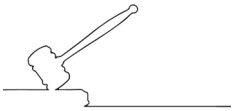
TEORIA E PRASSI
DELLA GIUSTIZIA PENALE CONTEMPORANEA

14

TEORIA E PRASSI
DELLA GIUSTIZIA PENALE CONTEMPORANEA



La collana avrà di mira l'analisi dei più attuali temi di "diritto vivente", conseguenti all'evoluzione delle fattispecie penali tradizionali e all'introduzione di nuove figure di illecito penale nei diversi settori del diritto (diritto penale commerciale, bancario, ambientale, transazionale, eccetera), non sempre in sintonia con i principi penali generali e con i correlati valori costituzionali, chiamati in causa dalle nuove forme di prevenzione e di repressione poste in campo dal legislatore per contrastare i più diffusi fenomeni criminali.

Nella medesima ottica troveranno ospitalità contributi di ricerca ed analisi di diritto processuale penale, volti a verificare il grado e le caratteristiche del mutato rapporto tra diritto sostanziale e processo penale, del nuovo volto della prova penale determinato dal sottosistema processuale del "doppio binario", e dalla strisciante contaminazione del complessivo sistema processuale in ragione dei nuovi obiettivi del diritto penale securitario.

In tale ambito verrà portata l'attenzione sulla diffusione di "scorciatoie" probatorie e di flessibilità interpretativa che connotano il sistema delle misure di prevenzione, soprattutto di quelle patrimoniali.

I contributi, di carattere non descrittivo ma problematico, saranno incentrati sull'analisi critica della giustizia penale contemporanea, nell'ambito della giurisprudenza nazionale e sovranazionale raffrontate alle diverse teoriche tradizionali e quelle prospettate dai più recenti studi ed approdi della dottrina.

Classificazione Decimale Dewey:
340.028563 (23.) DIRITTO. INTELLIGENZA ARTIFICIALE

ANTONIO CARLO OLIVERI DEL CASTILLO

LA RESPONSABILITÀ PENALE DELLE INTELLIGENZE ARTIFICIALI

aracne

ISBN
979–12–218–1531–3

PRIMA EDIZIONE
ROMA 24 OTTOBRE 2024

INDICE

9 Capitolo I
Diritto penale e Intelligenza Artificiale

1.1. In che modo l'Intelligenza artificiale incide sul diritto, 9 – 1.2. Cosa si intende per Intelligenza Artificiale, 29.

35 Capitolo II
Sistema penale tradizionale e Intelligenza Artificiale

2.1. Applicabilità del sistema penale tradizionale?, 35 – 2.2. Scomposizione analitica del reato, 39 – 2.3. Modello oggettivo o soggettivo del reato, 40 – 2.4. La sistematica quadripartita, 42 – 2.4.1. *Il fatto*, 45 – 2.4.2. *L'antigiuridicità*, 47 – 2.4.3. *La colpevolezza*, 53 – 2.4.4. *La punibilità*, 66 – 2.4.5. *Riferibilità degli elementi del reato alle IA: osservazioni preliminari*, 71 – 2.5. Le funzioni della pena, 76 – 2.5.1. *Risarcimento*, 78 – 2.5.2. *Dissuasione*, 80 – 2.5.3. *Riabilitazione*, 84 – 2.5.4. *Interdizione*, 90 – 2.5.5. *Riferibilità della pena alle IA: osservazioni preliminari*, 92.

95 Capitolo III
Dominio e crisi del brocardo "*Machina delinquere (et puniri) non potest*" e vuoto di responsabilità

3.1. Dominio del brocardo "*Machina delinquere et puniri non potest*" e responsabilità vicaria dell'uomo, 95 – 3.2. Ipotesi di reato doloso commesso dall'uomo a mezzo IA, 101 – 3.3. Ipotesi di reato colposo e responsabilità penale dell'utilizzatore, 116 – 3.4. Le *self–driving cars*: classificazioni, 127 – 3.5. Responsabilità penale del conducente, 132 – 3.6. Responsabilità penale del produttore o programmatore: danno da prodotto, 137 – 3.7. Fuori dall'area del danno da prodotto: "Vuoto" di responsabilità e crisi dell'assioma "*Machina delinquere et puniri non potest*", 141 – 3.8. IA in ambito medico, 147.

