# NUOVI STRUMENTI DI LOTTA ALL'ILLEGALITA', RIFLESSIONI NELL'ERA DELL'INTELLIGENZA ARTIFICIALE

*Elenia Esposito*


## Abstract

*Il presente contributo, ripercorre l'evoluzione in chiave preventiva del diritto penale in un contesto caratterizzato da un cambio di passo nei rapporti tra i servizi di intelligence, le forze di polizia e le autorità giudiziarie, nonché nell'uso nei procedimenti penali delle informazioni raccolte dalle agenzie di sicurezza. Partendo dalla presa di coscienza da parte dei governi degli indubbi vantaggi che l'intelligenza artificiale è in grado di apportare nel contrasto alla criminalità, lo scritto si sofferma sull'impiego degli algoritmi nelle operazioni di polizia. Su*

*quest'ultimo profilo si riflette, infine, sull'opportunità di un intervento legislativo che garantisca la conformità di tali strumenti ai diritti fondamentali dell'uomo.*

*This article explores the preventive evolution of criminal law against the backdrop of a significant transformation in the relationships between intelligence services, law enforcement agencies, and judicial authorities, as well as the use of intelligence information in criminal proceedings. Recognizing the undeniable advantages that artificial intelligence brings to crime prevention, the paper delves into the application of algorithms in policing operations. Finally it considers the need for legislative action to ensure that these technological tools align with fundamental human rights standards.*

# PREMESSA

L'affinarsi delle tecniche criminose ha richiamato l'attenzione degli Stati sulla necessità di rivedere i tradizionali strumenti utilizzati per tutelare i propri apparati dalle minacce che intaccano la sicurezza pubblica e l'assetto democratico.

Al fine di affinare le capacità operative i governi hanno dovuto attivarsi con tecniche sempre più sofisticate fino all'impiego dell'intelligenza artificiale (d'ora in avanti, anche "IA") che ormai dilaga in ogni ambito di competenza statale: dal settore militare e della sicurezza interna, a quello commerciale, all'ambito amministrativo e penale, alla lotta alla corruzione.

Invero, la digitalizzazione rappresenta il fulcro centrale di ogni politica di riforma contenuta nel PNRR[1], in quanto fattore trainante della trasformazione del nostro Paese che proprio in questo ambito ha accumulato nel corso degli anni un consistente ritardo, sia nell'adozione delle tecnologie digitali nel sistema produttivo e nei servizi pubblici, sia nelle competenze dei cittadini. La riduzione di questo deficit e la promozione di investimenti in tecnologie, infrastrutture e processi digitali, è essenziale per aumentare la competitività in Italia ed in Europa.

## 1. Un nuovo alleato per gli Stati: l'Intelligenza Artificiale. Pro e contra.

*"Siamo dieci volte più affascinati dalle imitazioni meccaniche che dai veri esseri umani che svolgono lo stesso*

*compito"*[2].

Frutto della quarta rivoluzione industriale, l'Intelligenza artificiale riveste ormai un ruolo di primo piano tra gli strumenti utilizzati dagli Stati per contrastare le insidie all'ordine e alla sicurezza pubblica. Ma cosa si intende per intelligenza artificiale?

Appare sin da subito opportuno chiarire che ad oggi, considerata la sua interdisciplinarità, non sembra possibile individuare una definizione univoca di "intelligenza artificiale"[3]. Trovando, infatti, applicazione in diversi ambiti - quali l'informatica, l'ingegneria, la filosofia, l'etica, la sociologia, il diritto - ogni disciplina tende a fornirne una definizione che più si adatti al proprio ambito di studio.

In via generale, l'intelligenza artificiale (IA) può essere definita approssimativamente come l'insieme dei metodi scientifici, delle teorie e delle tecniche che si prefiggono di emulare, mediante sistemi automatici, comportamenti intelligenti, tipici degli esseri umani[4].

Più specificamente l'università di Stanford l'ha definita come *"una scienza e un insieme di tecniche computazionali che vengono ispirate - pur operando tipicamente in maniera diversa - dal modo in cui gli esseri umani utilizzano il proprio sistema nervoso e il proprio corpo per sentire, imparare, ragionare e agire"*[5]. I sistemi di intelligenza artificiale si caratterizzano, infatti, per emulare il comportamento dell'essere umano: acquisiscono, in analogia con le funzioni cognitive umane, numerose informazioni sotto forma di dati ed eseguono compiti senza la necessità di una costante guida umana.

