L'AI ACT NELL'OTTICA DEL PROCESSUAL - PENALISTA:UNO SGUARDO PRELIMINARE

Carolina Teresi

Sommario **1. L'*AI Act* tra *unicum* legislativo e obsolescenza. Quanto velocemente progredisce la tecnica rispetto al diritto. - 2. Sistemi di IA ad alto rischio e amministrazione della giustizia. - 3. La riservatezza e gli altri diritti fondamentali come principale ostacolo al connubio giustizia–IA. - 4. IA e giustizia penale: un azzardo o una realtà già in atto? -**
***4.1 IA e indagini: un valido supporto per la ricerca della prova. - 4.2 IA e misure cautelari: giudizio prognostico ed esigenze cautelari. - 4.3 IA e fase decisoria: scenari di giustizia predittiva*. - 5. Conclusioni**

1. Il 21 maggio 2024 il Consiglio UE ha approvato all'unanimità il testo del Regolamento in materia di

Intelligenza Artificiale (di seguito IA), che lo scorso 13 marzo il Parlamento europeo aveva promosso con 523 voti favorevoli.

Per la prima volta nel panorama giuridico mondiale, la normativa si pone l'obiettivo di regolare la creazione, l'utilizzo e l'introduzione di sistemi e modelli di IA in diversi campi. In quanto regolamento, esso è destinato a essere automaticamente applicato in tutto il territorio dell'Unione, senza necessità di leggi di recepimento né possibilità di adattamento nei singoli ordinamenti nazionali.

In apertura si dichiara espressamente come l'intento sia quello di stabilire regole armonizzate sull'IA con conseguente modifica di regolamenti e direttive attualmente in vigore che subiranno un impatto per effetto delle nuove tecnologie. Giova notare, inoltre, che in tempi non sospetti e prima della vivace attenzione suscitata dal fenomeno IA, in data 3 dicembre 2018 la CEJEP aveva approvato la *Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi**[1]**. Questo dimostra la sensibilità dell'UE alla tematica, nonostante l'IA fosse un tema discusso dagli anni 50[2] del secolo scorso.

In genere, la legislazione sconta un evidente grado di ritardo rispetto alla tecnologia e alle sue rapide evoluzioni: al legislatore, con tutte le difficoltà e le insidie dell'elaborazione nonché dell'approvazione in sede parlamentare, non resta che raccogliere la sfida e cercare di ottenere un prodotto finale il più possibile completo e inclusivo.

L'*AI Act* si inscrive nell'ambito della legislazione digitale, nella quale figurano altre normative euro-unitarie precedenti, come il *Digital Markets Act* (DMA), il *Digital Services Act* (DSA),
il *Data Governance Act* (DGA) e il *Data Act*.

Il testo del Regolamento si presenta come un testo di non immediata e facile consultazione: composta da ben 458 pagine, 180 considerando, 113 articoli e 13 allegati, la normativa presenta un elevato livello di complessità anche per gli interpreti più allenati.

Il legislatore europeo si è confrontato con una tematica articolata e per molti versi incomprensibile persino per i tecnici della materia. Deve essergli deputato un grande sforzo, ma essa corre il rischio di diventare in breve tempo obsoleta, a causa della velocità impressionante con cui le tecniche di IA progrediscono. È sufficiente citare il caso della cd. IA generativa, nozione assente nella versione del testo normativo datata 14 giugno 2023, ora menzionata nei considerando nn. 99[3] e 105.

Tra le numerose modifiche apportate rispetto alla versione precedente è possibile notare l'eliminazione dell'art. 4 *bis*, dedicato ai principi generali. Invero, tali principi non sono stati del tutto rimossi dall'attuale testo, ma sono stati trasfusi nel Considerando n. 27 per come elaborati nel 2019 dall'*Artificial Intelligence High-Level Expert Group* (AI HLEG). Sulla efficacia cogente dei considerando posti in apertura di una normativa UE si discute[4]: essi vengono qualificati come atti di *soft law*, volti a esplicitare l'intento normativo del legislatore, ma non godono di una portata applicativa al pari delle disposizioni regolamentari.

Le norme del regolamento si concentrano sulla disciplina generale del fenomeno. L'UE guarda con favore alle nuove tecnologie. Per tutelare al meglio i propri cittadini ha scelto un approccio antropocentrico[5]. Data l'opportunità offerta dall'IA, coglierla è essenziale, seppur nel rispetto della dimensione umana. L'IA deve rimanere strumento, non assurgere ad attore principale e deve essere applicata al fine di migliorare e accelerare il soddisfacimento delle esigenze umane, senza comprimere la capacità di scelta e di autodeterminazione degli individui, né i loro diritti fondamentali.

Questo è probabilmente il significato più profondo dell'espressione utilizzata dal legislatore. Un'IA può dirsi "antropocentrica" e "affidabile", solo qualora ponga al centro gli interessi dell'uomo e consenta in qualunque momento di comprenderne il funzionamento e i risultati a cui è pervenuta. Gli utenti devono essere sempre al corrente di interagire con un macchina intelligente, gli sviluppatori e i produttori devono garantire il maggior grado di trasparenza possibile.

Tuttavia, uno dei maggiori problemi legati al mondo dell'IA è l'oscurità del suo funzionamento. In via estremamente semplificata, si può affermare che il modello di intelligenza artificiale cd. *forte**[6]* venga addestrato attraverso un numero incommensurabile di dati e informazioni (cd. *input*). In seguito, la macchina, sviluppata in base a un algoritmo, rielabora questi contenuti all'interno di un'immaginaria scatola nera (cd. *black box*) e all'esito emette dei prodotti finali (cd. *output*). Questi possono essere di varie tipologie, come testi, immagini, perfino contenuti multimediali e ciascun risultato è frutto di una combinazione innovativa e originale dei dati inseriti dallo sviluppatore e selezionati in base alla richiesta effettuata dal *deployer**[7]*.
Il segmento ancora ignoto si colloca all'interno della *black box*: neanche i tecnici sono in grado di descrivere esattamente cosa si verifichi al suo interno e come si giunga all'esito definitivo. Dunque, nonostante talune voci discordanti[8], il termine *intelligenza artificiale* risulta pertinente e adatto al caso. L'IA non è in grado di eguagliare la mente umana[9], poiché non è in grado di generare *output* senza aver avuto le adeguate nozioni di partenza, né risulta capace di riconoscere un'informazione falsa (*deep fake**[10]*) da una veritiera.

Una delle maggiori critiche mosse all'IA è quella di scontare dei *bias* cognitivi, dovuti alle informazioni che lo sviluppatore della tecnologia vi ha inserito. Nessun *output* può dirsi neutrale, ma esso è il risultato dei condizionamenti esterni, nonché dei limiti della conoscenza attuale di cui si è dato atto poc'anzi.

Da ciò, sorge un primo quesito, che nel prosieguo della trattazione verrà discusso: se si guarda al ragionamento umano, è possibile effettivamente spiegare come giunge a una decisione razionale? Possiamo affermare con assoluta certezza che in ogni circostanza chiunque assumerà la stessa decisione?[11] Ciascun essere umano è soggetto a influenze di vario tipo: la cultura, il paese di origine, la religione professata, gli studi intrapresi, gli incontri casuali, ecc. Anche innanzi a due situazioni analoghe e prendendo in considerazione una situazione di libera e volontaria autodeterminazione individuale, il medesimo soggetto potrebbe assumere decisioni differenti poiché ispirato diversamente o condizionato da una molteplicità di fattori concomitanti[12].