153 Capitolo iv
Nuove esigenze di tutela: *Machina delinquere potest?*
4.1. Responsabilità diretta delle IA: la tesi positiva di Gabriel Hallevy, 153 – 4.1.1. Actus reus, 155 – 4.1.2. Mens rea, 156 – *4.1.2.1. Libero arbitrio*, 158 – *4.1.2.2. Personalità giuridica*, 161 – 4.1.3. *Parallelismo con il sistema della responsabilità da reato degli enti*, 164 – 4.1.4. *Applicabilità della pena*, 166 – 4.1.5. *L'importanza del dibattito avente ad oggetto la diretta responsabilità penale degli agenti intelligenti*, 171 – 4.2. Le critiche fondamentali alla teoria positiva di Gabriel Hallevy, 173 – 4.2.1. *Assenza dell'elemento soggettivo*, 174 – 4.2.2. *Inapplicabilità della pena*, 179 – 4.2.3. *Fallibilità del parallelismo con il sistema della responsabilità da reato degli enti*, 185.

189 Capitolo v
Un'indagine destinata a rimanere ancora aperta
5.1. Conferma del brocardo "*Machina delinquere et puniri non potest*": due possibili indirizzi, 189 – 5.2. Prospettive attuali, 193 – 5.3. Prospettive future, 195.

199 *Bibliografia*

CAPITOLO I

DIRITTO PENALE E INTELLIGENZA ARTIFICIALE

1.1. In che modo l'Intelligenza artificiale incide sul diritto

Il tema della responsabilità penale delle Intelligenze artificiali per i reati da esse commessi rappresenta oggi una materia senza dubbio ancora non pienamente al centro del dibattito pubblico, ma sicuramente all'avanguardia, trovandosi la società moderna alle porte di una nuova era digitale, destinata a travolgere con tutta la sua forza il mondo oggi conosciuto.

Questo scenario, dunque, impone agli studiosi del Diritto di analizzare a fondo tale fenomeno, di interrogarsi sulle sue implicazioni di ordine giuridico, e di prospettare risposte adeguate alle questioni di rilevanza penale che tale realtà pone, affinché la società possa essere preparata ad affrontarne ogni aspetto quando quello che oggi è presente solo nell'immaginario collettivo o in alcune specifiche realtà più avanzate, diventerà abituale e quotidiano.

L'essere umano, ormai già da diversi decenni, vive sulla propria pelle una nuova rivoluzione industriale avente ad oggetto l'elaborazione di tecnologie sempre più avanzate e sofisticate e che procede a ritmi sempre più rapidi e impetuosi, tanto da aver fatto della tecnologia il nucleo essenziale della propria vita quotidiana, privata e non. Il mondo di oggi è ormai completamente dipendente dall'uso della tecnologia in ogni suo ambito, ed ora, in ultima istanza, si avvia ad esserlo anche in campo giuridico.

«Nell'arco dei prossimi cento anni, l'intelligenza dei computer supererà quella degli esseri umani»[1]. Potrebbe sembrare pura retorica, o mera fantascienza, ma l'affermazione del fisico, astrofisico e matematico Stephen Hawking manifesta con estrema semplicità e chiarezza la direzione verso cui inevitabilmente si dirige la società moderna grazie all'inarrestabile progresso tecnologico.

Già da diverso tempo, infatti, la società risulta caratterizzata dal ricorso sempre più frenetico all'utilizzo di sistemi di Intelligenza Artificiale e più in generale dei computer nei più svariati ambiti della vita quotidiana — nella sfera privata, negli ospedali, nelle banche, nelle compagnie di assicurazione — e si avvia ad esserne dominata man mano che vengono elaborate tecnologie sempre più avanzate e raffinate, «e quando questo accadrà, dovremo assicurarci che i computer condividano i nostri stessi obiettivi»[2]. Il progresso irrompe senza chiedere il permesso, senza concedere il tempo di elaborare un nuovo modello di società che sia in grado di accogliere con consapevolezza le sue conseguenze, travolgendo gli equilibri su cui attualmente essa si fonda e rivoluzionando i rapporti oggi conosciuti tra uomo e macchina.

