LUISS

Dipartimento di Giurisprudenza

Cattedra Metodologia della Scienza giuridica

Polizia predittiva: un'analisi critica di possibili sviluppi e limiti

Prof. Antonio Punzi
RELATORE

Prof. Ludovico Ercole
CORRELATORE

Allegra Peloni
Matr. 146813
CANDIDATO

Anno Accademico 2021 / 2022

A mia mamma, l'altra metà del mio cuore.
"Ho sceso, dandoti il braccio, almeno un milione di scale
e ora che non ci sei è il vuoto ad ogni gradino".

Indice

INTRODUZIONE

Il progresso tecnologico e la costante introduzione di nuove forme di tecnologia hanno apportato ingenti cambiamenti riscontrabili in ogni ambito della nostra vita: dal settore militare, luogo privilegiato per l'implementazione delle stesse, a quello del settore commerciale. L'intelligenza artificiale (d'ora in poi IA) pervade quindi il nostro vivere quotidiano al punto da prefigurare una società "algoritmica" che sancisce la definitiva transazione nell'era digitale. Le applicazioni basate sull'IA sono molteplici: è un algoritmo a suggerire i prodotti che potremmo apprezzare maggiormente durante gli acquisti online; a permettere ad un veicolo di spostarsi senza conducente; a suggerire il percorso più breve per giungere a destinazione. Tutte manifestazioni che semplificano notevolmente le nostre attività quotidiane. Si pensi alla recente *ChatGPT*, un modello di IA ad ampio spettro, capace di elaborare il linguaggio naturale in modo avanzato e di generare testo coerente e comprensibile.

Anche in ambito penale si riscontra ormai da anni l'utilizzo di strumentazioni digitali nel tentativo di migliorare l'ordine pubblico e l'efficacia delle indagini digitali, finalizzate alla repressione dei reati.

Tuttavia, con lo sviluppo e l'utilizzo di dispositivi di intelligenza artificiale, che cercano di emulare le attività umane, nuove opportunità e, soprattutto, nuovi interrogativi sono emersi per gli operatori del diritto. Se prima la discussione verteva sulla conformità dei nuovi mezzi di ricerca della prova ai tradizionali principi ordinamentali, ora, vista la disponibilità di dispositivi di polizia predittiva e algoritmi in grado di affiancare il giudice nella propria attività di *ius dicere*, l'attenzione si è posta anche sulla violazione dei diritti costituzionalmente garantiti e sull'esercizio della giurisdizione.

Le potenzialità e versatilità di questi strumenti permettono alle attività di prevenzione dei reati comuni di essere più incisive rispetto alle tradizionali misure di pattugliamento del territorio, ma causano inedite compressioni dei diritti tradizionali e pongono dinanzi la necessità di prevedere particolari tutele. È fondamentale, dunque, che gli operatori pubblici, in collaborazione con i soggetti privati e i ricercatori, diano delle linee guida per garantire che gli strumenti di IA rispettino la dignità umana ed operino sempre in relazione ai bisogni dell'uomo, il quale deve rimanere il fulcro dell'ordinamento giuridico.

Dunque, nel seguente lavoro di tesi si approfonditi gli aspetti riguardanti la polizia predittiva, i suoi sviluppi e le criticità.

Nel primo capitolo del presente lavoro, innanzitutto, si forniranno le definizioni utili per la comprensione della materia trattata, con particolare riferimento al concetto di IA. In seguito, verrà analizzato il fenomeno della polizia predittiva nel suo insieme. Si tratta di una tecnica di polizia che, mediante la combinazione dell'uso di tecniche analitico-statistiche e di algoritmi predittivi, consente di prevenire la futura commessione di un crimine, individuarne l'autore, il luogo e il tempo, al fine di evitare la commessione del reato stesso. Tali sistemi di *predictive policing*, nascono e si sviluppano con lo scopo ultimo di contrastare il fenomeno della criminalità, agevolare l'attuazione delle politiche volte a garantire la sicurezza urbana e più in generale la sicurezza della collettività, in modo da massimizzare l'allocazione delle risorse a disposizione delle forze dell'ordine. Il lavoro prosegue con una descrizione dei principali sistemi predittivi utilizzati nel panorama americano ed europeo, quali Pred Pol, SIMSI, Crime anticipation system, PreCobs e harm. Un focus maggiore è stato attribuito ai software americani poiché è a questi ultimi che si deve attribuire il merito di aver creato il primo algoritmo utilizzato dalle forze di polizia. Proseguendo poi con un'analisi dell'algoritmo Keycrime, ideato ma M. Venturini ex capo della questura di Milano, e XLAW, ideato da E. Lombardo ex ispettore superiore della Polizia di stato in uso in Italia ed al loro inquadramento normativo.

