

L'INTELLIGENZA ARTIFICIALE E L'ELEMENTO DI PROVA DEL FUTURO

Mattia Viggiano^{1*}

Questo articolo rappresenta una sintesi, una rielaborazione ed allo stesso tempo un approfondimento di alcuni argomenti oggetto della tesi di laurea in Procedura Penale discussa presso il Dipartimento di “Scienze Giuridiche” dell’Università degli Studi di Salerno, scuola di Giurisprudenza, il giorno 05/02/2024 dal titolo “Il ruolo dell'intelligenza artificiale nel sistema processuale penale”. Relatore: Prof. Felice Pier Carlo Iovino.

Presentazione del lavoro:

Il lavoro, corretto dal punto di vista sintattico-grammaticale, scorrevole, facilmente comprensibile e anche di piacevole lettura, si basa su di una buona impostazione metodologica ed una compiuta consapevolezza della difficoltà degli argomenti trattati.

L’adeguatezza della bibliografia utilizzata, aggiornata alle ricerche più recenti, permette la costituzione di una solida base di partenza per seguire le tappe dottrinali e giurisprudenziali. Le argomentazioni esposte coerenti e ben sviluppate evidenziano uno spiccato senso critico ponendo in risalto tematiche che potranno essere oggetto di successivi approfondimenti scientifici.

Il lavoro appare, pertanto, degno di pubblicazione quale pezzo di esordio.

Prof. Felice Pier Carlo Iovino (Associato di Procedura Penale, DSG).

L'estrema attualità del tema dibattuto, le sue molteplici implicazioni processuali, le controverse opinioni esistenti in letteratura sull'argomento, evidenziano un'attenta e consapevole analisi critica. L'autore si esprime con una particolare chiarezza espositiva, i riferimenti bibliografici sono molteplici e sostanzialmente recenti, le note particolarmente numerose danno profondità al redazionale.

L'impegno intellettuale di ricostruzione e di elaborazione di soluzioni richiesto dalla tesi, testimonia l'interesse del candidato verso gli argomenti affrontati, ed evidenzia qualità che certamente troveranno adeguato riscontro nei suoi futuri impegni.

Il lavoro è idoneo alla pubblicazione quale pezzo di esordio.

Prof. Angelo Alessandro Sammarco (Associato di Procedura Penale, DSG).

SOMMARIO: 1.- Introduzione 2.- L’approccio del legislatore europeo 3.- Intelligenza artificiale e processo: il principio fondamentale 4.- L’elemento di prova del futuro al vaglio della normativa contemporanea 5. Conclusioni.

1.Introduzione

L’intelligenza artificiale è la tecnologia del momento.

Negli ultimi decenni, il progresso scientifico ha cambiato radicalmente le nostre vite, dando vita ad una vera e propria rivoluzione². Con questa nuova tecnologia si pongono le basi per un ulteriore enorme passo avanti per l’umanità, sempre più digitale e all’avanguardia.

^{1*} Laureato in Giurisprudenza presso l’Università degli studi di Salerno. Praticante avvocato presso il tribunale di Salerno.

² Il concetto di "rivoluzione informatica" è stato definito per la prima volta in Information Revolution da Donald M. Lambertson nel 1974.

Nonostante tale fenomeno solo attualmente sia al centro dell'attenzione la nascita, risale a circa sessant'anni fa, con le scoperte di Alan Turing³ e la nascita del termine intelligenza artificiale coniato da John McCarthy.

Nella tempesta del progresso scientifico, il faro per il giurista è costituito dai diritti fondamentali costituzionalmente garantiti. Infatti, questa nuova tecnologia avrà un notevole impatto sulla società e, come sempre accade, il diritto dovrà adeguarsi di conseguenza.

In ambito penalistico il fenomeno desta non poche preoccupazioni, poiché il processo penale è particolarmente antropocentrico e il limite rappresentato dalla tutela dei diritti, presente in tutte le fasi del procedimento, non può essere facilmente superato dalle promesse di una nuova tecnologia.

L'esigenza, in questa prima fase, risiede nella necessità di garantire genuinità ai dati allo scopo di consentirne la loro utilizzazione all'interno del processo penale, nell'ottica di soddisfare i limiti imposti dalla Carta Costituzionale.

Nei prossimi anni la sfida per il Legislatore nazionale sarà quella di monitorare costantemente tale materia, e ciò non sarà certamente facile, dal momento che appare già complessa, di per se stessa, la semplice definizione di intelligenza.

Sul tema è intervenuto il Parlamento Europeo, inquadrando l'intelligenza artificiale come: "l'abilità di una macchina di mostrare capacità umane quali il ragionamento, l'apprendimento, la pianificazione e la creatività.

L'intelligenza artificiale permette ai sistemi di capire il proprio ambiente, mettersi in relazione con quello che percepisce e risolvere problemi, e agire verso un obiettivo specifico. Il computer riceve i dati (già preparati o raccolti tramite sensori, come una videocamera), li processa e risponde. I sistemi di IA sono capaci di adattare il proprio comportamento analizzando gli effetti delle azioni precedenti e lavorando in autonomia".

Questa definizione giunge al termine di un percorso di circa dieci anni, attraverso il quale l'Unione Europea ha cercato di farsi trovare pronta ad accogliere la tecnologia del futuro.