L'evoluzione tecnologica è giunta a dar vita ad un sistema di IA che - Prometeo dei tempi moderni[6] - rompe le catene dell'eterodirezione e, dotato di una propria intelligenza, è in grado di determinare il proprio comportamento rispondendo agli stimoli esterni, elaborando in maniera del tutto indipendente - attraverso algoritmi e reti neurali - i dati che incamera secondo modelli talvolta difficilmente intellegibili dall'uomo.

All'intelligenza artificiale si fa riferimento nella Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *"L'intelligenza artificiale per l'Europa"* del 25 aprile 2018, laddove si legge che *«"Intelligenza artificiale" (IA) indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi. I sistemi basati sull'IA possono consistere solo in software che*

*agiscono nel mondo virtuale (per esempio assistenti vocali, software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale); oppure incorporare l'IA in dispositivi hardware (per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle cose)».*

Il dilagare di forme di robotica intelligente ha determinato numerosi vantaggi sia in termini economici che di miglioramento della qualità della vita delle persone. Basti considerare l'enorme successo delle sperimentazioni in materia di auto a guida autonoma che, da prototipi semi-automatici, sono approdate a sistemi di guida totalmente *driverless*, con innumerevoli benefici. Si pensi soltanto alla possibilità di consentire la guida a soggetti disabili e alla prospettiva di ridurre drasticamente il numero degli incidenti stradali[7].

Tuttavia, oltre agli innumerevoli benefici, il dilagante sviluppo delle nuove tecnologie, ha comportato non pochi aspetti problematici, soprattutto quando gli stessi vengono impiegati in settori critici.

Ad esempio, nel campo della mobilità e dell'automatizzazione dei sistemi di trasporto una delle principali questioni è quella dell'individuazione di un centro di responsabilità in caso di danni provocati dalle IA, rispetto alla quale nei diversi ordinamenti è sempre più sentita l'esigenza di definire una nuova dimensione della responsabilità attraverso il superamento dei tradizionali canali legislativi e giurisprudenziali.

Analogamente l'impiego dei sistemi algoritmici applicati alla giustizia ha destato non pochi problemi applicativi per cui è emersa la necessità di vagliarli alla luce dei principi di equità e correttezza.

Tutto ciò in un panorama caratterizzato dalla generalizzata lentezza dei legislatori nazionali ad adeguare le normative vigenti al mutato assetto sociale ed economico determinato dall'evoluzione tecnologica.

## 2. L'evoluzione dell'attività di monitoraggio, le indagini digitali.

L'adozione crescente di tecnologie di intelligenza artificiale a supporto dei compiti statali si è spinta sino all'impiego degli algoritmi nelle operazioni di polizia[8]. Questi sviluppi si verificano in un contesto più ampio di cambiamenti: l'evoluzione del diritto penale verso un approccio più preventivo, il cambiamento nei rapporti tra i servizi di *intelligence*, le forze di polizia e le autorità giudiziarie, nonché nell'uso nei procedimenti penali delle informazioni raccolte dalle agenzie di sicurezza.

Quanto alla deviazione anticipatoria del diritto penale, seguendo l'esempio dei sistemi legali anglosassoni, anche negli ordinamenti giuridici di tipo continentale si è assistito a un'evoluzione[9]. In questi contesti, la linea di demarcazione tra le attività d'indagine (*investigating*) e quelle, in senso lato, di polizia (*policing*) si è notevolmente attenuata. In particolare, la polizia assume un ruolo più proattivo e autonomo nella gestione della criminalità, operando in modo indipendente dal controllo e dall'autorizzazione dell'Autorità giudiziaria[10]. Questa forma di attività di polizia, caratterizzata da una maggiore indipendenza, viene usualmente definita nei sistemi giuridici continentali come "sorveglianza". In questo sistema, ai compiti tradizionali di natura amministrativa, quali la garanzia dell'ordine pubblico e della sicurezza pubblica, si affiancano operazioni che mirano al controllo sociale o che sono tipicamente associate alle Agenzie di *intelligence*[11].