Nel secondo capitolo si presenta la distinzione, fondamentale per la comprensione del lavoro, tra la funzione di polizia di sicurezza e polizia giudiziaria. La prima ha carattere preventivo, in quanto è tesa ad impedire qualunque violazione dell'ordine sociale. La seconda, invece, ha carattere repressivo.

Nel presente capitolo viene quindi analizzata la polizia predittiva in relazione alla sicurezza pubblica, analisi che genera non pochi interrogativi, soprattutto riguardo la concreta utilizzabilità o meno degli algoritmi di polizia predittiva. Prevenire il compimento dei reati attraverso l'utilizzo di elaboratori automatici, fa sorgere numerose implicazioni e preoccupazioni riguardanti i diritti dell'individuo. Ci si riferisce prevalentemente: alla privacy, a causa della grande mole di dati trattati ed alla loro tipologia e qualità; le correlate problematiche riguardanti la profilazione degli individui; la mancanza di trasparenza, nonché la difficoltà di individuare quale sia l'esatto

funzionamento degli algoritmi in modo da assicurarne un controllo efficacie. L'ambito di applicabilità dei software in esame viene analizzato ai sensi della Diretta (UE) 2016/680 (GDPR).

Infine, nel terzo ed ultimo capitolo del lavoro, l'obiettivo è quello di verificare se e secondo quali parametri i dati frutto dell'elaborazione o della captazione algoritmica possono fare il loro ingresso nel processo penale ed essere utilizzati a fondamento di una decisione giudiziale.

In questo capitolo si analizza il dibattito innescato a seguito della rivoluzionaria modifica dell'attuale assetto dell'intero sistema penale che l'interferenza dell'IA ha in parte già comportato e comporterà. Il tema viene affrontato attraverso una tripartizione degli algoritmi. In primo luogo, si discute dell'utilizzo dei c.d. *risk assassment tools*, ossia algoritmi predittivi volti a computare il rischio di recidiva dell'imputato o più in generale la sua pericolosità sociale, quali strumenti di sussidio per il giudice nella determinazione della pena o nell'applicazione di altri istituti. Successivamente, si discute della prova fondata sull'Ia, ossia dell'utilizzo di strumenti di riconoscimento facciale e captatori informatici. Infine, viene affrontato il tema della responsabilità penale dei sistemi intelligenti.

In definitiva, l'elaborato si pone in prospettiva critica, ma non preclusiva rispetto alle recenti aperture del mondo giudiziario degli strumenti di intelligenza artificiale. L'obbiettivo primario è richiamare l'attenzione sulle violazioni che tali strumenti possono determinare per i diritti fondamentali e sui possibili sviluppi volti a cambiare e migliorare l'operare delle forze di polizia e del sistema penale nel suo insieme.

1. La Polizia Predittiva

1.1. Polizia predittiva e nuove tecnologie

«Insieme di attività e di forze impiegate nello studio e nell'applicazione di metodi statistici volti ad anticipare i criteri grazie alla combinazione di diversi tipi di dati, tra cui quelli relativi a notizie di reati precedentemente commessi o profili dei sospettati presenti nei siti di relazione sociale»[1]

Questa la definizione di Polizia Predittiva riportata nell'Enciclopedia Treccani.

Se nel film di Steven Spielberg *«Minority Report»*[2] la prevenzione dei reati sembrava essere solo uno scenario distopico, oggi sembra avvicinarsi alla realtà più di quanto avremmo mai potuto ipotizzare.