2. I sistema di IA sono notoriamente classificati sulla base del diverso livello di rischio che sono in grado di generare. La nozione di *rischio*[13] induce ad analizzare un'interazione tra due o più fattori, uno dei quali può subire una lesione o una messa in discussione.

Per apprezzare davvero una tecnologia di IA, occorre porla in connessione con attività umane già esistenti. Uno dei campi in grado di trarre i maggiori benefici dalla nuova *Techne* è la medicina. In ogni caso la presenza umana viene sempre mantenuta: nessun paziente è mai stato curato completamente ed esclusivamente da una macchina, ma sempre con la supervisione e l'interazione di un professionista, che ha la possibilità di intervenire in qualsiasi momento e di correggere eventuali errori di strategia o di valutazione compiuti dal sistema. *Mutatis mutandis*, è quanto disposto anche dal Regolamento in materia di protezione dei Dati personali n. 2016/679/UE. L'art. 22 par. 1 GDPR, recepito nell'ordinamento italiano all'art. 8 del d.lgs. 18 maggio 2018, n. 51, vieta l'assunzione di decisioni totalmente automatizzate, dunque il titolare dei dati ha diritto a che le sue informazioni personali, pur raccolte tramite *software* informatici, siano elaborate da una persona fisica.

Rispetto ai livelli di rischio, gli strumenti di IA sono notoriamente suddivisi in: sistemi a rischio assente o minimo, sistemi ad alto rischio e sistemi a rischio inaccettabile.

Nel primo caso, l'interazione uomo–macchina è lecita e anzi auspicata onde consentire
una riduzione delle tempistiche e un innalzamento del livello di precisione. Nel caso di settori a rischio cd.

inaccettabile, non è ammessa alcuna sperimentazione o interazione con l'IA, al fine di preservare valori e principi fondamentali e incomprimibili. L'art. 5 del regolamento individua le pratiche di IA vietate. Da un lato, la norma vieta "*l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di un sistema di IA per effettuare valutazioni del rischio relative a persone fisiche al fine di valutare o prevedere la probabilità che una persona commetta*
un reato, unicamente sulla base della profilazione di una persona o della valutazione dei tratti e delle caratteristiche della personalità", ma dall'altra esclude il divieto per *"i sistemi di IA utilizzati a sostegno della valutazione umana del coinvolgimento di una persona in un'attività criminosa, che si basa su fatti oggettivi e verificabili direttamente connessi a un'attività criminosa"***[14]**.

L'ambito più interessante, al contempo più delicato e di maggiore interesse, è rappresentato dai sistemi a rischio elevato. Non a caso è anche il campo in cui il regolamento si concentra con maggiore attenzione: vi è dedicato espressamente il Capo III, artt. 6-49. L'obiettivo è individuare il corretto equilibrio per evitare facili degenerazioni. Se questo viene centrato, ciò permette di sfruttare al meglio l'IA e di facilitare l'azione umana, aumentando prestazioni, qualità e ottimizzazione dei tempi. In caso contrario, si rischia la sostituzione dell'uomo con l'automazione.

Nel dettaglio, l'art. 6 dell'*AI Act* si occupa di definire i sistemi ad alto rischio. La norma è completata dall'elenco inserito nell'allegato III, tra cui figura – per quanto di interesse – l'amministrazione della giustizia.

L'art. 6 paragrafo 1 della bozza di regolamento qualifica un sistema di IA come ad alto rischio al verificarsi di due condizioni: il sistema di IA è un prodotto o una componente di sicurezza di
un prodotto, per come regolato dalla normativa di armonizzazione dell'Unione (lett. a);
tale prodotto o componente di sicurezza di IA è soggetta alla valutazione di terzi prima dell'immissione sul mercato in base alla normativa UE (lett. b). Modificando il testo precedente dell'art. 6, i redattori hanno aggiunto i paragrafi da 3 a 6. In particolare, il paragrafo 3 chiarisce quando un sistema non possa essere qualificato come ad alto rischio (lett. a-b-c-d).

Rimane tuttavia un sistema ad alto rischio qualora esso effettui una profilazione di persone fisiche (art. 3 par. 3 comma 2). Prima di immettere un sistema ad alto rischio sul mercato, il fornitore del servizio deve essere registrato a norma degli articoli 49 e 71 nella banca dati dell'UE costituita *ad hoc*.

Gli articoli 8 e 9 sono, poi, rispettivamente dedicati alla conformità ai requisiti e al sistema di gestione dei

rischi. La bozza di normativa sul punto si presenta sufficientemente dettagliata:
il legislatore ha previsto che la classificazione di un sistema di IA come ad alto rischio possa seguire diverse fasi, possa mutare nel corso del tempo e sia supervisionato costantemente.
In questa direzione si pone anche l'art. 14 dedicato alla sorveglianza umana: ogni sistema ad alto rischio viene supervisionato da non meno di due persone fisiche esperte, che siano in grado di intercettare i malfunzionamenti e di correggerli onde prevenire danni ulteriori.

Per quanto attiene al settore giudiziario, una lettura complessiva dell'*AI Act* rivela che in nessun caso il legislatore europeo ritiene possibile né auspicabile la sostituzione dei giudici con l'IA[15].

Quando l'All. III, par. 8, lett. a) menziona l'«amministrazione della giustizia», fa specifico riferimento all'attività giurisdizionale, all'uso che dell'IA può fare l'autorità giudiziaria nell'interpretare i fatti, le norme e nella ricerca delle prove. Occorre tuttavia evidenziare che tale espressione allude a un campo molto più vasto di quello strettamente e sinteticamente descritto e che, dunque, sembra non essere preso in considerazione dal legislatore europeo.
Bisogna comprendere se, la nozione non è specificata poiché non considerata tra le ipotesi ad alto rischio o perché oggetto di una traduzione nella lingua italiana eccessivamente sintetica o, infine, perché frutto di una dimenticanza legislativa.

È noto infatti che il settore giustizia comprende al suo interno anche un'attività di carattere più prettamente amministrativo. Tra le numerose attività, esso include, per esempio, l'organizzazione degli uffici giudiziari, la gestione del sistema carcerario, l'attività svolta dal personale a supporto dei magistrati, come cancellieri, segretari e, più di recente, addetti all'Ufficio per il processo.
Queste specifiche attività, pur fondamentali per rendere l'apparato più efficace ed efficiente[16]
si prestano a un connubio utile con i sistemi di IA, che potrebbero supportare il personale amministrativo al fine di rendere più celere la strutturazione della macchina giudiziaria. Benché non riguardi direttamente le modalità di svolgimento né i diritti esercitabili dalle parti in sede processuale, non può essere sottovalutata l'importanza di un'organizzazione capillare di questo tipo nel perseguimento degli obiettivi fissati dall'UE.

Se, però, con *amministrazione della giustizia* si vuole intendere *strictu sensu* l'attività giurisdizionale posta in essere da magistrati e professionisti del foro, occorre guardare
alle modalità con le quali l'IA può impattare sul procedimento probatorio e su quello decisionale.