2. Il percorso normativo del legislatore europeo.

L'approccio adottato dal legislatore europeo è incentrato sul raggiungimento di un obiettivo: la protezione dei diritti e delle libertà fondamentali delle persone fisiche, ⁴attraverso una continua regolamentazione dell'applicazione delle nuove tecnologie.

Il percorso normativo trova il suo punto di partenza con il GDPR del 2016 (Regolamento 2016/679), un regolamento con cui l'Unione Europea interviene decisamente sulla protezione dei dati personali e sulla loro libera circolazione.

Nel 2018, la Commissione europea per l'efficienza della giustizia (CEPEJ), ha pubblicato la "Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi"⁵.

Del concetto di rivoluzione digitale ne parla Gabriele Balbi in *"L'ultima ideologia, breve storia della rivoluzione digitale"*, Editori Laterza, 2022.

³ Si veda in particolare A.M. Turing, *Macchine intelligenti*, in *Intelligenza meccanica*, Bollati Boringhieri, 1994. Sul tema v. anche S. J. Russel e P. Norvig *Intelligenza artificiale: un approccio moderno*, volume I, 2021.

⁴ "Protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali." Art. 1 co. 2 Regolamento 2016/679

⁵ Per il testo completo vedi: <https://rm.coe.int/carta-etica-europea-sull-utilizzo-dell-intelligenza-artificiale-nei-si/1680993348>

Attraverso tale testo, la Commissione prevede una serie di principi fondamentali da tenere presenti, ed in particolare: a) Principio del rispetto dei diritti fondamentali⁶; b) Principio di non discriminazione⁷; c) Principio di qualità e sicurezza⁸; d) Principio di trasparenza, imparzialità ed equità⁹; e) Principio del controllo da parte dell'utilizzatore¹⁰.

La Commissione incoraggia l'utilizzo di strumenti di intelligenza artificiale nei sistemi giudiziari per aumentarne l'efficienza e la qualità. Se ne incoraggia l'utilizzo soprattutto in ambito civile, amministrativo e commerciale, mentre, in ambito penale, l'ingresso di tali strumenti deve essere affrontata con le massime riserve, vista la delicatezza della materia.

Nel 2020 si interviene nuovamente sul tema con il "Libro bianco sull'intelligenza artificiale". Attraverso tale documento l'Unione Europea pone gli obiettivi e le strategie da utilizzare per diventare *leader* mondiale nell'ambito in analisi.

La Commissione si sofferma su due temi di particolare interesse: promuovere l'IA nel settore pubblico e garantire l'accesso ai dati e alle infrastrutture di calcolo.

Nel 2024 tale lungo percorso viene concluso con l'emanazione dell'AI Act.

L'entrata in vigore del regolamento è prevista entro il primo gennaio 2026 e, contestualmente, è data la possibilità alle aziende di adeguarsi alle nuove regole fino al 2029.

Dalla proposta del 2021¹¹ si evince che l'approccio dell'Unione Europea sarà basato sui termini da conferire al concetto di rischio.

Al centro della protezione si rinviengono i diritti fondamentali, specificamente: "L'utilizzo dell'IA con le sue caratteristiche specifiche (ad esempio opacità, complessità, dipendenza dai dati, comportamento autonomo) può incidere negativamente su una serie di diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea ("la Carta")."¹²

La proposta mira a designare in maniera rigorosa i destinatari dell'atto.

Essa non è destinata ai soli fornitori o programmatori di sistemi di intelligenza artificiale, ma anche alle pubbliche amministrazioni¹³.

Nella materia che ci occupa, le consuete differenze, che spesso distinguono il settore pubblico da quello privato, non hanno ragione di sussistere in quanto la normativa si presenta con caratteristiche omogenee applicabili ad entrambi i sistemi.

L'Unione europea individua quattro categorie di rischio e le sottopone ad altrettanti regimi normativi.

I sistemi proibiti sono disciplinati dall'articolo 5, in particolare tra essi sono citate le tecnologie subliminali atte a minare i comportamenti di una persona, con particolare tutela per i soggetti fragili.

Sono, inoltre, vietate la categorizzazione biometrica dei dati personali sensibili, lo "*scraping*" di volti da internet, il riconoscimento di emozioni e i sistemi di *social score*.

Anche la polizia predittiva è vietata, a meno che non si tratti di sistemi di analisi del rischio che non si occupano di profilazione dell'individuo.

Il paragrafo d) dell'art.5 è uno dei più controversi e dibattuti della norma.

⁶ Assicurare l'elaborazione e l'attuazione di strumenti e servizi di intelligenza artificiale siano compatibili con i diritti fondamentali.

⁷ Prevenire specificamente lo sviluppo o l'intensificazione di discriminazioni tra persone o gruppi di persone.

⁸ In ordine al trattamento di decisioni e dati giudiziari, utilizzare fonti certificate e dati intangibili con modelli elaborati multidisciplinariamente, in un ambiente tecnologico sicuro.

⁹ Rendere le metodologie di trattamento dei dati accessibili e comprensibili, autorizzare verifiche esterne.

¹⁰ Precludere un approccio prescrittivo e assicurare che gli utilizzatori siano attori informati e abbiano il controllo delle loro scelte.