Nel nostro ordinamento non è presente una definizione chiara ed univoca di polizia predittiva.

Questa può essere descritta come la raccolta e l'analisi di dati riguardante reati pregressi, al fine di svolgere un'identificazione ed una previsione statistica su agenti o aree geo-spaziali all'interno delle quali vi è una maggiore probabilità di criminalità; ciò per aiutare a sviluppare interventi di polizia, strategie e tattiche di prevenzione[3].

La caratteristica principale della P.P. è l'uso di una quantità molto ampia di dati. Attraverso analisi descrittive ed elaborazioni di questi ultimi, si riescono, in parte, a comprendere le tendenze della criminalità.

Una seconda caratteristica chiave è la connessione con la funzione di prevenzione posta in essere dalle forze di polizia. Le forze dell'ordine anticipano il verificarsi di alcuni crimini, agendo in via preventiva.

Ovviamente per poter analizzare un così ampio spettro di dati è necessario l'utilizzo di algoritmi. Più specificatamente i sistemi di Polizia Predittiva operano attraverso sistemi

[1] Polizia Predittiva, in *Treccani.it – Enciclopedia on line*, Istituto dell'Enciclopedia Italiana, 2017.

[2] Minority Report è un film del 2002 diretto da Steven Spielberg, liberamente tratto dall'omonimo racconti di fantascienza di Philip K. Dick «Rapporto di minoranza», scritto nel 1956. Lo scrittore americano aveva immaginato uno scenario in cui i poliziotti della «Precrime», tramite un *software* particolare, riuscivano ad individuare con largo anticipo chi avrebbe commesso un crimine ed arrestarlo prima che questo venisse commesso.

[3] A. Meijer, M. Wessels, *Predictive Policing: Review of Benefits and Drawbacks*, in International Journal of Public Administration, 2019, v. 42, p. 1031.

di «*Machine Learning*»[4] che appartengono alla più ampia categoria dell'Intelligenza Artificiale.

Prima di specificare i concetti sopradetti e per meglio comprenderli, andiamo ad identificare il concetto di algoritmo. Il termine designa qualunque schema o procedimento sistematico di calcolo[5].

«*In informatica si definisce algoritmo una sequenza finita di operazioni elementari, eseguibili facilmente da un elaboratore che, a partire da un insieme di dati I (input), produce un altro insieme di dato O (output) che soddisfano un preassegnato insieme di requisiti*»[6].

L'algoritmo, unità di funzionamento dei software, può essere definito come un insieme preciso di istruzioni o regole, o come una serie metodica di passaggi che possono essere utilizzati per fare calcoli, risolvere problemi e prendere decisioni. Le tre caratteristiche dell'algoritmo sono state individuate nella capacità di risolvere sempre il problema che viene posto, di risolverlo in modo univoco ed in un numero finito di passaggi[7].

In conclusione, possiamo affermare che per algoritmo si intende una successione di istruzioni o passi che definiscono la sequenza delle operazioni di calcolo da eseguire sui dati per ottenere determinati risultati.

In secondo luogo, inquadriamo il concetto di Intelligenza Artificiale (IA).

L'espressione intelligenza artificiale viene utilizzata per la prima volta da John McCarthy[8], quest'ultimo organizzò, nel 1955, insieme ad altri colleghi, un convegno sull'intelligenza artificiale descrivendola in questi termini «*The study is to proceed on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely decribed that a machine can be made to simulate it. An attempt will be made to find how to make machines use language, form abstractions and concepts, solve kinds of problems now reserved for humans, and improve themselves*»[9].

---

[4] Il machine Learning (ML) è una sottocategoria dell'intelligenza artificiale, che si riferisce al processo tramite il quale i computer sviluppano il riconoscimento dei modelli, o la capacità di apprendere continuamente ed effettuare previsioni utilizzando i dati per poter apportare modifiche in autonomia, senza una programmazione specifica.

[5] Algoritmo, in *Treccani.it – Enciclopedia on line,* Istituto dell'Enciclopedia Italiana.

[6] Algoritmo In Informatica, in *Treccani.it – Enciclopedia on line,* Istituto dell'Enciclopedia Italiana.