L'uomo si ritrova così in balia della tecnologia, e in uno scenario di tal genere, per certi versi allarmante, egli rischia di venirne travolto e di essere del tutto sguarnito dei presidi tradizionali di protezione, concepiti dal legislatore per proteggerlo da condotte umane, e non dalle attuali e future illecite manifestazioni dell'innovazione tecnologica. D'altra parte, la veridicità e lucidità di tali previsioni parrebbe essere confermata anche dall'affermazione contenuta nei Considerando della Risoluzione del Parlamento Europeo sulla Robotica del 16 febbraio 2017[3], che dichiara che è possibile che a lungo termine l'Intelligenza Artificiale superi la capacità intellettuale umana.

Proprio in tali Considerando è possibile scorgere allora una sollecitazione nei confronti del giurista ad indagare a fondo le correlazioni tra Intelligenza Artificiali e Diritto — in particolar modo Diritto penale — nella misura in cui si afferma che se da sempre la mente umana ha

(1) Intervento di S. Hawking durante la Conferenza Zeitgeist, Londra, maggio 2015.

(2) Intervento di S. Hawking, citato *supra*, nota 1.

(3) Risoluzione del Parlamento europeo del 16 febbraio 2017, recante raccomandazioni alla Commissione concernenti nome di diritto civile sulla robotica.

spaziato dando libero sfogo all'immaginazione circa la possibilità di costruire macchine intelligenti, oggi davvero la civiltà umana si trova agli inizi di nuova rivoluzione industriale, di cui sono protagonisti esclusivi robot, bot, androidi ed ogni altra manifestazione di Intelligenza Artificiale, e che è destinata inevitabilmente a coinvolgere ogni aspetto della vita dell'uomo, divenendo quindi imprescindibile che la legislazione ne consideri le implicazioni e le conseguenze legali ed etiche, senza che venga ostacolata l'innovazione. A questo punto, come dinanzi ad ogni progresso nel corso della storia dell'uomo, l'attuale andamento pone un complesso scenario: l'elaborazione e lo sviluppo di macchine robotiche sempre più autonome e intelligenti, capaci di apprendere e adottare decisioni in modo indipendente e sulla base della propria stessa esperienza, comporta non solamente immensi vantaggi in termini economici e di efficienza, ma anche innumerevoli perplessità di carattere giuridico legate agli effetti pratici che l'utilizzo dei sistemi di Intelligenza artificiale può produrre sulla società.

È evidente, dunque, che tra i settori interessati da tale rivoluzione digitale non manca naturalmente il mondo del Diritto, ed in particolar modo quello del Diritto penale: è necessario, se non addirittura vitale, riflettere approfonditamente sulle già numerose implicazioni di rilevanza penale derivanti dall'utilizzo delle Intelligenze Artificiali ed iniziare a prospettare specifiche soluzioni giuridiche alle problematiche che emergeranno con sempre maggiore frequenza, al fine di contenere quanto più possibile il fisiologico ritardo del Diritto dinanzi all'incalzante e inarrestabile progresso tecnologico.

Come è stato efficacemente affermato, «Il progresso irrompe, non chiede il permesso. […] Oggi le tecnologie digitali irrompono molto più velocemente, e non ci danno affatto il tempo per organizzarci e per abituarci alle loro dirompenti innovazioni»[4].

All''interno di tale scenario, bisogna dunque verificare se le norme già esistenti siano idonee ad applicarsi alle questioni giuridiche poste dalle nuove tecnologie, potendosi persistere quindi con le medesime, o se sia invece opportuno procedere all'introduzione di nuove disposizioni *ad hoc*.

(4) G.F. Italiano, *Intelligenza artificiale, che errore lasciarla agli informatici*, in «Agendadigitale.eu», 11 giugno 2019.

Uno dei principali interrogativi che la sempre maggiore diffusione dei sistemi di Intelligenza artificiale nella società moderna impone di porre concerne la responsabilità penale nell'eventualità in cui si verifichi la commissione di un illecito penale da parte dell'Intelligenza artificiale stessa: sino a quando l'uomo si sia limitato a produrre dispositivi meccanici che fungessero da meri strumenti e a servirsene come meri strumenti, non è parso sorgere alcun dubbio circa l'applicabilità del sistema penale tradizionale e circa l'individuazione della responsabilità penale in capo all'agente umano — produttore o utilizzatore —. Ma *quid iuris* se le macchine robotiche elaborate dall'uomo raggiungono un grado di sofisticazione e di autonomia tale da renderle entità indipendenti dall'uomo, "soggetti" "pari" all'uomo? Quale dovrebbe essere la risposta dell'Ordinamento in termini giuridici quando tali dispositivi raggiungono un livello di complessità tale da divenire non solamente in grado di elaborare processi logici prestabiliti dal produttore o di rispondere ai suoi comandi, ma anche capaci di apprendere dalla propria stessa esperienza, di "pensare" e di "comportarsi" autonomamente?