Tradizionalmente, la repressione del crimine si concentra sulla valutazione della condotta criminale e sulla raccolta di prove per stabilire la colpevolezza del reo. La prevenzione, invece, mira a impedire la realizzazione di crimini attraverso interventi anticipati. Questi due approcci, nel contesto moderno, tendono a convergere in un'unica fase di "indagini proattive". Tale fase si caratterizza per l'uso di tecniche operative che combinano sia la ricerca che il contrasto del crimine, per una crescente sovrapposizione tra il presupposto per l'avvio delle indagini preliminari rappresentato dalla *notitia criminis* e altre forme di sorveglianza.

Tra i cambiamenti che hanno coinvolto l'ordinamento giuridico italiano, influenzato in particolare dalla legislazione contro il terrorismo internazionale e il crimine organizzato, si rileva l'ampliamento dei poteri di controllo sociale integrati nelle indagini penali[12] e l'estensione dell'area della punibilità, anticipando la soglia di intervento a condotte preparatorie relative a gravi delitti.

Sotto quest'ultimo profilo un esempio emblematico è l'incriminazione di determinate condotte preparatorie agli attentati terroristici[13] e l'introduzione di misure di prevenzione speciale *ante* o *praeter delictum*. Queste misure, di natura formalmente amministrativa, sono adottate in situazioni di pericolosità per prevenire la commissione di reati, fungendo da ponte tra il diritto amministrativo e il diritto penale[14]. Di conseguenza, la pericolosità sociale di certi individui, valutata come indicatore della loro propensione a delinquere basata su un giudizio prognostico, diventa un fattore predittivo del rischio di commissione o reiterazione di illeciti da parte di un soggetto specifico.

In seguito a questi sviluppi, la formalità degli istituti giuridici diventa più sfumata, rendendo meno chiare le coordinate per la verifica di proporzionalità delle misure suscettibili di incidere sui diritti fondamentali. In particolare, non è definita a priori la gamma di individui che potrebbero essere soggetti a tali misure; rimane incerto lo scopo dell'intervento e sfugge a valutazioni chiare e concrete la relazione tra la gravità del fatto temuto o commesso, i requisiti necessari per l'intervento dell'autorità e l'importanza del bene individuale limitato. Questo porta a un'estrema flessibilità nei bilanciamenti, che a sua volta può ridurre le garanzie individuali[15].

Con riferimento all'uso dell'intelligenza artificiale (IA) a supporto delle attività di polizia, l'assottigliamento delle linee di demarcazione tra attività di *intelligence* e attività amministrativa/giudiziaria di polizia ha portato a un'estensione dei compiti delle forze dell'ordine. Queste, partendo dall'ambito della pubblica sicurezza, hanno incrementato la raccolta occulta di informazioni tramite metodi tradizionali e "indagini digitali"[16]. La raccolta di informazioni di quest'ultimo tipo avviene sia al di fuori delle garanzie del procedimento penale, mediante strumenti informatici per il controllo del territorio e algoritmi per il *data mining*, sia durante il procedimento, con l'impiego di vari dispositivi tecnologici[17]. Tra questi spicca il captatore informatico, o *trojan*, una sorta di *virus* o *malware* che, una volta inserito segretamente in un dispositivo informatico e attivato, può svolgere molteplici attività.

L'introduzione di nuove tecnologie di sorveglianza nel campo investigativo deriva, come si è visto, dal cambiamento dell'orientamento delle indagini penali, che si sposta dalla tradizionale repressione verso la prevenzione, soprattutto per contrastare gravi forme di criminalità. Questo implica un rafforzamento significativo dei poteri di controllo sulla collettività e un maggiore ricorso a metodi occulti di raccolta delle informazioni, utilizzando strumenti di sorveglianza più invasivi[18].

Riguardo alla possibilità di impiegare strumentazioni intrusive anche in fasi prive di garanzie procedurali, è importante sottolineare che l'attività di polizia di sicurezza, per motivi di efficacia[19], è molto meno regolamentata dalla legge rispetto alla fase delle indagini preliminari nella quale, invece, sono previsti criteri rigorosi per l'acquisizione di informazioni e prove. Se ciò non fosse, verrebbe compromessa l'efficacia nell'identificazione di soggetti in procinto di commettere un reato. Inoltre, gli stessi trattati internazionali che tutelano diritti e libertà nel contesto penale tendono a riferirsi specificatamente al procedimento penale e non alla fase di prevenzione. Di conseguenza, in quest'ultima, le garanzie previste per gli indagati, che si traducono in vincoli per le autorità, non trovano applicazione[20].