[7] M.G. Losano, *Corso di Informatica Giuridica*, in Unicopli, Milano, 1983, Vol 1, p. 321.

[8] Famoso informatico statunitense, all'epoca era assistente universitario di matematica al Dartmouth College di Hanover, New Hamphsire. Nel 1971 ha vino il Premio Turing per i suoi contributi nel campo dell'intelligenza artificiale.

[9] «*Lo studio procederà sulla base della congettura che tutti gli aspetti dell'apprendimento o qualsiasi altra caratteristica dell'intelligenza possa essere di principio descritta in modo così preciso che una macchina*

In seguito, l'ingegnere Marco Somalvico la definì come «*una disciplina appartenente all'informatica che studia i fenomeni teorici, le metodologie e le tecniche che consentono la progettazione di sistemi hardware e sistemi di programmi software capaci di fornire all'elaboratore elettrico prestazioni che, ad un osservatore comune, sembrerebbero di pertinenza esclusiva dell'intelligenza umana*»[10].

Quindi l'IA è la scienza che studia se ed in che modo si possano riprodurre i processi mentali più complessi mediante l'uso del computer; nel settore dell'informatica invece, quest'ultima studia la possibilità di costruire computer che siano in grado di riprodurre il funzionamento di alcune capacità della mente umana o, nel caso della così detta intelligenza artificiale forte, dell'intero pensiero umano[11].

Oltretutto possiamo ricavare una definizione normativa di Intelligenza artificiale attraverso una comunicazione della Commissione Europea dalla quale si evince che:

«*Per "Intelligenza Artificiale" (IA) si intendono quei sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere obbiettivi specifici. I sistemi basati sull'IA possono consistere solo in software che agiscono in modo virtuale, oppure incorporare l'IA in dispositivi hardware*»[12].

Partendo da questa definizione, il Gruppo indipendente di 52 esperti ad alto livello, nominato dalla Commissione Europea al fine di svolgere funzioni di consulenza sull'intelligenza artificiale, ha elaborato un documento[13] in cui formula la seguente definizione di «sistemi di IA», affermando che sono tali:

«i sistemi *software* (ed eventualmente *hardware*) progettati dall'uomo che, dato un obbiettivo complesso, agiscono nella dimensione fisica o digitale percependo il proprio ambiente attraverso l'acquisizione di dati, interpretando i dati strutturati o non strutturati raccolti, ragionando sulla conoscenza o elaborando le informazioni derivate da questi dati

---

la possa simulare. Si tenterà di scoprire come si possa fare in modo che le macchine usino il linguaggio, formulino astrazione e concetti, risolvano tipi di problemi ora riservati agli esseri umani, e migliorino sé stesse». In tal senso, J. McCarty, M.L. Minsky, N. Rochester, C.E. Shannon, "*A proposal for the Dartmouth summer research project on artificial intelligence"*, in Dartmouth College, 1955.

[10] M. Smolvico, F. Amigoni, V. Schiaffonati, *Intelligenza artificiale*, in https://amigoni.faculty.polimi.it/teaching/IntelligenzaArtificiale.pdf, p. 1.

[11] Intelligenza artificiale, in *Treccani.it – Enciclopedia on line*, Istituto dell'Enciclopedia Italiana.

[12] Comunicazione della Commissione Europea al Parlamento Europeo, al Consiglio Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, Piano coordinato sull'intelligenza artificiale, 2018, Bruxelles.

[13] Il documento è intitolato: «*una definizione di IA: principali capacità e discipline scientifiche*», in https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai, 2019.

e decidendo le migliori azioni da intraprendere per raggiungere l'obiettivo dato. I sistemi di IA possono usare regole simboliche o apprendere un modello numerico, e possono anche adattare il loro comportamento analizzando gli effetti che le loro azioni precedenti hanno avuto sull'ambiente.