Ad ogni modo pare opportuna, a titolo introduttivo, una sintetica rassegna di quelli che sono i principali ambiti di rilevanza penale sui quali potrebbe incidere con maggior forza la rivoluzione innescata dalla diffusione delle Intelligenze Artificiali.

Tali settori, potenzialmente toccati dal sempre più frenetico ricorso ai sistemi di Intelligenza Artificiale nella moderna società, vengono identificati da autorevole dottrina[5] in primo luogo nelle attività di Law Enforcement, ed in particolare modo di polizia predittiva, in relazione alle quali le Intelligenze Artificiali sono in grado di offrire un prezioso contributo nel tentativo di contrastare, o anche di prevenire, la commissione di fatti criminosi, mettendo in correlazione una molteplicità di dati provenienti da fonti eterogenee; in secondo luogo nell'affiancamento, se non addirittura nella piena sostituzione, del giudice–macchina al giudice–uomo attraverso l'utilizzo di algoritmi decisionali; ancora, nell'impiego di algoritmi predittivi in grado di individuare e mettere in relazione tra loro enormi quantità di dati personali relativi all'individuo di cui si intende valutare la pericolosità sociale, al fine di

(5) F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in «Diritto penale e uomo – DPU», 29 settembre 2019.

far emergere coincidenze e correlazioni che, se osservate attentamente, consentirebbero di disegnare il profilo criminale del soggetto in esame e di ipotizzarne, con un grado di probabilità più o meno elevato, i successivi comportamenti di rilevanza penale; infine — ed è il tema che più interessa ai fini della presente trattazione — nel possibile coinvolgimento dei sistemi di Intelligenza Artificiale in qualità di strumento, di vittima, o di autore nella commissione di un reato.

Per quanto riguarda il primo dei quattro campi d'indagine — l'attività di Law Enforcement ed in particolar modo di polizia predittiva — il ricorso ai sistemi di Intelligenza Artificiale rappresenta già oggi una concreta realtà in atto, di cui si può prospettare una potente crescita e intensificazione nel prossimo futuro: nel documento del 2019 *Annual Police Experts Meeting: Artificial Intelligence and Law Enforcement: An Ally or an Adversary?*, dedicato per l'appunto al tema delle Intelligenze Artificiali e delle attività di Law Enforcement, si dichiara che

> Nei loro sforzi per aumentare l'efficienza e l'efficacia e per stare al passo con le innovazioni tecnologiche, le autorità e le agenzie di Law Enforcement di tutto il mondo stanno esplorando sempre più i potenziali dell'Intelligenza Artificiale per il lavoro. […] Anche se l'uso dell'Intelligenza Artificiale nel lavoro delle forze dell'ordine è un argomento relativamente nuovo, alcuni strumenti basati sull'Intelligenza Artificiale sono già stati testati e sono persino attivamente utilizzati dai servizi di polizia di diversi paesi del mondo. Questi includono Software di analisi di video e immagini, sistemi di riconoscimento facciale, di identificazione biometrica, droni autonomi e altri robot e strumenti di analisi predittiva per prevedere le "zone calde" del crimine o anche per identificare potenziali criminali futuri, in particolare i criminali ad alta pericolosità.(6)

E d'altra parte, una conferma dei preziosi risultati che il ricorso ai sistemi di Intelligenza Artificiale nell'ambito delle attività di Law Enforcement consentirebbe di produrre la si può rinvenire in alcuni episodi concreti: nel tempo, infatti, si sono susseguiti diversi casi in cui l'utilizzo di semplici algoritmi, qualora vi si fosse fatto ricorso, sarebbe stato probabilmente in grado di prevenire e dunque di evitare

(6) Documento di presentazione del 2019 OSCE, *Annual Police Experts Meeting: Artificial Intelligence and Law Enforcement: An Ally or an Adversary?*, 23–24 settembre, Vienna.