La presente indagine non contempla le implicazioni di carattere sostanziale: se l'IA è destinata a penetrare nella vita di tutti i giorni, è necessario ripensare al tema della responsabilità civile del produttore, sviluppatore, e utilizzatore di IA[17], ma anche al profilo della responsabilità penale[18] dei soggetti coinvolti, se maggiormente assimilabile alla tipologia di responsabilità degli enti (cd. sistema 231) oppure alla generale responsabilità individuale (art. 27 comma 1 Cost.).

Di profili sostanziali è giunta a occuparsi anche la giurisprudenza nazionale: una sentenza del Consiglio di Stato prendeva in considerazione la valutazione del grado di affidabilità e precisione di un algoritmo per l'assunzione di decisioni in sede amministrativa. Nel caso di specie il Collegio si è occupato della distinzione tra algoritmo di prevenzione e algoritmo di trattamento, preoccupandosi anche di tracciare un confine tra la nozione di algoritmo e quella di intelligenza artificiale[19].

Questa pronuncia, per altro non più così recente, testimonia quanto l'IA pervada ormai la vita quotidiana e di quanto ai giudici sia richiesto di sviluppare una conoscenza minima per comprenderne il funzionamento e stabilire, caso per caso, se l'utilizzo abbia rispettato i parametri.

Appare opportuno menzionare anche di una recentissima pronuncia della Terza sezione penale della Corte di Cassazione, dalla quale risulta che nel proprio atto il ricorrente menzioni l'utilizzo della nota IA generativa ChatGPT come ulteriore elemento a sostegno della propria tesi[20], ma questo non ha potuto influenzare il giudizio di revisione attuato nella specifica sede.

La presente trattazione si sofferma, dunque, sull'area ad alto rischio definita dal regolamento.
Ci si chiede come l'IA possa integrarsi con la dinamica processuale e, in particolare, con la giustizia penale. Invero, settori come quello civile e soprattutto quello tributario, si prestano in modo più confacente all'introduzione dell'IA.

Si pensi a contenziosi seriali come quelli di diritto del lavoro o a controverse in materia fiscale: anche in questi casi la decisione giudiziale non può essere completamente automatizzata né sostituita dal *machine* o *deep learning*, ma in essi non si giunge a lambire quei diritti fondamentali, primo fra tutti la libertà personale, che una sanzione penale è in grado di comprimere.

Prima di analizzare le possibili combinazioni tra IA e giustizia penale tradizionale, occorre indagare quali siano le principali barriere poste dal sistema attuale.

3. Un'introduzione massiva e illimitata di sistemi di IA in settori ad alto rischio può compromettere in maniera decisiva i diritti fondamentali. Giova sottolineare che il legislatore ha affrontato il punto nel nuovissimo *AI Act.*

L'art. 27 del Regolamento si occupa della valutazione di impatto sui diritti fondamentali
per i sistemi di IA ad alto rischio. In particolare, il primo paragrafo della norma è il più articolato e impone ai *deployers* pubblici o privati di effettuare detta valutazione tenuto conto di diversi parametri, come la categoria di persone fisiche che utilizzeranno il sistema e per quanto tempo, nonché di stabilire quali misure adottare nel caso in cui i rischi si concretizzino.
La valutazione deve essere notificata all'autorità di vigilanza (paragrafo 3) e l'Ufficio per l'IA elabora un questionario semplificato per velocizzare il procedimento valutativo dei *deployers* (paragrafo 5). Risulta, poi, interessante il testo del paragrafo 4 che rinvia a due delle normative attualmente vigenti da considerare in materia di protezione dei diritti fondamentali.
La norma menziona l'art. 35 del Regolamento (UE) 2016/679 e l'art. 27 della direttiva (UE) 2016/680. Entrambe le norme sono rubricate "*Valutazione di impatto sulla protezione dei dati personali*", la prima in relazione alla disciplina generale in materia di protezione dei dati personali. La direttiva (UE) 2016/680 si occupa nel dettaglio della protezione dei dati personali delle persone fisiche nell'ambito dell'attività investigativa e di applicazione delle sanzioni penali.

Nel contesto attuale, i cd. *Big Data* costituiscono il "nuovo petrolio" specie per le grandi aziende internazionali che scambiano i dati degli utenti al fine di trarne profitto[21]. L'approccio europeo, volto alla protezione dei diritti dei propri cittadini, ha optato sin dal 2016 per una riforma della materia con l'ormai noto GDPR. Tale regolamento ha abrogato e sostituito la precedente direttiva 95/46/CE e ha innovato il Codice della *privacy* d.lgs. 30 giugno 2003, n. 196.

La protezione dei dati di carattere personale deriva dal diritto della riservatezza.
A lungo i termini "riservatezza" e "*privacy*" sono stati utilizzati come sinonimi, sebbene presentino delle peculiarità specifiche.

Come ha avuto modo di osservare la più autorevole dottrina[22], la riservatezza non è direttamente

menzionata dal codice civile italiano e, per lungo tempo, è stata ritenuta immeritevole di tutela. Invero, il fondamento di tale diritto è rinvenibile nell'art. 2 Cost., norma diretta a garantire che la personalità dell'individuo si sviluppi libera e priva da condizionamenti in ogni contesto sociale in cui è l'individuo sia inserito. Sul piano sovranazionale, l'art. 8 C.e.d.u. tutela il rispetto della vita privata e familiare. Per l'epoca storica in cui essa fu redatta, i riferimenti ai dati personali e all'utilizzo delle tecnologie risultano assenti. La norma prescrive che eventuali limitazioni alla dimensione personale e familiare del soggetto possono avvenire solo per il tramite della pubblica autorità e per motivi di interesse pubblico superiore.

Dunque, quando si parla di "riservatezza", si allude e due piani: da un lato alla dimensione familiare e domestica della persona fisica; dall'altro al controllo relativo alla circolazione delle informazioni personali. In questa seconda accezione la riservatezza si distingue dal diritto all'identità personale. Quest'ultimo assicura la fedele rappresentazione alla propria proiezione sociale, la riservatezza, invece, garantisce la non diffusione all'esterno delle proprie vicende personali non aventi per i terzi un interesse socialmente apprezzabile.

Per quanto attiene al contesto euro-unitario, merita una speciale menzione la Carta UE del 2000. Come noto, la disciplina sancisce una vasta gamma di diritti fondamentali, espressione della cultura giuridica dell'ultimo secolo e avente, dal 2007, lo stesso valore giuridico dei trattati.
La Carta prende in considerazioni i mutamenti sociali, etici e tecnologici susseguitesi.
In particolare, l'art. 7 tutela il rispetto della vita privata e familiare, descrivendo dunque il primo profilo del diritto alla riservatezza poc'anzi ricordato. L'art. 8, invece, sancisce il diritto alla protezione dei dati di carattere personale, prendendo in considerazione dunque la seconda accezione del menzionato diritto. Il secondo comma della disposizione impone che i dati siano trattati in base al principio di lealtà, per finalità determinate e con il consenso della persona fisica.

Alla riservatezza, il legislatore della riforma in materia di IA dedica l'art. 78, così rubricato.
In particolare il secondo paragrafo dispone che: "*le autorità* [...] *richiedono solo i dati strettamente necessari per la valutazione del rischio posto dai sistemi di IA e per l'esercizio dei loro poteri conformemente al presente regolamento e al regolamento (UE) 2019/1020.*
Esse pongono in essere misure di cibersicurezza adeguate ed efficaci per proteggere la sicurezza e la riservatezza delle informazioni e dei dati ottenuti e cancellano i dati raccolti non appena non siano più necessari per lo scopo per il quale sono stati ottenuti, conformemente al diritto dell'Unione o nazionale applicabile".