Come disciplina scientifica, l'IA comprende diversi approcci e diverse tecniche, come l'apprendimento automatico (di cui l'apprendimento profondo e l'apprendimento per rinforzo sono esempi specifici), il ragionamento meccanico (che include la pianificazione, la programmazione, la rappresentazione delle conoscenze e il ragionamento, la ricerca e l'ottimizzazione) e la robotica (che comprende il controllo, la percezione, i sensori e gli attuatori e l'integrazione di tutte le altre tecniche nei sistemi ciberfisici)»[14].

Quindi il termine Intelligenza Artificiale deve essere inteso quale termine generico, riguardante un'ampia gamma di tecnologie, tecniche ed approcci che devono meglio intendersi come «Sistemi di Intelligenza Artificiale»[15]. Sono sistemi basati su macchine, guidate da una serie di obiettivi definiti dall'uomo che agiscono nella dimensione fisica o digitale percependo l'ambiente circostante, acquisendo dati al fine di raggiungere l'obiettivo preposto[16].

Le applicazioni dei sistemi di intelligenza artificiale sono innumerevoli, tra questi possiamo ricordare: la pianificazione autonoma di attività ed operazioni; i giochi; il controllo autonomo; la dimostrazione automatica di teoremi matematici e la programmazione automatica (tra cui il ML); la robotica e la visione artificiale; l'elaborazione del linguaggio naturale; i sistemi esperti e ontologie[17].

In conclusione, analizziamo la fattispecie del «Machine Learning (ML)».

---

[14] *«artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans3 that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behavior by analyzing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)», Op. cit.*, p. 6.

[15] Parlamento Europeo, Relazione sull'intelligenza artificiale in un'era digitale – A9-0088/2022, 5.04.2022.

[16] U. Pagallo, *Etica e diritto dell'Intelligenza Artificiale nella governance del digitale: il Middle-out Approach*, in *Intelligenza artificiale: il diritto, i diritti e l'etica,* a cura di U. Ruffolo, *Giuffrè Francis Lefebvre*, Milano, 2020, p. 29 ss.

[17] Intelligenza artificiale, *approfondimento* in *Treccani.it – Enciclopedia della scienza e della tecnica*, Istituto dell'Enciclopedia Italiana, F. Amigoni, V. Schiaffonati, M. Somalvico, 2008.

Per ML si intende un sottoinsieme dell'IA che si occupa di creare sistemi che apprendono o migliorano la loro performance sulla base dei dati che utilizzano. Processo attraverso il quale il computer impara senza la necessità di ricevere istruzioni dirette, consentendogli di continuare ad apprendere e migliorare in modo autonomo, senza il bisogno di una programmazione specifica[18].

Anche Google ha provato a spiegare come funzioni questo tipo di apprendimento, tramite il sito «*Teacheble Machine*» è possibile verificare in modo diretto come si allena un sistema: attraverso l'inserimento di dati di partenza e la successiva corrispondenza a risultati specifici[19].

Per esempio, il ML viene usato da Google anche per correggere gli errori di battitura che vengono commessi quando si effettua una ricerca nella barra «*google search*»[20].

L'apprendimento automatico quindi, viene posto in essere attraverso differenti meccanismi che permettono ad una macchina intelligente di migliorare le proprie prestazioni e capacità nel tempo. Attraverso l'esperienza la macchina migliorerà sempre le sue funzioni.

[18] Hawlett Parckard Enterprise, *Machine learning,* 2021, in https://www.hpe.com/it/it/what-is/machine-learning.html.
[19] D. Parlangeli, *Google ti mostra come funziona il Machine Learning, dal tuo browser,* in *Wired*.it, *2017*.
[20] C. Morelli, *Algoritmi e diritti umani: si rischia la collisione? (immaginate a danno di chi?),* in *Altalex*, 2018.

1.2. Evoluzione storica della polizia predittiva.

Il merito per aver immaginato il primo modello di polizia predittiva deve attribuirsi a William J. Bratton, al tempo commissario della polizia di New York, ed al suo vice, Jack Maple, per aver realizzato CompStat[21] nell'aprile del 1994.

Si trattava di un modello di gestione che collegava le statistiche sulla criminalità e sull'applicazione della legge mediante il tracciamento dei crimini che avvenivano nella citta di New York, raccogliendo informazioni sull'ora, il luogo e le vittime dei reati.