¹¹ Per il testo completo vedi: <https://data.consilium.europa.eu/doc/document/ST-8115-2021-INIT/it/pdf>

¹² Commissione Europea, "Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi dell'unione", p.14

¹³ Art. 2 del Regolamento.

Esso, infatti, fa riferimento alla possibilità di utilizzo di sistemi di riconoscimento facciale in tempo reale.

L'UE ribadisce il divieto già previsto nel 2021, tuttavia vi sono alcuni casi eccezionali elencati dalla norma: a) la ricerca di vittime di reati e di persone scomparse; b) minacce certe alla vita o alla sicurezza fisica delle persone o di attacco terroristico; c) localizzazione e identificazione dei presunti autori di una lista di 16 reati¹⁴.

Le fattispecie di reato previste nell'allegato IIA sono particolarmente gravi.

In tali casi la polizia può procedere all'utilizzo del sistema di riconoscimento facciale soltanto per operazioni di identificazione.

Vi sono anche altre regole da seguire: per utilizzare questi sistemi è necessaria l'autorizzazione di un giudice; in casi d'urgenza essa deve essere richiesta entro 24 ore per il riconoscimento facciale *live* e fino ad un di massimo 48 ore per quello *ex post*. Nel caso in cui manchi l'approvazione, i dati devono essere immediatamente cancellati.

La normativa lascia volutamente molta discrezionalità allo Stato membro, il quale dovrà valutare se le conseguenze pregiudizievoli del riconoscimento facciale siano giustificabili in funzione dello scopo finale.

I sistemi di IA "ad alto rischio" sono disciplinati dall'articolo 6 del Regolamento.

"La logica complessiva che la Commissione ha inteso seguire al riguardo si articola secondo due linee che si riferiscono alla compatibilità ed armonizzazione con gli altri atti normativi europei e, ancora una volta, alla ricerca di un equilibrio fra certezza del diritto e flessibilità della disciplina."

Viene lasciato molto spazio ai *providers* circa la scelta di quale debba essere lo strumento di intelligenza artificiale idoneo a rispettare la normativa europea.

Vale la pena sottolineare come il legislatore comunitario individui i sistemi "ad alto rischio" basandosi sullo scopo complessivo, non soffermandosi solo sulla funzione attribuita al dispositivo.

In particolare, sono considerati tali gli strumenti che mettono in pericolo i diritti fondamentali, la salute o la sicurezza dei cittadini.

Sono richieste particolari garanzie di sicurezza agli sviluppatori di questi sistemi.

Infatti, essi sono tenuti a fornire l'origine delle informazioni usate, garantire il funzionamento dell'algoritmo, gestire in modo trasparente i dati e stabilire ulteriori ed eventuali sistemi di controllo, ove necessario.

Nel caso in cui il sistema presenti problemi, è necessario uno "stop" da poter utilizzare istantaneamente, onde evitare di mettere a repentaglio i diritti garantiti dall'Unione Europea.

Il legislatore comunitario si sofferma particolarmente sulla raccolta dati¹⁵, laddove prescrive che essi debbano essere rilevanti, completi ed esenti da errori.

Negli articoli 10 e 15 viene imposto che i sistemi di *cybersecurity* siano adeguatamente sicuri e tali da gestire i rischi connessi.

¹⁴ Questa lista è contenuta nel paragrafo IIA: terrorismo; traffico di esseri umani; abusi sessuali su minori e pedopornografia; traffico di droghe e sostanze psicotrope; traffico illecito di armi, munizioni ed esplosivi; omicidio o gravi feriti; traffico di organi; traffico di materiale radioattivo e nucleare; sequestro di persona e ostaggi; crimini sotto la giurisdizione della Corte penale internazionale; dirottamento di aerei e navi; stupri; crimini ambientali; rapine organizzate e armate; sabotaggio; partecipazione a una organizzazione criminale coinvolta in uno o più crimini tra quelli elencati.

¹⁵ Le pratiche di gestione dei dati devono concernere: a) le scelte rilevanti operate nel design del sistema; b) la raccolta dei dati; c) le operazioni preparatorie quali l'annotazione, l'etichettatura, la pulizia, l'arricchimento e l'aggregazione dei dati; d) la formulazione degli assunti ricavabili dai dati; e) un accertamento previo della disponibilità, quantità e appropriatezza dei dati necessari; f) un esame in vista di possibili biases; g) la individuazione di possibili gaps.

Viene richiesto anche un tracciamento delle operazioni effettuate, attraverso la modalità di registrazione automatica dei *logs*.

Un punto fondamentale dell'analisi del legislatore europeo riguarda la trasparenza.

Non è possibile richiederla nella sua totalità, in quanto ci si scontrerebbe con la disciplina del segreto industriale; tuttavia è necessario il rispetto di alcuni requisiti fondamentali.