la commissione di reati, con particolare attenzione ai reati di terrorismo. In special modo si ricordi l'episodio del terrorista Umar Farouk Abdulmutallab, il quale nel lontano 2009 si imbarcò sul volo Amsterdam–Detroit con dell'esplosivo collocato all'interno della cucitura della propria biancheria intima. A seguito dell'intervento di alcuni passeggeri, l'attacco terroristico fallì, ma ciò su cui converrebbe soffermarsi è che l'Intelligence certamente deteneva dati e informazioni sufficienti per essere a conoscenza del grado di pericolosità sociale del passeggero–terrorista, e per negargli pertanto la possibilità di imbarcarsi, e tuttavia ciò che è mancata è stata la capacità — del tutto umana — dell'Intelligence di mettere in relazione le informazioni in suo possesso. L'errore parrebbe essere umano. Le manchevolezze sembrerebbero essere attribuibili all'abilità umana. Con ogni probabilità, dunque, l'utilizzo anche di semplici algoritmi avrebbe consentito di correlare tra loro i dati conosciuti, di riscontrare anomalie e attività sospette, o comunque di ricondurre le numerose informazioni a disposizione, provenienti da fonti eterogenee, all'interno di un unico e coerente quadro, tale da evidenziare chiaramente la pericolosità criminale dell'individuo e quindi la necessità di adottare, da parte dell'uomo, concreti provvedimenti volti a prevenire il verificarsi dell'evento terroristico.

Ad ogni modo, sono diverse le modalità con cui i sistemi di Intelligenza Artificiale possono essere adoperati in questo campo: si tratta principalmente di macchine robotiche, umanoidi e non, utilizzate con un'ampia varietà di funzioni, come attività di sorveglianza, di riconoscimento facciale, di pattugliamento, di individuazione di atteggiamenti sospetti, di disinnesco di bombe, ecc.

E tuttavia di tali impieghi dei sistemi di Intelligenza Artificiale è possibile prospettare una serie di controindicazioni che inevitabilmente fanno da contraltare agli immensi benefici: se da un lato è infatti innegabile il merito di preservare da una serie di fonti di pericolo l'agente umano, il quale ha la possibilità di non esporsi in prima linea, nonché il merito di garantire un elevato livello di efficienza e precisione delle prestazioni poste in essere dalla macchina robotica, dall'altro lato non possono trascurarsi una serie di perplessità legate al loro utilizzo.

Un primo punto interrogativo riguarda l'intensità più o meno elevata del controllo da esercitarsi sui sistemi di Intelligenza Artificiale da

parte dell'operatore umano, che potrà solo limitarsi all'individuazione degli obiettivi da realizzare, o potrà invece supervisionare più profondamente lo svolgimento della prestazione da parte della macchina robotica, anche a rischio di comprometterla.

In secondo luogo, sorge il rischio di violazione del diritto alla privacy dell'individuo, in considerazione della capacità di tali sistemi algoritmici di acquisire ed elaborare enormi quantità di dati ed informazioni relative alla vita — anche privata — dei cittadini. Infine, bisogna considerare che spesso tali dispositivi risultano equipaggiati con armi letali e non, e da tale circostanza scaturiscono profonde preoccupazioni in merito al grado di affidabilità e fallibilità di tali applicazioni, in merito al rischio di commissione di uccisioni o lesioni per errore, ed in merito all'individuazione della relativa responsabilità in capo alla macchina o all'agente umano.

Rimanendo nell'ambito dell'attività di Law Enforcement, merita un attento e approfondito sguardo il tema della Polizia predittiva, per la quale si intende il complesso di attività volte appunto a predire chi potrà commettere un reato, o dove e quando potrà essere commesso, al fine di prevenirne la verificazione.

Tale previsione si basa principalmente sull'acquisizione, rielaborazione, e messa in relazione tra loro, di diverse tipologie di dati, che possono essere relativi a precedenti penali, ai luoghi, orari e periodi dell'anno maggiormente connessi alla commissione di determinati fatti criminosi, agli spostamenti e alle attività svolte da soggetti sospettati, o ancora dati inerenti al livello di scolarizzazione, all'origine etnica, alle caratteristiche somatiche, o alle condizioni economiche di un individuo. In altre parole, il sistema di polizia predittiva basa il suo funzionamento su dei software in grado di rielaborare enormi quantità di dati e informazioni, scoprendo ed evidenziando correlazioni difficilmente individuabili dal nudo occhio dell'operatore umano. Tali software di polizia predittiva si suddividono in due principali categorie: in primo luogo quelli che si ispirano alla criminologia ambientale e individuano i luoghi dove è più elevata la probabilità che si possa verificare la commissione di determinati reati, vale a dire le cosiddette "zone calde" ("*hotspot*"); in secondo luogo quelli che si ispirano al concetto di *crime linking* e monitorano non tanto i luoghi a rischio, quanto i comportamenti di determinati soggetti,