Tra le varie tecniche di prevenzione, l'impiego dell'intelligenza artificiale in questo ambito non è limitato da disposizioni procedurali specifiche. Piuttosto, le restrizioni si applicano alla selezione delle "fonti" di dati e informazioni utilizzabili per tali fini e al rispetto di alcuni principi fondamentali.

## 3. Il ruolo dell'IA nella prevenzione del crimine.

L'applicazione alle attività di polizia di nuove strumentazioni tecnologiche[21] ha condotto all'estensione delle capacità operative delle forze di polizia fino a giungere alla possibilità di prevedere le possibili condotte illecite.

Si è assistito all'affermazione della c.d. "polizia predittiva" (*predictive policing*) che è stata efficacemente definita come «*l'insieme delle attività rivolte allo studio e all'applicazione di metodi statistici con l'obiettivo di "predire" chi potrà commettere un reato, o dove e quando potrà essere commesso un reato, al fine di prevenire la commissione dei reati stessi*»[22].

La diffusione della polizia predittiva si inserisce in quel filone volto a superare la concezione dell'attività di polizia come meramente repressiva, a vantaggio di una configurazione anche preventiva, e costituisce uno dei fattori che ha portato all'accrescimento del ruolo delle attività di *intelligence* – intese come ricerca e raccolta di informazioni – accanto alle tradizionali operazioni di polizia.

I dispositivi di polizia predittiva si dividono sostanzialmente in due categorie: sistemi che «*ispirandosi alle acquisizioni della criminologia ambientale, individuano le c.d. "zone calde" (hotspot), vale a dire i luoghi che costituiscono il possibile scenario dell'eventuale futura commissione di determinati reati*»[23]; e sistemi di «*crime linking*» (connessione criminale) che, sulla base di dati investigativi, raccolti sul *locus commissi delicti* «*seguono le serialità criminali di determinati soggetti (individuati o ancóra da individuare), per prevedere dove e quando costoro commetteranno il prossimo reato*»[24].

Ebbene, l'impiego degli strumenti di IA in questo ambito consente, tramite l'elaborazione ed estrazione di informazioni utili dall'enorme mole di dati disponibili, la rilevazione di «*connessioni prima difficilmente individuabili dall'operatore umano*»[25] (*data mining*).

Le tecniche di polizia predittiva più recenti, dunque, sulla base di dati raccolti attraverso fonti diverse e

l'incrocio degli stessi, mediante algoritmi, consentono di prevenire il compimento di specifici reati oggetto della statistica e la loro localizzazione nonché di elaborare profili criminali individuali.

In questo contesto si inserisce la recente sperimentazione di un nuovo sistema di polizia predittiva che il Ministero dell'Interno vorrebbe dare in dotazione alle Questure di tutta Italia. Si tratta del c.d. sistema "Giove", un *software* di elaborazione e analisi automatizzata (basato su un algoritmo di intelligenza artificiale) per l'ausilio delle attività di polizia che potrebbe essere in grado di indicare dove e quando è probabile si verifichino determinati tipi di reato, in base ai dati del passato, così da "prevenire e reprimere" i reati di maggior impatto sociale.

Questo sistema, nato nel Dipartimento di pubblica sicurezza del Ministero dell'Interno nel 2020, sulla base delle sperimentazioni portate avanti dalla questura di Milano a partire dal 2008, dovrebbe essere in grado di analizzare migliaia di dati riguardanti dove sono stati compiuti i reati, a che ora, in che modo, il comportamento e i mezzi usati dai responsabili e altro ancora, il tutto per mettere in correlazione diversi crimini e determinare quali sono stati compiuti dagli stessi soggetti o dallo stesso soggetto.

Pertanto, diversamente dai sistemi *hotspot*, questo sistema non andrebbe a segnalare aree con alta incidenza di reati andando a criminalizzare le zone stesse senza risolvere il problema, ma punterebbe alla ricerca di comportamenti ripetuti che possano condurre ai responsabili.