CompStat prendeva vita attraverso l'interrogazione settimanale di capitani, tenenti ed altri vertici della polizia, questo permetteva la raccolta di dati in tempo reale e la successiva analisi statistica in preparazione delle riunioni, a cedenza settimanale, durante le quali si discutevano le strategie per un miglior controllo sulla criminalità[22].

Grazie allo sviluppo di questo modello di gestione, gli agenti di polizia, per la prima volta, usufruirono delle statistiche sui crimini per poter effettuare un'analisi quotidiana di questi ultimi.

Inoltre, CompStat ha permesso l'avvicinamento ad una più controllata gestione delle risorse di polizia ed un'analisi più serrata riguardante la responsabilità personale da attribuirsi ad i singoli agenti[23].

Di conseguenza, grazie ad uno studio attento sui dati ricevuti, durante le riunioni, i comandanti venivano istruiti su come poter migliorare i tassi elevati di criminalità ed in generale su come poter migliorare il loro operato.

CompStat ha dunque contribuito a far scendere il tasso di criminalità della città di New York ai minimi storici[24] e per questo, tra gli anni 90 ed i primi anni 2000, si è diffuso

[21] Compstat si riferisce a:
- «COMP» computer e comparative;
- «STAT» statistics.

[22] J.J. Willis, S.D. Mastrofski, D. Weisburd, *Compstat in Practice: An In-Depth Analysis of Three Cities,* in *National Policing Institute*, 2003, p. 4.

[23] C. Smith, *The controversial crime-fighting program that changed big-city policing forever. Is Compstat's main legacy safe street – or stop and frisk?,* in *Intelligencer*, 2018.

[24] Gli omicidi passarono da 1.946 nel 1993 a 673 nel 2000; i furti d'auto passarono da 111.611 a 34.422; gli atti di stupro scesero da 2.813 a 2.068. Gli arresti per reati minori aumentarono bruscamente. Invece il numero di residenti delle carceri statali ha raggiunto un picco di 47.315 nel 1998. In riferimento a J.J. Willis, S.D. Mastrofski, D.Weisdurd, *Op. cit.*, p. 6.

rapidamente anche in altre citta statunitensi (come Boston, San Francisco, Philadelphia, Miami, New Orleans and Newark)[25].

Nel 2001 però la situazione mutò in maniera significativa, a seguito degli attacchi terroristici dell'11 settembre, l'allora sindaco di New York Michael Bloomber e il commissario della polizia Ray Kelly furono costretti a dedicare molte energie per potenziare le capacità antiterroristiche della polizia Newyorkese, che si erano appunto dimostrate lacunose soprattutto per quanto riguarda la condivisione dei dati tra polizia locale e statale[26].

La Commissione Nazionale sugli Attacchi Terroristici contro gli Stati Uniti[27] venne infatti istituita alla fine del 2002 «per predisporre un completo resoconto sulle circostanze in cui avvennero gli attentati dell'11 settembre 2001»[28].

La commissione ha descritto quel giorno come il risultato di una serie di catastrofici fallimenti nella condivisione di informazioni all'interno dell'Intelligence della polizia.

Il rapporto della polizia ha rilevato che diverse autorità statunitensi disponevano di informazioni rilevanti che avrebbero potuto identificare la minaccia e prevenire gli attacchi, ma non esistevano sistemi per condividere tali informazioni tra agenzie e piattaforme[29].

Tra le iniziative che furono adottate dalla Commissione ricordiamo: l'Information Sharing Enviroment (ISE), istituito dall'Intelligence Reform and Terrorism Prevention Act del 2004; ed il Real Time Crime Center, che ha permesso l'utilizzo delle telecamere di sorveglianza e dei database CompStat per raccogliere le informazioni e distribuirle agli investigatori immediatamente dopo la commissione di un crimine ed in alcuni casi mentre il crimine era ancora in atto[30].

---

[25] San Francisco Police Commission, *CompStat Policing in San Francisco*, in https://sfgov.org/policecommission/compstat#:~:text=COMPSTAT%2C%20short%20for%20computer%20statistics,Orleans%2C%20Los%20Angeles%20and%20Newark.