al fine di prevedere dove e quando potrebbero commettere il prossimo reato. Ovviamente, tali algoritmi funzionano oggi non in maniera generalizzata, ma solo in relazione alla previsione di specifiche categorie di reati (come rapine o spaccio di stupefacenti, attinenti quindi alla criminalità da strada) — quei reati, cioè, rispetto ai quali assumono particolare rilevanza determinate caratteristiche (come luoghi o fasce orarie in cui è più probabile che vengano commessi), le quali vengono captate e rielaborate dal software ai fini della predizione —.

Rientra nella prima categoria di software di polizia predittiva il cosiddetto "*Risk Terrain Modeling (RTM)*": si tratta di un algoritmo capace di prevedere dove e quando è più elevata la possibilità che si verifichino attività di spaccio di sostanze stupefacenti, sulla base dell'esame di una serie di fattori spaziali e ambientali tradizionalmente in grado di favorirne la commissione, quali ad esempio la vicinanza a locali notturni, a stazioni ferroviarie, a fermate di mezzi pubblici, scarsa presenza di luminarie stradali, orari notturni, ecc. Tale *modus operandi*, dunque, si è rivelato capace di consentire di disegnare una vera e propria mappatura delle aree urbane dove è maggiore il rischio di spaccio di sostanze stupefacenti, e di programmare e porre in essere con adeguato anticipo interventi volti ad impedire la commissione del fatto criminoso. Un altro esempio di software di polizia predittiva che si ispira alle acquisizioni della criminologia ambientale potrebbe corrispondere anche a un dispositivo attualmente utilizzato dalla Polizia di Stato italiana: il cosiddetto "*X–LAW*", messo a punto in origine dalla questura di Napoli. Anche il funzionamento di tale algoritmo si basa sostanzialmente sulla rielaborazione di un'ingente mole di dati e informazioni derivanti dalle denunce inoltrate nel tempo alla Polizia di Stato, volta a far emergere coincidenze, correlazioni e fattori ricorrenti che l'agente umano potrebbe non essere altrettanto capace di osservare. In questo modo diviene possibile disegnare una mappa del territorio che evidenzi le zone e gli orari "caldi", dove è più elevato il rischio di commissione di attività criminali, e sulla base delle indicazioni che risultano, predisporre le forze dell'ordine al fine di impedire che tali attività vengano portate a compimento, cogliendo in flagranza i relativi autori.

È riconducibile, invece, alla categoria dei software ispirati al concetto di *crime linking* il cosiddetto "*Software Keycrime*", elaborato presso

la Questura di Milano, non dissimile da altri software della medesima tipologia elaborati e attualmente in uso in Germania, Inghilterra e Stati Uniti. Mentre i sistemi di individuazione degli *hotspots* si basano sulla individuazione delle "zone calde", al contrario i sistemi di *crime linking* si concentrano sul profilo della persona potenziale autore di un reato. Il funzionamento di tali algoritmi, dunque, individua il proprio nucleo nella capacità di disegnare il profilo criminale del possibile autore di una serie di fatti criminosi, al fine di ipotizzarne la mossa successiva.

Eppure di tali sistemi di polizia predittiva, di cui si è tentato di offrire un sintetico quadro descrittivo, se da un lato siano considerevoli ed innegabili i vantaggi sul piano della prevenzione del crimine — vantaggi che col tempo sono certamente destinati a crescere e ad intensificarsi — dall'altro lato non se ne possono trascurare le perplessità che scaturiscono dal loro utilizzo, al fine di una loro efficiente ed allo stesso tempo sicura attuazione.

In primo luogo bisogna osservare che tale primo impiego dei sistemi di Intelligenza Artificiale, ad oggi, non è stato affatto disciplinato in nessuno Stato, ragione per la quale il loro uso rimane affidato esclusivamente al buon senso, alla sensibilità e all'esperienza degli operatori di polizia, e del tutto svincolato da ferree disposizioni scritte.