“Ogni sistema ad alto rischio, così, deve essere accompagnato da istruzioni per l'uso che contengano, del dispositivo, informazioni sintetiche, complete, corrette e comprensibili agli utenti. In particolare, oltre ai contatti del provider, dovranno essere specificati elementi come gli scopi previsti, i livelli di accuratezza, robustezza e cybersicurezza su cui il dispositivo è stato testato, le caratteristiche degli input data e dei training, validation e testing data, la durata attesa e ogni circostanza che possa condurre ad un rischio per la salute, la sicurezza o altri diritti fondamentali (art. 13).”¹⁶

In applicazione di una normativa rispettosa dei diritti fondamentali, il requisito della trasparenza gioca un ruolo chiave soprattutto ora, nella fase iniziale di utilizzo di tali strumenti. Infine, altro requisito fondamentale concerne il controllo umano, disciplinato dall'art. 14 del regolamento: “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 il sistema di IA è in uso.”

3. Intelligenza artificiale e processo: il principio fondamentale.

Nell'analisi del funzionamento dell'intelligenza artificiale e delle sue possibili applicazioni nel processo penale, occorre necessariamente partire da un assunto che: “l'intelligenza artificiale non può ricoprire le funzioni del giudice”.

Ciò trova conferma nell'articolo 25 della Costituzione, a tenore del quale viene sancito il principio della naturalità del giudice precostituito secondo legge.

Nel primo comma dell'art.22 del Regolamento (UE) 2016/6799, inoltre, si prevede: *«l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona»*.

Il regolamento appena richiamato esclude categoricamente la possibilità di essere giudicati da un giudice non umano; tuttavia, non esclude la possibilità di un supporto al giudice da parte della macchina.

Tale previsione è sancita, altresì, nell'art. 11 della Direttiva (UE) 2016/68011 che ribadisce il principio di «non esclusività» di *automated decision making*, ovvero di pronunce in cui “non vi è alcun coinvolgimento umano nel processo decisionale¹⁷”, “salvo che sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che preveda garanzie adeguate per i diritti e le libertà dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento”.¹⁸

Anche la CEDU presenta le medesime garanzie nell'articolo 5 e, in particolare, il diritto ad essere giudicati secondo le forme contemplate dai paragrafi 3 e 4, nonché l'obbligo di motivazione.

¹⁶ C. Casonato, B. Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, BioLaw Journal – Rivista di BioDiritto, n. 3/2021,p.427

¹⁷ Così, testualmente, Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, 2017, p. 20.

¹⁸ L. Lupària Donati, G. Fiorelli, *Diritto probatorio e giudizi criminali ai tempi dell'Intelligenza Artificiale*, Diritto Penale Contemporaneo, 2/2022,p.34

In tale norma è contemplato il diritto ad essere tradotti davanti a un giudice: tradizionalmente, facendo leva sul testo inglese secondo il quale il soggetto arrestato «shall be brought promptly before a judge».¹⁹ Il legislatore nazionale e quello europeo hanno elevato uno scudo dinanzi alla possibilità di un processo totalmente automatizzato confermando, almeno per ora, l'importanza del fattore umano. Al momento, quindi, l'utilizzo di sistemi di intelligenza artificiale può essere solo previsto in forma assistenziale. Tuttavia, anche questa possibilità deve essere ben monitorata.

La strada intrapresa con l'intelligenza artificiale porterà alla formazione di elementi di prova sempre più dettagliati e capaci di dimostrare la colpevolezza o l'innocenza dell'imputato.

Tale possibilità, tuttavia, deve sempre rispettare il principio di rieducazione della pena ex art. 27 Cost., mantenendo al centro del processo la figura dell'imputato "innocente fino a prova contraria". Di talché, è necessario individuare i nuovi strumenti che si affacciano al panorama processuale come possibilità per garantire gli interessi delle parti in causa, nel rispetto delle dottrine dell'individualizzazione della pena, scongiurando recrudescenze di dottrine di stampo deterministico.

4. L'elemento di prova del futuro al vaglio della normativa contemporanea.

L'elemento di prova rappresenta il momento fondamentale della sequenza probatoria per la sua centralità gnoseologica. Viene introdotto nel procedimento per svolgere le sue funzioni nella successiva fase inferenziale. Infatti, è su questo che andrà a svolgersi il procedimento intellettuale del giudice, finalizzato al raggiungimento del risultato probatorio, ovvero la situazione di fatto su cui il giudice baserà la successiva decisione.

La disamina verte su varie possibilità: attraverso l'articolo 189 c.p.p., come indizio o come prova digitale appartenente al *genus* della prova scientifica.

L'art. 189 recita testualmente: "Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova."

Il legislatore del 1988 ha espressamente riconosciuto la possibilità di introdurre prove non disciplinate dalla legge, il cui scopo è quello di utilizzare ogni contributo gnoseologico nella dimensione epistemica del processo, senza escludere lo "sviluppo tecnologico che estende le frontiere dell'investigazione e, soprattutto, senza mettere in pericolo le garanzie difensive."

Quando non si è in presenza di un istituto previsto dagli artt. 194 c.p.p. e 271 c.p.p., sarà compito del giudice decidere se la prova può trovare una propria collocazione in sede processuale attraverso due valutazioni: il dato deve essere idoneo all'accertamento dei fatti e non deve pregiudicare la libertà morale della persona.

Il termine prova "atipica" può riguardare due diverse realtà. La prima riguarda una prova non rientrante nel catalogo legale che viene definita "innominata"; la seconda riguarda il caso in cui ci siano deviazioni dal procedimento previsto dalla legge per l'assunzione di una prova tipica.