Al titolare è, dunque, garantito il diritto a immettere in circolazione i propri dati personali in modo veritiero

per finalità conosciute e consapevolmente accettate. Lo stesso gode del diritto di controllare, rettificare e cancellare i propri dati: si delinea dunque un duplice sistema di tutela, che comprende sia la dimensione interna di divulgazione delle informazioni di carattere personale, quanto quella esterna, dunque la protezione da incursioni altrui circa l'utilizzazione, la diffusione e la distorsione delle medesime.

Appare evidente quanto l'IA possa mettere a repentaglio questo diritto fondamentale.
Ne era consapevole la CEPEJ sin dall'adozione della *Carta etica europea*. Essa menziona cinque principi[23] di *soft law*, che mirano a un utilizzo omogeneo e rispettoso dell'IA nel settore giurisdizionale.

Se dunque la riservatezza e la tutela dei dati sono i beni immateriali maggiormente in pericolo sul piano sostanziale, spostandoci sul piano processuale vengono messi a repentaglio altri diritti fondamentali del soggetto sottoposto a indagini e, poi, a processo.

L'art. 6 C.e.d.u. sancisce il rispetto del *due process of law*. Tale principio contempla il diritto a un equo processo[24], il diritto al contraddittorio nella formazione della prova, il diritto alla parità delle armi, il diritto a un giudice terzo e imparziale. Gli stessi, recepiti all'art. 111 Cost.
con la l. cost. n. 23 novembre 1999 n. 2, devono essere letti in combinato disposto
con gli artt. 24 comma 2 e 27 comma 2 Cost., relativi al diritto inviolabile di difesa e
alla presunzione di innocenza.

Un utilizzo indiscriminato di tecnologie di IA potrebbe infrangere in pochissimo tempo
il percorso storico-giuridico che ha condotto all'odierno assetto giurisdizionale, espressione di una cultura laica, libera e democratica. Come ha avuto modo di osservare la migliore dottrina[25] , la violazione delle garanzie procedurali imposte dal menzionato art. 6 C.e.d.u. può compromettere la legalità della prova e, di conseguenza, la decisione. Si afferma che:
"*So far, we must stick to the general conclusion that a violation of a guarantee enshrined in the Convention does not provoke, as a general consequence a violation of art. 6 if its results are used as evidence in criminal proceedings. However, in the case-by-case approach of the Court, violations of art. 3 almost always end up in a breach of art. 6, due to the need to deny a legal shield to evidence obtained from torture, inhuman or degrading treatment****[26]*** […]".

Ad ogni modo, ignorare il fenomeno IA e lasciare il sistema giudiziario escluso dall'impiego di questi strumenti dimostrerebbe cecità, ancorando la giustizia al passato innanzi a una realtà che progredisce a

velocità inarrestabile. Occorre sfruttare al meglio le potenzialità dei sistemi di IA e, al contempo, proteggere i diritti individuali.

4. Nel sistema penale, nonostante i diffusi sentimenti di diffidenza, si registrano le prime applicazioni dell'IA all'interno del processo.

Come è stato acutamente affermato, "*per ridimensionare o almeno ridurre al minimo l'impatto negativo sull'esercizio della giurisdizione penale dei* biases *cognitivi, l'ordinamento giuridico appresta una fitta rete di regole epistemologiche e di legalità, sia del procedere che*
del ragionamento probatorio, mirate al controllo del buon funzionamento e dell'efficacia di quel giudizio. Esse si ispirano innanzitutto a meta-valori costituzionali che, a fronte delle difficoltà pratiche di ricostruzione del fatto e della strutturale incertezza del giudizio, disciplinano
il «giusto processo»"[27]

Quasi nessuna fase processuale è rimasta immune al fenomeno IA, fatta eccezione per la fase decisoria, nella quale, a ragion veduta, si pongono i maggiori interrogativi. Nel contesto europeo a differenza di altre realtà, prima fra tutte quella cinese, sostituire i giudici con macchine o *robot* intelligenti non è mai stata un'opzione. L'unica modalità di interazione rimane uno *standard* di collaborazione debole (*weak*) senza che la macchina possa minimamente soppiantare l'operato giurisdizionale.

Si inizia però a valutare la possibilità di usufruire delle potenzialità offerte dai sistemi computazioni per accelerare i tempi della giustizia e, a determinate condizioni, avere un più elevato grado di precisione, tenendo altresì conto di limiti e *bias* attualmente rimasti irrisolti.

4.1 Come noto la fase investigativa prende avvio dalla notizia di reato. Ormai da tempo,
le indagini condotte dal Pubblico Ministero incaricato sono governate dalla prova scientifica:
la raccolta di prove con l'uso di tecniche specialistiche, come il test del DNA o le analisi informatiche, costituiscono il principale strumento di accertamento di un fatto di reato.

I mezzi di ricerca della prova, tipici della fase investigativa, sono utilizzati per raccogliere elementi sufficienti a formulare *una ragionevole previsione di condanna*[28], mentre i mezzi di prova si formano in dibattimento nel rispetto del principio del contraddittorio *nella* formazione della prova (art. 111 comma 4 Cost.), il cui prototipo è rappresentato dalla testimonianza.

Dal canto suo, la prova scientifica si colloca nell'ambito delle prove atipiche (art. 189 c.p.p.), che il giudice può ammettere senza particolari impedimenti, purché esse siano idonee e prive di elementi che possano condizionare la libertà morale dell'individuo (art. 220 comma 2 c.p.p.).

Nel libro III del codice di procedura penale è prevista un altro istituto che consentirebbe l'accesso all'IA sul piano probatorio[29]: il Titolo I, Capo V è dedicato agli esperimenti giudiziali, ovvero alla riproduzione in sede processuale di quanto avvenuto nella realtà materiale. Questo strumento può essere veicolo di utilizzo di un modello computazionale per la valutazione concreta dell'andamento dei fatti. L'immissione nel processo dell'esperimento giudiziale avviene tramite provvedimento motivato del giudice che: "*dà le opportune disposizioni affinché esso si svolga in modo da non offendere sentimenti di coscienza e da non esporre a pericolo l'incolumità delle persone o la sicurezza pubblica*" (art. 219 comma 4 c.p.p.).

Una volta raccolti e documentati con apposito verbale i risultati della prova scientifica, essi vengono successivamente valutati dal giudice, in base a quelli che con una sentenza del 1993 della Corte Suprema degli Stati Uniti sono passati alla storia come criteri *Daubert*.

In Italia, con la sentenza *Cozzini* del 17 settembre 2010, n. 43786, la Quarta sezione penale della Corte di Cassazione ha individuato le regole per la valutazione della prova scientifica, onde garantire il passaggio dalla probabilità statistica alla probabilità logica al fine di condannare l'imputato *al di là di ogni ragionevole dubbio* (art. 533 c.p.p.). Nonostante il ruolo di *peritus peritorum* del giudice, egli deve confrontarsi con la legge scientifica e non ha la possibilità di aderire a proprio piacimento all'una o all'altra teoria. La sentenza Cozzini si è occupa di fissare una serie di parametri che il giudice deve osservare per selezionare la tesi scientifica che meglio si adatti al caso concreto: l'attendibilità degli esperti che hanno condotto lo studio, nonché la loro autorevolezza, indipendenza e integrità, l'elevato grado di consenso riscosso dalla ricerca, la sua ampiezza, il suo rigore e la sua oggettività.