In secondo luogo vanno considerate anche le implicazioni circa la tutela della privacy, in considerazione del fatto che il funzionamento della maggior parte di tali sistemi di polizia predittiva si basa principalmente su algoritmi in grado di acquisire e rielaborare notevoli quantità di informazioni e dati personali, nel necessario rispetto del divieto di discriminazione nell'analisi delle caratteristiche etniche, somatiche, religiose e sociali.

Ancora, per quanto attiene al loro meccanismo di funzionamento, tali software si auto–alimentano con i dati che essi stessi rilevano, emergendo così il rischio che il loro utilizzo divenga controproducente rispetto agli obiettivi da raggiungere e che si inneschino irrimediabili circoli viziosi. In altre parole, se il software individua una determinata area come "zona calda", con conseguente intensificazione dello spiegamento delle forze dell'ordine, sorge il rischio che da quel momento in poi i sistemi di polizia predittiva continuino a qualificare quella regione come zona calda non già in ragione dell'effettiva verificazione di fatti

criminosi, bensì in ragione dell'intensificazione dei controlli e dei pattugliamenti e del fatto che quell'area sia stata qualificata in origine come zona a rischio dal software stesso.

Inoltre va rilevato come tali sistemi di polizia predittiva conducano alla prevenzione dei reati attraverso la militarizzazione delle aree emerse come "zone calde" — tramite cioè il pattugliamento e l'intervento attivo delle forze di polizia — lì dove sarebbe invece più auspicabile condurre la battaglia al crimine sul piano sociale, attraverso cioè un'azione che si rivolga ai fattori criminogeni, quali i fattori economici, ambientali, individuali, ecc.

Da ultimo, bisogna tener conto che la maggior parte di questi software, in quanto messi a punto da aziende private, sono coperti dal segreto industriale e commerciale, ragione per la quale non sarebbe possibile comprendere a fondo il meccanismo del relativo funzionamento, con conseguente pregiudizio delle esigenze di trasparenza e pubblicità.

Naturalmente, tali perplessità legate all'utilizzo dei sistemi di polizia predittiva non dovrebbero rappresentare una ragione per arrestarsi dinanzi al progresso, quanto invece un incentivo a regolamentarne l'impiego ed a predisporre una specifica risposta giuridica alle questioni legali che l'uso di tali algoritmi può presentare.

Il secondo ambito coinvolto dalla diffusione delle Intelligenze artificiali concerne l'impiego di algoritmi decisionali volti a consentire l'affiancamento, o addirittura la sostituzione, del giudice–macchina rispetto al giudice–uomo.

Tali sistemi di Intelligenza Artificiale, definiti "*Automated decision system*", sono in fase di forte crescita e diffusione sia nel pubblico che nel privato e, in ragione della loro capacità di acquisire in tempi rapidi una molteplicità di dati da innumerevoli fonti quali Codici, banche–dati giurisprudenziali, legislative e raccolte di precedenti, si sono rivelati in grado di assumere decisioni volte a prevenire e comporre le controversie tra i privati.

Si tratta dunque, anche da questo diverso angolo visuale, di una potenziale rivoluzione avente ad oggetto l'introduzione di veri e propri meccanismi alternativi di risoluzione delle controversie che rispetto al sistema giuridico tradizionale comportano vantaggi di non poco momento nell'economia globale di un procedimento giudiziario, quali

la riduzione dei tempi e rilevanti risparmi di spesa per le parti in causa. Ciononostante, gli "*Automated decision system*" sono oggi adoperati quasi esclusivamente nell'ambito di alcune questioni civili, concernenti ad esempio il risarcimento dei danni, danni da prodotto, pratiche assicurative, mancando ancora un loro utilizzo in ambito penale, in ragione, probabilmente, della maggiore delicatezza e rilevanza di tale settore. Naturalmente l'attuale realtà non esclude affatto che l'incalzante progresso tecnologico possa condurre in tempi brevi ad un ruolo decisionale attivo di tali software anche nelle cause penali. Ed infatti, proprio la prospettiva di una diffusione di algoritmi decisionali anche in materia penale ha destato l'attenzione e suscitato le preoccupazioni del Consiglio d'Europa, la cui commissione per l'efficacia della giustizia (CEPEJ), lo scorso 3 dicembre 2018, ha redatto la cosiddetta *Carta etica europea per l'uso dell'Intelligenza artificiale nei sistemi di giustizia penale e nei relativi ambienti*. Si è trattato di un epocale momento di svolta nel mondo dell'interazione tra Intelligenza Artificiale e Diritto: per la prima volta, sebbene solo limitatamente al contesto di tale impiego dei sistemi di Intelligenza artificiale, si è preso atto del loro smisurato potenziale e del ruolo attivo che sono inevitabilmente destinati a svolgere nella società moderna, e sulla base di questo, si è tentato di cristallizzare alcune fondamentali linee guida a cui dovranno necessariamente attenersi i responsabili dei progetti aventi ad oggetto lo sviluppo e l'uso delle IA.