La disciplina in analisi può essere applicata anche ai mezzi di ricerca della prova. L'assunto si regge sull'analisi della collocazione della norma nel libro III del codice di rito, con possibilità di applicazione anche nella fase delle indagini.

Anche la giurisprudenza è favorevole a tale orientamento²⁰.

¹⁹ Corte e.d.u., 21 dicembre 2000, Egmez c. Cipro.

²⁰ Cass. Sez. Un., 28 marzo 2006, n.26795/2006, Prisco: in tema di videoregistrazioni, la cassazione ha ritenuto ammissibili come prove atipiche le videoriprese di comportamenti non comunicativi.

Le criticità del sistema per un'eventuale introduzione di mezzi di prova o di ricerca della prova basati su IA sono molteplici.

Il *passepourtout* dell'art. 189 potrebbe non bastare a causa delle problematiche inerenti l'opacità della raccolta dati e del procedimento seguito dall'algoritmo. L'accertamento dei fatti richiesto dalla norma non può essere garantito da uno strumento che segue un procedimento sconosciuto. Il dato più preoccupante è quello riguardante il modo in cui viene "allenato" l'algoritmo, le informazioni inserite nel *database* non possono rappresentare un'incognita dal momento che esse saranno potenzialmente utilizzate in sede processuale. Invero, il semplice inserimento di un dato errato durante la fase di programmazione condurrebbe ad un successivo *bias* del sistema e ad una catena di errori non ammissibile nel processo.

Inoltre, questi strumenti presentano le cosiddette "*black box*", fasi del procedimento in cui nemmeno i programmatori sono a conoscenza del procedimento seguito dall'algoritmo.

Al fine di contrastare la mancanza di trasparenza degli algoritmi, negli Stati Uniti è nato un movimento scientifico con l'obiettivo di sviluppare una "*Explainable Artificial Intelligence*" (XAI) con il supporto della "DARPA" (Defense Advanced Research Projects Agency).²¹

Secondo questo studio, l'algoritmo va costruito seguendo la "*explainability*" o "*interpretability*".

Nel GDPR non si fa esplicito riferimento a questo concetto di matrice americana che, tuttavia, è possibile ricavare attraverso un'interpretazione sistematica. Vi sono due orientamenti diversi: il primo preferisce un'interpretazione letterale della norma sostenendo che una verifica *ex post* non sia possibile, laddove una verifica *ex ante* lo sarebbe. Il secondo si rifà al corollario dell'articolo 12, con una lettura funzionale della norma: in questo modo è possibile ricavare il concetto di "*explainability*".²²

Nel GDPR non è presente una norma specifica contro i *bias* del sistema; tuttavia, è ricavabile dalla lettura combinata degli articoli 9 e 22 e dal generale dovere di correttezza espresso dall'articolo 5.

Infine, le statistiche sul tasso di successo non sono, allo stato, incoraggianti, in quanto solo alcuni algoritmi presentano una buona percentuale di operazioni riuscite.

Il necessario controllo umano può limitare alcune di queste problematiche, ma per avere un quadro d'insieme chiaro servirebbe la collaborazione delle aziende che si occupano dello sviluppo del *software*, tutelando ovviamente il loro diritto al segreto industriale.

Attualmente, nemmeno la libertà morale della persona sembra essere tutelata.

In particolare, la capacità intrusiva di tali mezzi, unita alla opacità dei dati, si scontra con quanto previsto dagli articoli 13 e 25 comma 2 della Costituzione e dall'articolo 8 della CEDU.

Soprattutto nel caso di un dato acquisito con un mezzo di ricerca della prova, solitamente durante la fase delle indagini, le possibilità di una violazione dei diritti fondamentali aumentano a causa della segretezza con cui vengono condotte, unita alla particolare intrusività dei sistemi di intelligenza artificiale.

²¹ "Come messo in luce dalla letteratura informatica specialistica, tuttavia, la *explainability*, o *interpretability* di un sistema di IA, è un concetto relativo, che cambia a seconda di numerosi fattori: il soggetto che vuol conoscere un certo sistema; il suo grado di conoscenza tecnologica; le finalità per cui si vanta questa pretesa; il linguaggio con cui si chiede di rendere le spiegazioni; se la spiegazione deve essere riferita all'architettura dell'intero sistema o ad una singola decisione e agli interessi con essa toccati; finanche la natura stessa degli algoritmi, più complessa nella misura in cui, come nelle reti neurali artificiali e del machine learning, essi manifestano una natura dinamica che gli consente di cambiare e aggiornarsi "imparando" continuamente. Le variabili considerate dall'algoritmo e le inferenze realizzate, poi, non sempre sono intellegibili all'uomo. Accanto a questi fattori, inoltre, bisogna anche considerare che spesso più un algoritmo è complesso e strutturato su molte variabili, più sarà accurato nei compiti che dovrà svolgere, ma meno sarà comprensibile e facilmente spiegabile." G. Mobilio, *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR*, Federalismi.it, 16/2020, pp.290-291.

²² Mobilio, *L'intelligenza* cit. p. 290.

In sostanza, e segnatamente allo scopo di rispettare i limiti imposti dall'articolo 189 c.p.p., risulta fondamentale assicurare il contraddittorio riguardo l'individuazione del procedimento acquisitivo.