Gli indizi e le fonti di prova raccolti con IA figurano nel campo della prova scientifica.
Per esempio, l'IA può essere un valido supporto per l'identificazione di un soggetto, attraverso una Tecnologia di Riconoscimento Facciale (TFR)[30]. Questo genere di strumenti è ormai molto diffuso non solo nella vita quotidiana, ma anche nelle attività tipiche di polizia giudiziaria.
Uno degli *automated facial recognition system**[31]* più noti è SARI, in uso dal 2017 presso la Procura della Repubblica di Milano e poi acquisito su tutto il territorio nazionale.
La P.G. utilizza anche altri tipi di *software* a base algoritmica in specifici contesti criminali[32] o per altre

finalità[33].

Nonostante il terreno investigativo sia il più proficuo per l'interazione uomo–macchina, non possono essere taciuti i rischi potenziali. Limitandoci all'esempio delle TFR, il principale pericolo attiene all'attendibilità dei sistemi di riconoscimento[34], che possono commettere errori sia a causa di fattori esogeni, come la scarsa qualità dell'immagine, tanto endogeni, come l'inidoneo allenamento ai dati. Ulteriore problematica riguarda lo scarso livello di trasparenza di questi sistemi a base algoritmica, poiché solo l'azienda privata che ha creato il *software*, normalmente oggetto di brevetto, conosce il suo effettivo funzionamento. Ancora più di frequente però nemmeno ingegneri e sviluppatori sono in grado di spiegare cosa si verifichi all'interno della *black box*, elemento che porterebbe dei seri problemi di attendibilità in caso di una loro eventuale testimonianza in dibattimento.

Pericoli più specifici attengono alla violazione del diritto alla *privacy*, nella duplice accezione declinata agli artt. 7-8 della Carta UE, ma anche dall'art. 10 dir. 2016/680/UE relativo al trattamento di determinate categorie di dati. Occorre osservare, inoltre, che sulla materia manca una legislazione nazionale, affidata al momento a una regolamentazione ministeriale[35]: in sede processuale la raccolta del materiale probatorio deve essere valutata in base alla disciplina generale delle invalidità, in particolar modo dell'inutilizzabilità e, nei casi compatibili, della nullità.

La scienza informatica utilizza le espressioni *data mining* e *data profiling*.
La distinzione tra le due è sottile e a tratti difficile da individuare. Il *data mining* può essere considerato come la raccolta delle informazioni, mentre il *data profiling* come l'attività di profilazione dei dati. Quest'ultima operazione è foriera di maggiori criticità per i diritti individuali, tra cui il diritto all'oblio, il diritto all'equo processo, il principio di non colpevolezza e il principio di parità delle armi. Infatti, se è noto che queste strumentazioni sono in dotazione all'investigazione pubblica, dovrebbero essere parimenti accessibili alla classe forense, al fine di porre le investigazioni difensive su un piano il più possibile analogo.

4.2 Sebbene utilizzare un algoritmo a fini prognostici sia considerato altamente pericoloso per la libertà personale, non bisogna ignorare che il sistema penale è congeniato in modo tale per cui al giudice è richiesto di compiere una valutazione di rischio in un momento spesso molto lontano dalla dichiarazione definitiva di responsabilità dell'imputato.

Infatti, l'indagine sulla sussistenza dei gravi indizi di colpevolezza (art. 273 comma 1 c.p.p.) per l'applicazione di una misura cautelare, non è altro che un giudizio prognostico[36] compiuto dal giudice, nella maggior parte delle ipotesi, nella fase investigativa. La richiesta del P.M. deve essere corroborata da tali elementi e deve recare con sé la prova di una delle esigenze cautelari previste dall'art. 274 c.p.p. Si tratta di prognosi che solo parzialmente coincide con la successiva valutazione di responsabilità dell'indagato, ma che è priva delle caratteristiche della prova dibattimentale.

Specie quando viene richiesta l'applicazione di una misura cautelare personale di tipo custodiale, emerge con tutta evidenza il sacrificio imposto alla libertà individuale, tanto è vero che la legge fissa dei criteri ben definiti per l'applicazione delle restrizioni, in base al tipo di reato per cui si procede e dettando specifici limiti temporali sia di fase che complessivi per la durata massima della misura. Nella pratica giudiziale, si assiste sovente all'utilizzo di automatismi, raramente in grado di resistere alle critiche. Per decenni si è cercato un valido strumento di supporto
per il giudice e l'IA potrebbe concretamente aiutare in questo ambito. Per ciascuna delle specifiche esigenze cautelari imposte dal sistema penale per l'applicazione di misure cautelari,
è possibile addestrare l'algoritmo con le informazioni necessarie ad assumere la decisione.
Come più volte ribadito, "*una cosa è utilizzare l'IA per aiutare i giudici, ben altra è affidare alla macchina la decisione sulla libertà o la reclusione delle persone*[37]". Deve, infatti, essere rifuggita qualsiasi valutazione personalistica dell'individuo, che trasformi il sistema in un diritto penale d'autore, in luogo di un diritto penale del caso concreto.

Ad esempio, per calcolare il rischio di reiterazione del reato, in alcuni Stati della Federazione americana viene impiegato l'ormai notissimo algoritmo COMPAS, noto ai più per il caso *State of Winsconsin vs Loomis*. In quell'occasione, l'algoritmo fu applicato in sede di condanna definitiva per valutare il tasso di recidiva dell'imputato, ma non mancano sue applicazioni anche in via preventiva. Gli sviluppatori di COMPAS hanno a lungo rifiutato di svelare il suo contenuto, trincerandosi dietro i diritti di *copyright*. Ciò che è noto, è che COMPAS compatta insieme informazioni di diversa natura, frutto delle informazioni statistiche raccolte tra i detenuti. L'algoritmo identifica il soggetto in base a 137 *items*, come il livello di studi, il consumo di alcol o sostanze, ecc. Il caso Loomis ha evidenziato i limiti del sistema, affetto fortemente da razzismo, poiché generava una percentuale del tasso di recidiva più elevata in caso di individui afro-americani rispetto a individui bianchi.

Con lo stesso criterio, il sistema può essere parimenti addestrato a calcolare la percentuale di rischio relativa al pericolo di fuga o quella relativa al possibile inquinamento probatorio.

Ad ogni modo, sistemi come COMPAS sono destinati a stabilizzarsi, ma è necessario correggere i pregiudizi da cui sono influenzati. Per farlo occorre nutrire il programma con dati il più possibile neutri e non sintomatici del pensiero dello sviluppatore. Bisogna altresì conoscere
il loro funzionamento intrinseco per non compromettere irrimediabilmente il diritto di difesa e per renderli un valido supporto per il giudizio prognostico del giudice. È, infatti, indispensabile tenere sotto controllo l'applicazione delle misure cautelari per prevenire ingiustificati automatismi ed evitare successivi processi di risarcimento del danno per ingiusta detenzione.

Algoritmi predittivi del tasso di recidiva di un indagato possono costituire solo uno dei fattori presi in considerazione dal giudice per l'applicazione della sanzione cautelare, dal momento che il sistema fornisce un dato del tutto sintetico, mentre l'ordinanza con cui viene comminata
la misura poggia necessariamente sulla motivazione.