In merito a tale sistema, tuttavia, restano i comuni dubbi e i rischi legati all'utilizzo dell'IA nel campo della prevenzione dei reati. Si tratta, in particolare, della difficoltà di individuare con certezza dei *modus operandi* che possano effettivamente collegare un reato a un altro senza il rischio di cadere in errori dovuti ai pregiudizi algoritmici legati in particolare all'etnia e alla provenienza geografica delle persone. Inoltre, l'uso di un sistema del genere potrebbe comportare una violazione del rispetto alla *privacy* e delle libertà personali degli individui ed è per questo che un intervento del Garante della *privacy* risulterebbe fondamentale.

Invero, trattandosi in buona sostanza di tecniche che si inquadrano nel più ampio contesto della «*sorveglianza statale sugli individui per fini di sicurezza pubblica e nazionale*»[26] non pochi interrogativi sono sorti circa l'utilizzo di questi nuovi sistemi e le possibili ricadute che il controllo sociale, determinato dall'analisi continua di dati eterogenei e generati in tempo reale, può avere sulle libertà fondamentali e su aspetti importanti quali appunto la *privacy*, nonché il rischio di discriminazione e la presunzione di innocenza[27].

Di tali criticità sono ben consapevoli, tra l'altro, gli stessi operatori del settore.

Invero, tenuto conto della capillare diffusione dei sistemi informatici basati sull'IA nell'ambito della sicurezza interna degli Stati, dal 2018 annualmente si tiene un incontro mondiale sul tema[28] organizzato dall'INTERPOL[29] in collaborazione con l'Istituto Interregionale delle Nazioni Unite per la Ricerca sul Crimine e la Giustizia (UNICRI[30]) per esaminarne i risvolti positivi e negativi e delineare delle linee guida etiche per il loro sviluppo.

Come si legge nel report dell'INTERPOL-UNICRI sull'Intelligenza Artificiale per le forze dell'ordine del 2020, infatti, «*se da un lato c'è un grande potenziale nell'IA, dall'altro l'uso di questa tecnologia da parte delle forze di polizia solleva anche preoccupazioni molto reali e serie sui diritti umani, che possono essere estremamente dannose e minare la fiducia che le comunità ripongono nelle forze di polizia. I diritti umani, le libertà civili ed anche i principi fondamentali di legge sui quali si basa il nostro sistema di giustizia penale potrebbero essere inaccettabilmente esposti o anche irreparabilmente compromessi, se non intraprendiamo questo cammino con estrema cautela*»[31].

Pur di fronte all'evidenza di tali rischi, è generalizzato il convincimento che al fine di fronteggiare le diffuse minacce alla sicurezza dei cittadini e alla stabilità dell'ordinamento è necessario inasprire la risposta punitiva anche per mezzo del ricorso a straordinari strumenti normativi e strumentazioni informatiche molto invasive[32]. Il bilanciamento tra esigenze di libertà e di sicurezza deve necessariamente avvenire in maniera tale da non intaccare i livelli minimi di tutela da considerarsi irrinunciabili, al di sotto dei quali le attività di prevenzione non appaiono più proporzionate all'obiettivo e, dunque, accettabili[33].

# CONCLUSIONI

Tra gli strumenti preventivi messi a punto dagli Stati per reagire al costante affinarsi delle tecniche criminose, sempre maggiore rilievo stanno assumendo le moderne tecnologie e, dunque, l'intelligenza artificiale.

L'utilizzo dei sistemi di IA può ritenersi utile per supportare gli operatori del diritto in diversi settori: dalla giustizia, coadiuvando il giudice in ogni fase del processo, ivi compresa l'adozione di decisioni elementari e

standardizzate, consentendogli di smaltire enormi moli di lavoro in tempi celeri; alla polizia predittiva, permettendo di anticipare la commissione di reati e, in alcuni casi, l'arresto in flagranza del reo; al contrasto della corruzione, attraverso la prevenzione dei reati corruttivi tramite la rilevazione anticipata dei sintomi di infedeltà; alla lotta all'evasione fiscale, dove l'algoritmo, attraverso l'incrocio di dati provenienti da diverse banche dati, consente di selezionare le posizioni dei contribuenti verso cui avviare un'attività istruttoria.

Tuttavia, l'impiego dei sistemi di IA in quest'ambiti così complessi richiede studi approfonditi e accorte sperimentazioni volti a garantire che lo stesso sia conforme ai principi fondamentali degli ordinamenti ed in particolare a quello di equità.