In tal modo, le parti possono confrontarsi prima del momento di formazione della prova che avverrà in dibattimento, discutere apertamente sul rispetto dei requisiti morali e di accertamento dei fatti dinanzi al giudice.²³

La garanzia del contraddittorio è ciò che consentirebbe di pervenire ad una prova pienamente scientifica²⁴.

Infatti, da una prima disamina, la prova fondata su IA sembra rispettare perfettamente quanto previsto per questo genere di prova, composta da una serie di attività, generalmente svolte da un perito o un consulente tecnico, con l'utilizzo di tecniche o strumenti conosciuti e consolidati ovvero nuovi e controversi.

L'intero sistema si regge sull'articolo 190 c.p.p. rubricato proprio "diritto alla prova".

La norma prevede un filtro contro la manifesta "superfluità" o "irrilevanza" della prova, ed il legislatore ne ha volutamente mantenuto ampia la soglia di interpretabilità onde lasciare il maggiore spazio possibile al contraddittorio tra le parti.

L'obiettivo del sistema è rappresentato dal raggiungimento dell'equilibrio tra il lavoro scientifico dell'esperto e la valutazione giurisprudenziale del giudice.

D'altra parte, l'articolo 189 non presenta requisiti di specialità dall'articolo 190 c.p.p., laddove la tecnica legislativa non potrebbe mai inserire un'eccezione prima della regola. Semplicemente, l'articolo 189 si pone come una continuazione logica dell'articolo 188. Il riferimento presente in entrambe le norme alla "libertà morale della persona" non è casuale, bensì frutto di una specifica scelta del legislatore.

Il lavoro del giudice, in sede di valutazione della ammissibilità, si sostanzia in una verifica sulla congruenza tra il risultato raggiungibile con il mezzo di prova e ciò che si intende dimostrare.

L'inidoneità probatoria può dipendere anche da situazioni di "non verificabilità", cioè tutti i casi in cui non sia possibile controllare e giustificare razionalmente il dato probatorio perché ottenuto in modo non conciliabile con i parametri epistemologici.²⁵

Nel nostro ordinamento lo strumento in analisi può essere introdotto da una consulenza, nel corso delle indagini preliminari, ovvero da una perizia nella fase dibattimentale²⁶.

Il giudice, una volta completata la perizia, non sarà vincolato al parere dato dall'esperto, in quanto nel nostro sistema vige la figura dello "*iudex peritus peritorum*"²⁷.

Ciò significa che il perito fornirà il suo apporto fornendo un'analisi di natura scientifica che, tuttavia, il giudice valuterà con riferimento al caso concreto, avvalendosi di tutte le risultanze probatorie emerse nel corso dell'istruzione dibattimentale.

Ogni eventuale discostamento dalla teoria scientifica dovrà essere adeguatamente motivato dal giudice in sentenza.

Una rivoluzione nel campo della prova scientifica si è avuta con la sentenza Cozzini. Con essa, la Suprema Corte ha ammesso l'ingresso nel nostro ordinamento dei criteri di *Daubert*²⁸.

²³ R.M. Agostino, G.Dalia, M.A. Imbrenda, S. Pietropaoli, *Frontiere digitali del diritto: Esperienze giuridiche a confronto su libertà e solidarietà*, Giappichelli, 2021.p.66 ss.

²⁴ Vedi anche L. De Cataldo Neuburger, *La prova scientifica nel processo penale*, Cedam, 2007

²⁵ Vedi anche A. Gaito, *La prova penale*, Vol.I, Utet, 2008

²⁶ Articolo 220 c.p.p.: La perizia è ammessa quando occorre svolgere indagini o acquisire dati o valutazioni che richiedono specifiche competenze tecniche, scientifiche o artistiche.

²⁷ C. Mingo, *La valutazione della prova scientifica: la questione dello iudex peritus peritorum e il rapporto con l'intelligenza artificiale*, EJPLT online news, 2023.

²⁸ *Daubert v. Merrel-Dow Pharmaceutical, Inc.*, 509 U.S. 579 (1993)

Grazie a questa sentenza è possibile orientarsi nel panorama sconfinato della prova scientifica; invero il giudice opererà seguendo i criteri espressi dalla Corte in sede di valutazione della prova.

Inoltre, non è da trascurare il contributo fondamentale offerto dalle parti in dibattimento.

Proprio alla luce dei parametri stabiliti dalla Suprema Corte può essere valutata una prova scientifica formata con IA.

Inoltre, è possibile immaginare alcuni requisiti specifici per la prova in analisi: “a) controllo pubblico sul funzionamento dell’algoritmo, tramite meccanismi di peer review; b) precisazione del tasso di errore; c) spiegazione delle formule tecniche costitutive dell’algoritmo, comprensiva del collegamento con le regole giuridiche ad esso sottese; d) contraddittorio tra le parti sulla scelta dei dati archiviati, sui loro raggruppamenti e sulle loro correlazioni, elaborate dal tool di intelligenza artificiale, in particolare in relazione all’oggetto della controversia; e) valutazione dell’elemento di prova generato o raccolto tramite strumenti di intelligenza artificiale secondo il canone del libero convincimento del giudice.”²⁹

Non tutte le prove di questo tipo rientrano nel filtro dell’articolo 189 c.p.p., in quanto altre trovano dei limiti nel dispositivo dell’articolo 188 c.p.p. in tema di libertà di autodeterminazione.