La motivazione di un provvedimento restrittivo della libertà personale non può essere meramente tautologica, né limitarsi a riportare un dato percentuale, ma deve contenere solide argomentazioni logico-giuridiche ed elementi gravi, precisi e concordanti circa la colpevolezza del soggetto.

4.3 L'ambito più discusso per l'introduzione dell'IA nel processo penale attiene sicuramente alla fase conclusiva e dunque alla decisione di condanna, assoluzione o proscioglimento dell'imputato[38].

In primo luogo, occorre salvaguardare il ruolo istituzionale del giudice e la sua indipendenza innanzi alle capacità superiori dell'IA: ammettendo, infatti, che la tecnologia in questione goda di un livello di precisione superiore, irraggiungibile per la mente umana, si sottomette
il giudicante alla macchina senza possibilità di rettifica o di smentita. Come è stato autorevolmente osservato, se portato alle estreme conseguenze, questo renderebbe vano
il sistema delle impugnazioni, poiché l'unico giudice potrebbe essere un algoritmo potenziato rispetto a quello utilizzato per la decisione di primo grado. Questo condurrebbe a domandarsi perché lo stesso *software* non sia stato utilizzato sin dal principio per evitare un inutile aggravio di tempo e di denaro per il sistema giudiziario[39].

Un primo aspetto che l'IA può migliorare riguarda la ricerca dei precedenti giurisprudenziali, non solo di legittimità, ma anche dei gradi di merito. Da tempo, sono in fase di sperimentazione progetti per la realizzazione di banche dati relative a pronunce di merito dei vari distretti di Corte d'Appello, ma risulta

assente un programma uniforme su scala nazionale che sia basato sul medesimo *software*. La più nota piattaforma realizzata dal Centro Elettronico di Documentazione (C.E.D.) della Corte di Cassazione è *ItalgiureWeb*: una notevole raccolta di precedenti della Suprema Corte, i più rilevanti dei quali massimati da parte dell'apposito Ufficio del Massimario e del Ruolo. *ItalgiureWeb* è messa a disposizione gratuitamente per magistrati e personale amministrativo, ma richiede un abbonamento per la classe forense e gli studiosi. Per trovare precedenti utili, occorre utilizzare i cd. indici *booleani* all'interno della maschera di ricerca. Benché si tratti di un metodo sufficientemente semplice, una banca dati progettata con
un algoritmo potrebbe rendere la ricerca ancora più rapida e intuitiva, abbreviando notevolmente i tempi.

Negli Stati Uniti, infatti, sono da tempo in uso algoritmi che funzionano in base a dati statistici raccolti nelle ricerche precedenti e che supportano i giudici nella decisione.
Uno di essi è ALIBI[40]: un algoritmo in grado di predire il futuro comportamento degli indagati.

In sede penale, la pronuncia di condanna può pervenire solo *al di là di oltre ragionevole dubbio*: un'ipotesi motivazionale della sentenza può essere fornita al giudice tramite una tecnologia di IA, che individui ed elabori precedenti conformi. L'interprete cerca la soluzione più coerente dal punto di vista epistemologico, ma il diritto è una scienza umana e dunque non può raggiungere quel grado di certezza e di ripetibilità all'infinito, tipici delle scienze naturali.

Innanzi all'idea di sostituire i giudici con l'IA, molti paventano un attacco diretto alla democrazia con rischi di sottomissione all'automazione. Non è necessario arrivare a tanto. Occorre piuttosto pensare di riformare la professione giudiziaria dall'interno, adattandola ai tempi odierni, sfruttando al meglio le potenzialità offerte dalla tecnologia senza lasciarsi dominare da essa.

Quando redige un provvedimento, la porzione più importante che il giudice prepara è
la motivazione. È solo attraverso l'argomentare logico-giuridico che la decisione diviene valutabile, comprensibile a chi non ha preso parte al processo ed eventualmente riformabile in sede di impugnazione. È fuor di dubbio che solo l'interprete possa scriverla, poiché così ne assume la responsabilità giuridica e professionale.

Se un'IA coadiuvasse il giudice nella redazione della motivazione, non vi sarebbero rischi di degenerazione del sistema. Del resto, è quanto avviene attualmente in moltissimi (se non tutti gli) uffici giudiziari, dove il personale a supporto spesso prepara le bozze di decisione

per i contenzioni seriali o per i casi più semplici. In ogni caso, il magistrato incaricato ha l'onere di controllare, correggere e implementare quella proposta di decisione, poiché sua è la firma sulla versione finale della sentenza.

Emerge con chiarezza dunque che l'IA sarebbe in grado di migliorare notevolmente il dato quantitativo del sistema giudiziario: nessun essere umano potrebbe preparare una bozza di provvedimento alla stessa velocità della macchina intelligente e dunque questo potrebbe contribuire ad abbattere del 25% il *disposition time*[41] nel settore penale entro giugno 2026 come stabilito dall'UE. Il P.N.R.R. impone altresì di rafforzare la giustizia anche sul piano qualitativo. Quest'aspetto deve essere curato e raggiunto attraverso una serie di rimedi che agiscano su più fronti: occorre selezionare più rigidamente i futuri magistrati e predisporre dei programmi di aggiornamento costanti che comprendano anche l'informatica giuridica e l'uso delle moderne tecnologie computazionali. Anche da questo punto di vista l'IA può accelerare la crescita:
se il giudice deve limitarsi a limare una bozza di provvedimento seriale, può dedicare più tempo alla cura dei dettagli linguistici, tecnico-giuridici, poiché lo scheletro della sentenza è già a sua disposizione.

5. Volendo muovere delle preliminari considerazioni sull'*AI Act*, è possibile notare profili positivi quanto negativi.

L'UE è stata la prima istituzione a tentare l'individuazione di una regolazione, laddove paesi come gli Stati Uniti o la Cina, in cui l'avanzamento tecnologico e l'implementazione dell'IA in diversi ambiti del vivere sociale è assai più progredito rispetto al contesto europeo, sono ancora lontani dal dotarsi di un *corpus* normativo in materia. Bisognerebbe addirittura domandarsi se l'assenza di disciplina in questi ordinamenti non riveli una specifica scelta, per evitare di prendere posizione su tematiche politicamente ostiche, che vengono lasciate al legislatore del futuro.

L'IA è destinata a fare il suo ingresso nella vita dei cittadini 4.0, innovando il mondo del lavoro, il tempo libero, la vita domestica, le modalità di trasporto. Allo stato attuale, manca ancora
una legislazione di dettaglio che disciplini l'impiego dell'IA nei diversi campi, ma è apparso primario individuare una disciplina generale in grado di fornire limiti e coordinate per il corretto utilizzo di questo straordinario strumento.

Tuttavia, si potrebbe affermare che legiferare sull'IA sia come "tentare di afferrare
il vento": il testo rischia di invecchiare precocemente innanzi alle innovazioni che gli sviluppatori di IA sono in

grado di raggiungere in pochissimo tempo. L'approvazione del Regolamento è stata una vera e propria lotta contro il tempo per licenziare il testo in via definitiva prima delle elezioni europee di giugno 2024 e, dunque, del termine della IX legislatura. In ogni caso, le norme entreranno in vigore gradualmente e, per una loro applicazione completa, si dovranno attendere ancora due anni. In questo arco temporale, l'IA potrebbe mutare ancora rispetto a quel (poco) che conosciamo con conseguente vetustà delle norme approvate.

