 433 ss.;

UBERTIS, *Intelligenza artificiale e giustizia predittiva,* in *Sistema penale online*, 16 ottobre 2023;

UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, 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, pp. 9 ss.;

UBERTIS, *La valutazione bayesiana delle prove incerte*, in *Cassazione penale*, 2021, pp. 1093 ss.;

UBERTIS, *Verso una teoria degli* standard *di prova*, in *Cassazione penale*, 2021, pp. 2214 ss.;

VASTA, *Diritto dell'Unione Europea e intelligenza artificiale. Riflessi sul procedimento penale*, in *Rivista Italiana di Diritto e Procedura Penale*, 2024, pp. 271 ss.;

VICOLI, *Nuovi equilibri delle indagini preliminari*, in AA.VV., *Commenti alla legge n. 134 del 2021. Riassetti della penalità, razionalizzazione del procedimento di primo grado, giustizia riparativa*, Catalano - Kostoris - Orlandi (a cura di), Torino, 2023, pp. 71 ss.;

VIGONI, *Giudizi prognostici e ragionevole dubbio,* in AA. VV., *Giudizio penale e ragionevole dubbio*, Incampo - Scalfati (a cura di), Bari, 2017, pp. 373 ss.;

VINCENTI, *Il «problema» del giudice-robot*, in AA.VV., *Decisione robotica,* Carleo (a cura di), Bologna, 2019, pp. 111 ss.;

WEAVER, *Regulation of artificial intelligence in the United States*, in AA. VV., *Research Handbook on the Law of Artificial Intelligence*, Barfield - Pagallo (*edited by*), Cheltenham, 2018, pp. 155 ss.;

WHITMAN, *The Origins of Reasonable Doubt. Theological Roots of the Criminal Trial*, Yale University Press, New Haven, 2008;

ZANICHELLI, *Ecosistemi, opacità, autonomia: le sfide dell'intelligenza artificiale in alcune proposte recenti della Commissione europea*, in AA. VV., *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, D'Aloia (a cura di), Milano, 2020, pp. 67 ss.