In particolare, tecniche o metodi idonei ad alterare la capacità di valutare e ricordare i fatti non sono utilizzabili (ex art. 191 c.p.p.), neanche nel caso in cui vi sia il consenso della persona interrogata.

Infine, è presente un ulteriore orientamento che tende ad inquadrare la categoria delle “*digital evidence*” in esame nella disciplina prevista dall’articolo 192 co.2 c.p.p. in materia di indizi.

L’assunto parte dalle disposizioni in campo internazionale e nazionale, che garantiscono il diritto a non essere sottoposti a decisioni la cui fonte sia un trattamento automatizzato.

Nonostante la rigidità del sistema, questa appare una strada percorribile.

La sussunzione degli elementi generati o raccolti con strumenti di IA entro la categoria della prova indiziaria è possibile grazie a due caratteristiche.

Infatti, solitamente tali elementi di prova forniscono o informazioni di carattere generale, utili a descrivere genericamente i contesti in cui si sono svolti i fatti controversi, ma prive di un’autonoma capacità dimostrativa in riferimento a specifiche condotte, ovvero informazioni assai specifiche che però colgono porzioni di realtà assai ridotte.

Dunque, è possibile ritenere che tali informazioni siano idonee solo se supportate da altri elementi di prova grazie ai quali bilanciare eventuali criticità.³⁰

Il principio da tutelare è anche il cosiddetto “principio di parità delle armi”³¹, non esplicitamente previsto nell’art. 6 CEDU ma, dalla giurisprudenza³² della Corte.

Ovviamente, la “parità delle armi” non è da intendersi nei termini di un’assoluta uguaglianza di mezzi a disposizione delle parti, bensì in una generale possibilità di presentare le argomentazioni in modo da non creare squilibri tra le parti processuali.³³

²⁹ G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, Diritto Penale Contemporaneo, 4/2020. p. 23

³⁰ G. Di Paolo, L. Pressacco, *Intelligenza artificiale e processo penale: criticità emergenti e sfide per il giurista*, Università di Trento, 2022. pp.121-122.

³¹ A. Pajno, M. Bassini, G. De Gregorio, M. Macchia, *AI: profili giuridici* *Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, *BioLaw Journal – Rivista di BioDiritto*, n. 3/2019, p.23 ss.

³² CEDU, *Delcourt v. Belgium*, ric. 2689/65 (1970), : «The principle of equality of arms does not exhaust the contents of this paragraph; it is only one feature of the wider concept of fair trial by an independent and impartial tribunal»

³³ Serena Quattrocolo, *Per un’intelligenza artificiale utile al processo penale*, *BioLaw Journal–Rivista di BioDiritto*, 2/2021.

5. Conclusioni

Il dibattito circa l'utilizzo di elementi di prova fondati su intelligenza artificiale è ancora aperto. Nonostante i molti pareri contrari, alcuni sistemi di intelligenza artificiale, una volta superati i filtri e limiti imposti dalla normativa vigente, potrebbero trovare una propria collocazione nell'apparato processuale disposto dal legislatore. Tuttavia, gli istituti attualmente presenti nel codice presentano evidenti criticità in ordine alla possibilità di veicolare i dati probatori acquisiti, attraverso gli strumenti offerti dall'intelligenza artificiale. Per questi motivi, nei prossimi anni dovranno essere condotti molti studi sulla tecnologia oggetto di analisi; vi è assoluta necessità di risultati certi ed essi potranno essere raggiunti soltanto affrontando le problematiche che si presenteranno lungo la strada del cambiamento.

INDICE

INTRODUZIONE

1. RIVOLUZIONE DIGITALE E INTELLIGENZA ARTIFICIALE

- 1.1. Storia di un cambiamento inevitabile.
- 1.1.2 Una rivoluzione flessibile e permanente.
- 1.1.3 Una rivoluzione senza criticità?
- 1.2 Intelligenza artificiale: Nascita, evoluzione e tentativi di definizione.
- 1.2.2 "Big data" e grandi multinazionali.
- 1.3. Il concetto di "persona" nella modernità.
- 1.3.2. Definizione moderna di persona e prospettive future.

2. IL PERCORSO EUROPEO: DAL GDPR ALL'AI ACT

- 2.1 Il GDPR, i dati personali sotto lo scudo protettivo dell'UE.
- 2.2 Il lavoro della CEPEJ e il Libro bianco sull'intelligenza artificiale.
- 2.3. La fine del percorso: l'AI ACT.

3. INTELLIGENZA ARTIFICIALE, GIUSTIZIA PREDITTIVA E INDAGINI PRELIMINARI

- 3.1. Processo e intelligenza artificiale, un binomio difficile.
- 3.2 L'intelligenza artificiale e prevenzione dei reati, i sistemi di polizia predittiva.
- 3.3 L'intelligenza artificiale durante le indagini preliminari: focus sul riconoscimento facciale.