Per quanto concerne gli strumenti di polizia predittiva, sebbene sussistano al riguardo delle criticità in merito alla loro concreta applicazione, le stesse non possono certamente considerarsi un limite assoluto al loro utilizzo; dovendosi piuttosto contrastare determinate modalità operative (come, ad esempio, i dispositivi di "*hotspot*") e regolamentare correttamente l'utilizzo dei dati al fine di evitare che gli stessi siano viziati, per poterli così impiegare anche nell'esercizio delle attività di polizia giudiziaria e, in un'ultima analisi, a fondamento delle decisioni giudiziarie.

Come si è visto, infatti, l'utilizzo di algoritmi predittivi nell'ambito dell'attività di polizia giudiziaria, infatti, può certamente portare ad anticipare la commissione di reati e, in alcuni casi, a favorire l'arresto in flagranza del reo. D'altra parte, non si ritiene che sussista il pericolo che attraverso l'impiego di tali sistemi si arrivi a punire la mera volontà criminale al di là e a prescindere da un disvalore prima oggettivo e poi soggettivo. In questo senso, invero, fungono da veri e propri argini i principi di materialità e offensività, i quali richiedono che affinché una fattispecie di reato risulti integrata è necessario che sussista un fatto che offenda o, quantomeno, metta in pericolo il bene giuridico tutelato dalla norma incriminatrice[34].

In ogni caso, è necessario che i risultati dell'elaborazione algoritmica siano compatibili con le regole che governano l'acquisizione delle prove nel processo penale. Da questo punto di vista, viene certamente in soccorso l'art. 189 c.p.p. sulle prove atipiche, secondo cui possono essere assunte dal giudice prove non disciplinate dalla legge (dunque anche gli esiti dei calcoli matematici di un programma informatico) laddove risultino idonee ad assicurare l'accertamento dei fatti, non pregiudichino la libertà morale della persona e, secondo quanto stabilito dagli artt. 6 e 8 della CEDU, vengano garantiti il diritto ad un equo processo e il diritto al rispetto della vita privata e familiare. Pertanto, qualora vengano rispettati i parametri di cui sopra nonché, ovviamente, i diritti inviolabili dell'uomo di cui all'art. 2 Cost. e, i risultati in parola potranno essere

oggetto di valutazione ai sensi dell'art. 192 c.p.p.

Ciò posto, al fine di evitare che l'utilizzo delle prove raccolte per mezzo di algoritmi venga lasciato esclusivamente all'interpretazione degli operatori giudiziari e che lo stesso si traduca in atti contrari ai principi costituzionali, è auspicabile che il legislatore introduca una disciplina volta ad individuare un equilibrio tra gli interessi in gioco, ad esempio anche prevedendo una preventiva autorizzazione giurisdizionale allo svolgimento di determinate attività di indagine.

---

[1] Il PNRR, acronimo di Piano Nazionale di Ripresa e Resilienza, è il documento strategico contenente un pacchetto di investimenti e riforme che il Governo italiano ha predisposto per accedere ai fondi del programma *Next generation EU (NGEU)*. Approvato il 13 luglio 2021, con Decisione di esecuzione del Consiglio, che ha recepito la proposta della Commissione europea, rilanciare il Paese dopo la crisi pandemica, stimolando una transizione ecologica e digitale, ha lo scopo di favorire un cambiamento strutturale dell'economia, a partire dal contrasto alle diseguaglianze di genere, territoriali e generazionali.

[2] In questi termini, P. MCCORDUCK, *Storia dell'Intelligenza Artificiale. Gli uomini, le idee, le prospettive*, Franco Muzzio Editore, Padova, 1987, p. 10.

[3] Sull'assenza di una definizione di IA, *ex multis*, M.B. MAGRO, *Biorobotica, robotica e diritto penale*, in D. PROVOLO, S. RIONDATO e F. YENISEY (a cura di), *Genetics, Robotics, Law, Punishment, Padova University Press*, 2014, p. 508 (reperibile su: https://discrimen.it/wp-content/uploads/Provolo-Riondato-e-Yenisey-a-curadi-Genetics-Robotics-Law-Punishment.pdf, S. SIGNORATO, Giustizia penale e intelligenza artificiale. Considerazioni in tema di algoritmo, in Rivista di Diritto Processuale, n. 2/2020, p. 605; F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in Diritto Penale e Uomo (DPU), 2019, n. 10, p. 4 (reperibile su: principale https://dirittopenaleuomo.org/wpcontent/uploads/2019/09/IA-dirittopenale.pdf, oppure al collegamento secondario https://archiviodpc.dirittopenaleuomo.org/upload/3089-basile2019.pdf).