Tale Carta etica europea ha avuto il merito di affermare, dunque, anche nell'ambito dell'utilizzo dei sistemi di Intelligenza artificiale, principi basilari quali il rispetto dei diritti fondamentali, il divieto di discriminazione, principio di qualità e sicurezza, trasparenza, imparzialità, sicurezza e garanzia del controllo umano. Tra tutti, quest'ultimo rappresenta il principio di maggior interesse in quanto volto a scongiurare eccessivi automatismi e ad assicurare sempre il controllo sul funzionamento di tali algoritmi decisionali da parte dell'operatore umano.

Inoltre il loro impiego, specialmente nell'ambito dei procedimenti penali, oltre a destare preoccupazioni in merito a scongiurabili automatismi, solleva anche altre perplessità: in primo luogo occorre considerare che il mezzo probatorio a cui più di frequente si fa ricorso in un procedimento penale è la testimonianza orale, e sarebbe corretto ritenere che una macchina robotica, non disponendo delle medesime

qualità umane, non sarebbe altrettanto in grado di stabilire se il teste menta, sia reticente, o al contrario affermi il vero. In secondo luogo, tali sistemi di Intelligenza Artificiale si rivelano in generale inidonei a valutare la prova in un processo penale, in ragione soprattutto della pluralità e non predeterminatezza dei criteri di valutazione, in special modo in un processo indiziario dove, ai sensi dell'art. 192 comma 2 c.p.p., gli indizi devono essere gravi, precisi e concordanti, perché possa essere desunta da essi l'esistenza — o l'inesistenza — di un fatto. Ancora, l'art. 533 comma 1 c.p.p. àncora la pronuncia di una sentenza di condanna al rispetto del principio dell'"oltre ogni ragionevole dubbio", e a tal proposito si deve tener conto, come già rilevato a proposito della testimonianza, che tali sistemi di Intelligenza artificiale ragionano sulla base di una logica essenzialmente binaria, e difficilmente sono capaci di elaborare valutazioni di ampio respiro che solo la mente umana è in grado di effettuare. Infine, la Carta etica europea mette in guardia in merito al rischio che il funzionamento di questi software, benché non discriminatori, trascuri il fondamentale principio dell'individualizzazione della pena, favorendo invece teorie deterministiche.

Proprio queste perplessità, legate all'impiego dei sistemi di Intelligenza artificiale in questo secondo campo d'indagine, spiegano la ragione per la quale «[…] Nel 2018 l'uso di algoritmi di Intelligenza artificiale nei sistemi giudiziari europei rimane principalmente un'iniziativa commerciale del settore privato, rivolta a compagnie assicurative, uffici e studi legali, avvocati e privati»[7], sebbene dall'altro lato debba essere evidenziato come tali software, in virtù dei loro innegabili vantaggi, meritino di essere presi in seria considerazione anche nell'ambito pubblicistico della giustizia civile, commerciale e amministrativa per una risoluzione precontenziosa delle controversie online. Qualora il sistema giudiziario europeo sia evolvesse sino a tal punto, la *condicio sine qua non* perché ciò possa accadere si dovrebbe identificare, per esigenze di garanzia, nella predisposizione di un sistema di successivi ricorsi al giudice–uomo, affinché il progresso tecnologico in sede decisionale non infici le garanzie fondamentali del giusto processo.

(7) Carta etica europea sull'utilizzo dell'Intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi, adottata dalla CEPEJ nel corso della sua 31 Riunione plenaria, Strasburgo, 3–4 dicembre 2018.