4. IL PROCESSO DEL FUTURO: L'INTELLIGENZA ARTIFICIALE E LA TUTELA DEI PRINCIPI DEL GIUSTO PROCESSO

- 4.1 L'intelligenza artificiale nel processo penale.
- 4.2 Elementi di prova formati con intelligenza artificiale al vaglio della normativa processuale.
- 4.3 Gli strumenti in supporto del giudice, i risk assessment tools e il principio di rieducazione della pena.

CONCLUSIONI

BIBLIOGRAFIA

AGOSTINO ROSA MARIA, DALIA GASPARE, IMBRENDA MARIA ASSUNTA, PIETROPAOLI STEFANO, “Frontiere digitali del diritto: Esperienze giuridiche a confronto su libertà e solidarietà”, Giappichelli, 2021.

BALBI GABRIELE, *“L’ultima ideologia, breve storia della rivoluzione digitale”*, Editori Laterza, 2022.

CASONATO CARLO, MARCHETTI BARBARA “Prime osservazioni sulla proposta di regolamento dell’Unione Europea in materia di intelligenza artificiale”, *BioLaw Journal–Rivista di BioDiritto*, 3/2021.

CASONATO CARLO, “Intelligenza artificiale e giustizia: potenzialità e rischi”, *DPCE online*, 3/2020.

DE CATALDO NEUBURGER LUISELLA, “La prova scientifica nel processo penale”, Cedam, 2007.

DI PAOLO GABRIELLA, PRESSACCO LUCA, “Intelligenza artificiale e processo penale: criticità emergenti e sfide per il giurista”, Università di Trento, 2022.

DI PINTO STEFANO, “La prova scientifica nel processo penale”, *Rivista di polizia*, Settembre-ottobre 2018 fascicolo IX-X anno LXXI.

DONATI LUPARIA LUCA, FIORELLI GIULIA, “Diritto probatorio e giudizi criminali ai tempi dell’Intelligenza Artificiale”, *Diritto Penale Contemporaneo*, 2/2022.

GAITO ALFREDO, “La prova penale: il sistema della prova”, Vol.I, Utet, 2008.

GAITO ALFREDO, “La prova penale: le dinamiche probatorie e gli strumenti per l’accertamento giudiziale”, vol. II, Utet, 2008.

LEYEN URSULA VON DER, “Orientamenti politici per la prossima Commissione europea 2019-2024: Discorso di apertura della seduta plenaria del Parlamento europeo 16 luglio 2019;

MINGO CRISTINA, “La valutazione della prova scientifica: la questione dello iudex peritus peritorum e il rapporto con l’intelligenza artificiale”, *EJLPT online*, 2023.

MOBILIO GIUSEPPE, “L’intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR”, *Federalismi.it*, 16/2020.

NAGNI EMANUELE, “Artificial intelligence, l’innovativo rapporto di (in)compatibilità fra machina sapiens e processo penale”, *Sistema Penale*, 07/2021.

PAJNO ALESSANDRO (et. al.), “Intelligenza artificiale: criticità emergenti e sfide per il giurista”, *BioLaw Journal–Rivista di BioDiritto*, 3/2019.

QUATTROCCOLO SERENA, “Per un’intelligenza artificiale utile al processo penale”, *BioLaw Journal–Rivista di BioDiritto*, 2/2021.

TABASCO GIUSEPPE, “Prove non disciplinate dalla legge nel processo penale, le prove atipiche tra teoria e prassi”, Edizioni scientifiche italiane, 2011.

TURING ALAN MATHISON, “Intelligenza meccanica”, Bollati Boringhieri, 1994.

TURING ALAN MATHISON, “On computable numbers, with an application to the entscheidungs problem”, Princeton, 1936.

UBERTIS GIULIO, “Intelligenza artificiale, giustizia penale, controllo umano significativo”, Diritto Penale Contemporaneo, 4/2020.

Abstract.- L’avvento dell’intelligenza artificiale apre nuove discussioni in merito al processo del futuro. La scienza è in costante evoluzione e il diritto non può restare indietro, ogni nuova scoperta deve essere analizzata attentamente dall’operatore del diritto, individuando eventuali criticità e punti di forza. Tuttavia, mai come ora, è necessario proteggere i diritti fondamentali su cui sono fondate le moderne democrazie occidentali. Il dato da tenere in considerazione, prima di tentare proiezioni future sul tema, è la normativa attuale europea e nazionale, con le garanzie assicurate da questi sistemi, non sacrificabili sull’altare del progresso. Il processo penale del futuro dovrà confrontarsi con queste nuove problematiche, aprendo a nuovi orizzonti per quanto riguarda l’analisi dell’elemento di prova e il ragionamento inferenziale seguito dal giudice.

The advent of artificial intelligence opens new discussions regarding the process of the future. Science is constantly evolving and law cannot lag behind, every new discovery must be carefully analyzed by the legal practitioner, identifying any critical issues and strengths. However, never before has it been necessary to protect the fundamental rights on which modern Western democracies are founded. The data to take into consideration, before attempting future projections on the topic, is the current European and national legislation, with the guarantees ensured by these systems, which cannot be sacrificed on the altar of progress. The criminal trial of the future will have to deal with these new problems, opening up new horizons regarding the analysis of the evidence and the inferential reasoning followed by the judge.