[4] Nel sito web del Consiglio d'Europa è indicata la seguente definizione: «*Un insieme di scienze, teorie e tecniche il cui scopo è quello di riprodurre, attraverso la macchina, le capacità cognitive di un essere umano. Gli sviluppi attuali mirano ad affidare a una macchina compiti complessi precedentemente svolti da esseri umani*» (reperibile su: https://www.coe.int/en/web/artificial-intelligence/glossary).

[5] Stanford University. 2016. *Artificial Intelligence and life in 2030, One hundred year study on Artificial Intelligence*, p. 4 (https://ai100.stanford.edu/sites/g/files/sbiybj18871/files/media/file/ai100report10032016fnl_singles.pdf).

[6] E ESPOSITO, *Prometeo 2.0 Verso una disciplina europea dell'Intelligenza Artificiale* in i-lex Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale. Disponibile su: http://www.i-lex.it/index.php/volume-14/fascicolo-1-ai-and-fairness/79-prometeo-2-0

[7] Uno degli esempi più diffusi di intelligenza artificiale è, difatti, l'auto a guida autonoma, ovvero un veicolo che, attraverso diversi dispositivi come radar, lidar, GPS, telecamere e sensori e di sistemi di rilevamento dell'ambiente circostante, è in grado di avanzare compiendo autonomamente le attività tipiche del guidatore. Ad oggi si distinguono sei livelli di automazione degli autoveicoli, individuati sulla base della classificazione predisposta dalla SAE (*Society of Auto-motive Engineers*). Si passa dal livello 0, che corrisponde alla completa assenza di sistemi di automazione, per passare progressivamente ai veicoli che presentano alcuni livelli di automazione (driver assistance, partial automation), in cui però il controllo del veicolo rimane in capo al guidatore, fino ad arrivare ai sistemi con *high* o *full automation*, questi ultimi a guida totalmente autonoma.

[8] Cfr., W. NOCERINO, *Le nuove tecniche di investigazione proattiva e le ricadute processuali (Prima parte)*, op. cit., pp. 821-827 e, *Le nuove tecniche di investigazione proattiva e le ricadute processuali (Seconda parte)*, op. cit., pp. 1020-1031. Invece, sul secondo punto, brevemente, D. BENEDETTI, *IA e (in)sicurezza informatica*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli Editore, Torino 2018, pp. 253-255.

[9] Circa i rapporti tra prevenzione e repressione, cfr. S. SIGNORATO, *Le indagini digitali*, op. cit., pp. 318-321.

[10] Ad esempio, le forze di polizia di Stati Uniti d'America ed Inghilterra conducono le indagini fino alla richiesta di rinvio a giudizio dell'indagato.

[11] Si veda S. QUATTROCOLO*, Equità del processo penale e automated evidence alla luce della Convenzione Europea dei Diritti dell'Uomo, in Revista italo-española de Derecho Procesal, vol. 1, 2019, pp. 107-123.*, p. 110; S. QUATTROCOLO, *Artificial Intelligence, Computational modelling and Criminal Proceedings: A Framework for a European Legal Discussion*, Springer, 2020, p. 37.

[12] In questi termini, D. NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, in *Archivio Penale*, n. 1/2016, p. 44.

[13] Tra queste si segnalano: il reclutamento, l'addestramento, il trasporto, il finanziamento o la fornitura di equipaggiamento a soggetti che si spostano verso Stati diversi da quelli di propria nazionalità, al fine di commettere, organizzare o partecipare ad atti di terrorismo (artt. 270-*quater* e ss., c.p.).

[14] La normativa italiana di riferimento per le misure di prevenzione è il d.lgs. 159/2011 (Codice delle leggi antimafia e delle misure di prevenzione), ma previsioni ulteriori si rinvengono altresì nella legislazione speciale.