[26] S. Brayne, *Predict and Surveil: Data, Discretion, and the Future of Policing*, Oxford University Press, 2020, p. 20.

[27] In inglese: National Commission on Terrorist Attacks Upon the United States, nota anche come 9/11 Commission.

[28] Commissione d'indagine sugli attentati dell'11 settembre 2001, in *Wikipedia, L'enciclopedia libera, 2021*,

[29] P. Zelikow, C.A. Kojm, D. Marcus, *The 9/11 Commission Report*, in National Commission on Terrorist Attacks upon the United States, 2002, in https://9-11commission.gov/report/911Report.pdf, p. 401.

[30] C. Smith, *The controversial crime-fighting program that changed big-city policing forever. Is Compstat's main legacy safe street – or stop and frisk ?*, In *Intelligencer*, 2018.

Oltretutto ricordiamo anche i centri di fusione, centri di sorveglianza dove agenzie federali, statali e locali si riuniscono per raccogliere, confrontare, analizzare e condividere informazioni. Sebbene la loro missione originaria fosse destinata esclusivamente all'attività di antiterrorismo, il loro lavoro in quel campo non era sufficiente e presto il mandato degli analisti si è ampliato fino ad includere la raccolta e la condivisione di informazioni relative a tutti i crimini, tutti i rischi e tutte le minacce[31].

Attualmente vi sono ottanta centri di fusione distribuiti tra tutti gli Stati Uniti[32].

In definitiva, l'11 settembre ha catalizzato ed accelerato l'enfasi sulla condivisione dei dati ai fini della previsione e della prevenzione del crimine tra le agenzie locali e federali, grazie a ciò le forze dell'ordine federali e statali hanno ottenuto nuove e potenti risorse per raccogliere, analizzare, condividere ed utilizzare un'ampia gamma di dati.

La stessa CompStat tuttavia è rimasta sostanzialmente inalterata, vista la continua diminuzione del tasso di criminalità[33].

Silverman, professore di giustizia penale al John Jay College, che ha seguito e studiato l'evoluzione di CompStat, ha affermato che «*La saggezza prevalente era che la polizia fosse un attore minore e che le condizioni socioeconomiche fossero le cause principali del crimine, attraverso CompStat la polizia ora può non solo controllare il crimine ma deve controllarlo*»[34].

Nel 2008, la polizia di New York ha iniziato una collaborazione con Microsoft per la realizzazione di un sistema digitale più avanzato rispetto a CompStat, e grazie al fondamentale aiuto tecnologico ha sviluppato il Domain Awareness System (DAS).

Si tratta di una rete di sensori, database e dispositivi software che forniscono informazioni e analisi su misura, a dispositivi mobili e direttamente ai desktop dei singoli distretti. Programma inizialmente nato esclusivamente per l'ufficio centrale antiterrorismo della Polizia di New York, ma presto diventato una delle più grandi reti di sorveglianza al mondo.[35]

---

[31] B. Friedman, *Unwarred: Policing without permission,* in *Ferrar Straus and Giroux,* 2017, p. 267.

[32] *United States Department of Homeland Security, «Fusion Center Locations and Contact Information*», 2022.

[33] Gli omicidi sono scesi da 587 nel 2002 a 419 nel 2013; gli atti di stupro sono passati da 2.144 a 1.445 ed i furti da 31.275 a 19.168 nello stesso periodo.

[34] C. Smith, *The controversial crime-fighting program that changed big-city policing forever. Is CompStat's main legacy safe street – or stop and frisk?, cit.*

[35] Nel 2013 la Polizia di New York ha introdotto DAS per l'intero corpo. Nell'aprile 2016 tutti i 36.000 agenti della Polizia di New York potevano accedere a DAS sui loro telefonini o tablet.

Fino ad adesso non abbiamo in realtà parlato di veri e propri sistemi di polizia predittiva, quanto più di programmi di informatizzazione e quantificazione, predecessori dei software di polizia predittiva.

Possiamo affermare che la polizia predittiva nasce dopo la recessione del 2008 negli Stati Uniti.