I sistemi intelligenti sono in grado di migliorare il settore penale, individuando la giusta dosimetria tra efficienza, qualità e rispetto dei diritti.

Dal punto di vista amministrativo, l'IA può essere uno strumento utilissimo per il personale degli uffici giudiziari al fine di smistare fascicoli, comporre i ruoli di udienza e individuare i precedenti conformi. Vero è che quest'attività non può rientrare nella giustizia vera e propria e, come tale non rientra nemmeno nelle attività ad alto rischio. Infatti, in base all'art. 6 par. 3 lett. d) dell'*AI Act* un sistema non è considerato ad alto rischio quando svolge *un compito preparatorio per la valutazione pertinente*.

Da questa preliminare disamina, si è cercato di dimostrare che ogni fase del processo penale è compatibile con i modelli computazionali, nel rispetto delle garanzie costituzionali e delle finalità tipiche della giustizia. Se i mezzi di ricerca della prova venissero rafforzati dalla tecnologia, questo consentirebbe di ridurre i tempi e la dispersione delle fonti, ma in ogni caso rimarrebbero liberamente valutabili dal giudice in base ai criteri logico–giuridici attualmente applicati.
Così il giudizio prognostico sul grado di pericolosità per l'applicazione di una misura cautelare, può essere corroborato da un algoritmo, basato su indici oggettivi e non su valutazioni peritali parcellizzate e dirette a giudicare unicamente la personalità del soggetto.

Infine, il terreno più scivoloso rimane quello della decisione giudiziale, innanzi alla quale si dipanano le maggiori perplessità per l'uso dei modelli computazionali. Esponenti illustri della dottrina e della giurisprudenza ritengono che solo la mente umana possa decidere sul singolo caso, specie in presenza del processo penale che può compromettere la libertà individuale e applicare una pena quale estrema sanzione comminata dall'ordinamento.
I giudici penali si attengono a rigidi parametri interpretativi per emettere la sentenza: valutazione del materiale probatorio, rispetto delle garanzie processuali, osservanza dei diritti e delle prerogative dell'imputato e delle altre parti.

Eppure, è possibile affermare con assoluta certezza, in modo razionale, ripetibile all'infinito, calcolabile *ex ante* alla stregua di un dato matematico, quale sarà la decisione giudiziale?
Esiste innegabilmente una fase sconosciuta del procedimento intellettivo del giudicante, che si concreta nel momento creativo di stesura della motivazione. Questa oscurità appare a tratti confrontabile con quella della *black box* algoritmica, nella quale non è noto come si addivenga agli *output* finali.

Con ciò non si intende suggerire di soppiantare *in toto* i giudici con i sistemi di IA: in ossequio alla legislazione attualmente in vigore, è vietata qualsiasi decisione fondata esclusivamente sull'automazione (art. 22 par. 1 GDPR, art. 11 dir. 2016/680/UE), ma è sempre richiesta
una rielaborazione da parte della persona fisica[42].

I presupposti per l'implementazione dell'IA nel settore penale ci sono, ma occorre individuare un giusto punto di caduta, rifuggendo tanto da tesi di applicazione illimitata tanto da teorie post-apocalittiche di governo delle macchine.

Giova concludere utilizzando le parole dello stesso legislatore europeo, che al Considerando
n. 42 dell'*AI Act,* così si esprime: *"In linea con la presunzione di innocenza, le persone fisiche nell'Unione dovrebbero sempre essere giudicate in base al loro comportamento effettivo.*
Le persone fisiche non dovrebbero mai essere giudicate sulla base di un comportamento previsto dall'IA basato unicamente sulla profilazione, sui tratti della personalità o su caratteristiche quali la cittadinanza, il luogo di nascita, il luogo di residenza, il numero di figli, il livello di indebitamento o il tipo di automobile, senza che vi 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. [...]*".*

---

[1] QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta Etica Europea, gli spunti per un'urgente discussione tra scienze penali e informatiche,* in rivista Legislazione Penale, ISSN 2421-552X, https://www.lalegislazionepenale.eu/intelligenza-artificiale-e-giustizia-nella-cornice-della-carta-etica-europea-gli-spunti-per-unurgente-discussione-tra-scienze-penali-e-informatiche-serena-quattrocolo/, 22 marzo 2018.

[2] Il padre teorico dell'IA è considerato John McCarthy, informatico statunitense, che in un saggio pubblicato nel 1956 coniò per la prima volta il termine "*Artificial Intelligence*", qualificandola come "*the science and*

engineering of making intelligent machines".

[3]https://www.europarl.europa.eu/news/it/press-room/20240308IPR19015/il-parlamento-europeo-approva-la-legge-sull-intelligenza-artificiale .

[4] KLIMAS, VAICIUKAITE, *The Law of Recitals in European Community Legislation*, in ILSA Journal of Int. & Comparative Law, 2008, 15, 63, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1159604 .

[5] L'art. 1 par. 1 del regolamento recita: "*Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di intelligenza artificiale (sistemi di IA) nell'Unione nonché promuovere l'innovazione*".

[6] CANZIO, *Intelligenza artificiale e processo penale,* in CANZIO – LUPARIA DI DONATI (a cura di), *Prova scientifica e processo penale,* II edizione, Wolters Kluwer, CEDAM, pag. 903.

[7] Definizione prevista all'art. 3 par. 1 n. 4 *AI Act*.

[8] ZENO-ZENCOVICH, *Artificial intelligence, natural stupidity and other legal idiocies*, in rivista Media Laws, ISSN 2532-9146, https://www.medialaws.eu/rivista/artificial-intelligence-natural-stupidity-and-other-legal-idiocies/ 28 marzo 2024.

[9] BALSAMO, *L'impatto dell'intelligenza artificiale nel settore della giustizia,* in rivista Sistema penale, ISSN 2704-8098, 22 maggio 2024, https://www.sistemapenale.it/it/articolo/balsamo-limpatto-dellintelligenza-artificiale-nel-settore-della-giustizia

[10] Definizione art. 3 n. 60 *AI Act*.

[11] QUATTROCOLO, *Per un'intelligenza artificiale utile al giudizio penale,* rivista BioDiritto, ISSN 2284-4503, n.

2/2021, https://teseo.unitn.it/biolaw/article/view/1674.

[12] FORZA – MENEGON – RUMIATI, *Il giudice emotivo. La decisione tra ragione ed emozione*, Bologna, 2017.

[13] Definizione art. 3 n. 65 *AI Act*.

[14] CAMERA, *A proposito dell'indagine conoscitiva sull'impatto dell'intelligenza artificiale nel settore della giustizia*, in rivista Sistema Penale, ISSN 2704-8098, https://sistemapenale.it/it/documenti/camera-indagine-conoscitiva-sullimpatto-dellintelligenza-artificiale-nel-settore-della-giustizia , marzo 2024, pag. 9.

[15] CAMERA, op. cit., pag. 5.

[16] Come richiesto dagli obiettivi fissati dalla stessa Unione europea con il Piano Nazionale di Ripresa e Resilienza (PNRR). Per maggiori dettagli, è consultabile il portale del Ministero della Giustizia: https://www.giustizia.it/giustizia/page/it/attuazione_misure_pnrr.