[15] In questi termini, D. NEGRI, *ult. cit.*, p. 46.

[16] Vedi, S. SIGNORATO, *Le indagini digitali*, op. cit., p. 44.

[17] Quali, ad esempio, i programmi che indentificano un soggetto a partire da un fotogramma messo a confronto con i dati già in possesso delle forze di polizia o con le telecamere di sorveglianza. Il *software* utilizzato dalla Polizia di Stato italiana è il SARI (Sistema Automatico di Riconoscimento Immagini). Sui sistemi di IA utilizzati dalle forze di polizia italiane, vedasi V. GUARRIELLO, *I sistemi di intelligenza artificiale in uso alle Forze dell'Ordine in Italia*, in www.salvisjuribus.it, 10 maggio 2020 (reperibile su: http://www.salvisjuribus.it/i-sistemi-di- intelligenza-artificiale-in-uso-alle-forze-dellordine-in-italia/).

[18] In questi termini, F. NICOLICCHIA, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *Diritto Penale Contemporaneo*, fasc. n. 2/2018, p. 177 (reperibile su: https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/nicolicchia.pdf).

[19] In inglese «*for reasons of effectiveness*» S. QUATTROCOLO, *Artificial Intelligence, Computational modelling and Criminal Proceedings*, op. cit., p. 38.

[20] Cfr. *Eadem,* p. 38.

[21] Cfr., L. PASCULLI, *Genetics, robotics and crime prevention*, in D. PROVOLO – S. RIONDATO – F. YENISEY (a

cura di), *Genetics, Robotics, Law, Punishment*, Padova University Press, 2014, pp. 187-203.

[22] F. BASILE, *Intelligenza artificiale e diritto penale*, op. cit., p. 10.

[23] *Ivi*, p. 11.

[24] *Idem*.

[25] Così, F. BASILE, Intelligenza artificiale e diritto penale, op. cit., p. 10.

[26] In questi termini, A. BONFANTI, *Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla* privacy *e dei dati personali*, in www.medialaws.eu (*Rivista di diritto dei media*), n. 3/2018, pp. 208-209 (reperibile su: https://air.unimi.it/retrieve/handle/2434/605891/1116513/bonfanti%20-%20medialaws%202018.pdf e al collegamento secondario https://www.medialaws.eu/rivista/big-data-e-polizia-predittiva-riflessioni-in-tema-di- protezione-del-diritto-alla-privacy-e-dei-dati-personali/).

[27] In argomento, *ex multis*, J. KREMER, *The End of Freedom in Public Places? Privacy problems arising from surveillance of the European public space*, 2017, in particolare il cap. 3.4.2, "Prediction", pp. 269-272 (reperibile su: https://helda.helsinki.fi/handle/10138/176300,) e A. ZAVRŠNIK (a cura di), *Big Data, crime and social control*, Routledge – Taylor & Francis Group, 2018.

[28] Vedasi Rapporti INTERPOL – UNICRI, *Artificial Intelligence and Robotics for Law Enforcement*, 2019 (reperibile su: http://www.unicri.it/index.php/artificial-intelligence-and-robotics-law- enforcement) e *Towards Responsible Artificial Intelligence Innovation*. *Second INTERPOL-UNICRI Report on Artificial Intelligence for Law Enforcement*, 2020.

[29] The International Criminal Police Organization – INTERPOL.

[30] United Nations Interregional Crime and Justice Research Institute.

[31] INTERPOL – UNICRI, *Towards Responsible Artificial Intelligence Innovation*. op. cit., pp. 3-4.

[32] Con riferimento all'ambito penale vedasi, W. NOCERINO, *Le nuove tecniche di investigazione proattiva e le ricadute processuali (Prima parte)*, in *Studium Iuris*, n. 7-8/2020, p. 821.

[33] In questi termini, W. NOCERINO, *Le nuove tecniche di investigazione proattiva e le ricadute processuali (Seconda parte)*, in *Studium Iuris*, n. 9/2020, p. 1030. Sul rapporto tra prevenzione e libertà, si veda anche S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, pp. 313-317.

[34] In questi termini, D. POLIDORO, *Tecnologie informatiche e procedimento penale: la giustizia penale "messa alla prova" dall'intelligenza artificiale*, in *Archivio penale*, n. 3/2020, p. 10.