[17] DI DONNA, *Intelligenza artificiale e rimedi risarcitori,* CEDAM editore, settembre 2022. ALPA e altri (a cura di), *Diritto e intelligenza artificiale. Profili generali – Soggetti – Contratti – Responsabilità civile – Diritto bancario e finanziario – Processo civile,* Pacini Giuridica, Pisa, 2020.

[18] FRAGASSO, *La responsabilità penale del produttore di sistemi di intelligenza artificiale*, in rivista online Diritto Penale Contemporaneo, ISSN 2240-7618 volume 1/2023, https://dpc-rivista trimestrale.criminaljusticenetwork.eu/pdf/DPC%20Riv_Trim_1_23_fragasso.pdf.

[19] Consiglio di Stato, sez. III, sentenza 25 novembre 2021, n. 7891, Punto 9.1 *"La nozione, quando è applicata a sistemi tecnologici, è ineludibilmente collegata al concetto di automazione ossia a sistemi di azione e controllo idonei a ridurre l'intervento umano. Il grado e la frequenza dell'intervento umano dipendono dalla complessità e dall'accuratezza dell'algoritmo che la macchina è chiamata a processare. Cosa diversa è l'intelligenza artificiale. In questo caso l'algoritmo contempla meccanismi di machine learning e crea un sistema che non si limita solo ad applicare le regole software e i parametri preimpostati (come fa invece l'algoritmo "tradizionale") ma, al contrario, elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni,*

secondo un processo di apprendimento automatico".

[20] Corte di Cassazione, sez. III pen., sentenza 15 aprile 2024, n. 14631.

[21] FOGLIA, *Identità digitale, trattamento dei dati e tutela della persona,* in Rassegna di Diritto Civile diretta da P. Perlingeri, ISSN 0393-182X, Edizioni Scientifiche Italiane, 1/2021.

[22] ALPA – RESTA (a cura di), *Le persone fisiche e i diritti della personalità*, UTET Giuridica, 2019, cap. III, pag. 97.

[23] "*I principi richiamati dalla Carta Etica europea per l'uso dell'IA sono: questione sono i seguenti: 1) rispetto dei diritti fondamentali: assicurare l'elaborazione e l'attuazione di strumenti e servizi di intelligenza artificiale compatibili con i diritti fondamentali; 2) non discriminazione: prevenire specificamente lo sviluppo e l'intensificazione di discriminazioni tra persone o gruppi di persone; 3) qualità e sicurezza: in ordine al trattamento di decisioni e dati giudiziari, utilizzare fonti certificate e dati intangibili con modelli elaborati multi-disciplinarmente in un ambiente tecnologico sicuro; 4) trasparenza, imparzialità ed equità: rendere le metodologie di trattamento dei dati accessibili e comprensibili, autorizzare verifiche esterne; 5) controllo da parte dell'utilizzatore: precludere un approccio prescrittivo (id est, deterministico) e assicurare che gli utilizzatori siano attori informati e abbiano il controllo delle loro scelte*". Così CAMERA G., op. cit., pag. 4.

[24] CAPPONI – TISCINI, *Introduzione al diritto processuale civile – seconda edizione,* G. Giappichelli Editore, Torino, 2011, pag. 25 e ss.

[25] QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings – A framework for a European legal Discussion,* in Legal Studies in International, European and Comparative Law Volume n. 4, Springer Nature, Switzerland AG 2020, pag. 81 e ss.

[26] QUATTROCOLO, op. cit. pag. 80-81.

[27] CANZIO, op. cit., pag. 905.

[28] Espressione oggi utilizzata *a contrario*, nell'art. 408 c.p.p., per come riformulato dall'art. 22 comma 1 lett.

e) d.lgs. 10 ottobre 2022, n. 150.

[29] CAMERA, op. cit., pag. 7.

[30] COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini (capitolo VIII),* in BALBI – DE SIMONE – ESPOSITO – MANACORDA, op.cit., pag. 119.

[31] GIALUZ – QUATTROCOLO, *AI and administration of criminal justice in Italy,* in rivista e-Revue Internationale de Droit Pénal (ISSN□-□2522-2945), 01/2023, https://www.penal.org/en/2023-0.

[32] È il caso di GIANOS, acronimo di Generatore Indici di Anomalia per Operazioni Sospette, utilizzato per il contrasto a reati contro il patrimonio come la ricettazione o il riciclaggio effettuati con mezzi informatici.

[33] X-Law è un sistema predittivo per la prevenzione di reati probatori, brevettato dall'ufficiale Elia Lombardo e oggi in uso in ben undici questure. È un sistema a base algoritmica euristica, che lavora su base probabilistica. Altro caso è rappresentato da Delia, che ha sostituito il precedente sistema KeyCrime, altro software di giustizia predittiva che consentirebbe di prevedere il luogo e il tempo della commissione di delitti.

[34] DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?* in DI PAOLO e PRESSACCO, *Intelligenza artificiale e processo penale,* in Quaderni della Facoltà di Giurisprudenza dell'Università degli Studi di Trento n. 63, Editoriale Scientifica, Napoli, 2022, pag. 18 e ss.

[35] È stato un Decreto del Ministero dell'Interno del 2016 ad avviare la procedura che dotato la PG del menzionato sistema SARI.

[36] UBERTIS, *Intelligenza artificiale e giustizia predittiva,* in rivista Sistema Penale, ISSN 2704-8098, 16 ottobre 2023, https://www.sistemapenale.it/it/articolo/ubertis-intelligenza-artificiale-e-giustizia-predittiva .

[37] NIEVA – FENOLL, *Intelligenza Artificiale e Processo,* G. Giappichelli Editore, Torino, 2018, pag. 58.

[38] KOSTORIS, *Intelligenza artificiale, strumenti predittivi e processo penale,* in Cassazione Penale, ISSN 2704-6338, 5 marzo 2024 https://discrimen.it/intelligenza-artificiale-strumenti-predittivi-e-processo-penale/.

[39] Suggestione sollevata, e condivisa da chi scrive, dall'Avv. Paolo Nesta, Presidente dell'Ordine degli Avvocati di Roma, durante il Convegno *"Intelligenza artificiale: rischi e opportunità"*, organizzato nei giorni 5-6 aprile 2024 dall'Associazione AS.F.EUR. in Roma, via del Banco di Santo Spirito n. 42.

[40] NISSAN, *Digital technologies and artificial intelligence's present and foreseeable impact on lawyering, judging, policing and law enforcement*, Open Forum Published: Springer Verlag London, DOI 10.007/s00146-015-0595-5,
Volume 32, https://www.researchgate.net/publication/283541194_Digital_technologies_and_artificial_intelligence's_present_and_foreseeable_impact_on_lawyering_judging_policing_and_law_enforcement , 14th October 2015, pag. 441–464.

[41] L'indicatore *disposition time***,** la misura di durata utilizzata a livello europeo, fornisce una stima del tempo medio atteso di definizione dei procedimenti mettendo a confronto il numero dei pendenti alla fine del periodo di riferimento con il flusso dei definiti nel periodo. https://www.giustizia.it/giustizia/it/mg_1_8_1.page?facetNode_1=4_10&facetNode_2=1_1%282021%29&facetNode_3=0_57&contentId=SDC354365&previsiousPage=mg_1_8#.

[42] 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, ISSN 0035-6182, vol. 76, 1/2021.