L'intento dei vertici delle forze dell'ordine era quello di ottimizzare il lavoro e contemporaneamente tagliare i costi. Al tempo la soluzione più adatta, e decisamente la migliore, è stata quella di utilizzare dei software per indicizzare le operazioni di polizia in maniera più precisa[36].

Nata quindi come risoluzione per contenere i costi, la polizia predittiva ha subito mostrato tutto il suo potenziale. Nel 2009 infatti, la Polizia di Los Angeles ricevette tre milioni di dollari per effettuare i primi esperimenti riguardanti il funzionamento dei software, l'obiettivo prefissato era quello di prevedere le aree in cui si sarebbe verificato il crimine e quindi dispiegare gli agenti, in quei luoghi, come deterrente. Tale operazione è stata guidata dal capo della polizia in carica William Bratton, il che ha conferito molta credibilità all'operazione in virtù della stima guadagnatasi negli ambienti delle forze dell'ordine ed ha contributo all'espansione del progetto anche ad altri dipartimenti del paese[37].

Bratton ha lavorato a stretto contatto con il direttore ad interim del «*Bureau of Justice Assistance*»[38], James H. Burch II, ed il diretto re ad interim del «*National Institute of Justice*»[39], Kristina Rose, per esplorare il nuovo concetto di polizia predittiva e le sue implicazioni per le forze dell'ordine. Ciò ha condotto a due simposi, ospitati del NIJ, per raccogliere i pareri di esperti, ricercatori, professionisti, funzionari di governo e vertici delle forze dell'ordine[40].

---

[36] V. Kerber, *A short history of predictive policing in the United States*, in *Medium*, 2022.

[37] W.L. Perry, B. McInnis, C.C. Price, S. Smith, J.S. Hollywood, *Predictive policing: The Role of Crime Forecasting in Law Enforcement Operations*, in *RAND Corporation*, 2013, p. 4.

[38] Il BJA fornisce leadership ed assistenza ai programmi locali sulla giustizia penale per migliorare e rafforzare il Sistema penale della nazione. È uno dei componenti dell'«*Office of Justice Programs*», all'interno del «*United States Department of Justice*».

[39] Il NIJ è l'agenzia di ricerca sviluppo e valutazione del «*United States Department of Justice*»; e fa parte dell'«*Office of Justice Programs*».

[40] U.S. Department of Justice; Office of Justice Programs, «*Transcript: Perspectives in Law Enforcement -The Concept of Predictive Policing: An Interview With Chief William Bratton*», 2009, in https://bja.ojp.gov/sites/g/files/xyckuh186/files/publications/podcasts/multimedia/transcript/Transcripts_Predictive_508.pdf.

Il primo simposio si è tenuto nel 2009 a Los Angeles, in quell'occasione Kristina Rose ha definito Bratton come «il mezzo che ha portato alla ribalta la polizia predittiva»[41]. Inoltre, ha sottolineato l'interesse delle industrie a conoscere il termine polizia predittiva, con le relative implicazioni politiche, tecniche ed operative. Il primo simposio è stato ampiamente discusso ed ha generato molto interesse, sia a livello istituzionale che mediatico[42].

Il secondo simposio si è tenuto nel giugno del 2010 a Providence, Rhode Island. Quest'ultimo è stato caratterizzato da discussioni che proseguivano il filo logico di quelle del primo; se da una parte è stata riconosciuta l'importanza della condivisione dei dati, dall'altra si è fatta sempre più forte la necessità di una regolamentazione ad hoc. Sfide, successi, regolamentazione e limitazioni sono stati gli argomenti principali toccati nel secondo simposio[43].

Da quel momento l'interessamento e verso questo tipo di software non può essere che accresciuta, dato anche il successo dei simposi.

A conferma di ciò, nel 2011 la Polizia di Los Angeles ha iniziato ad utilizzate PredPol. Un software di polizia predittiva sviluppato dalla collaborazione tra Jeff Brantingham, antropologo dell'Università di Los Angeles, e George Mohler, allora professore di informatica all'Universit di Santa Clara e la Polizia di Los Angeles. L'algoritmo di PredPol è ancora oggi il più utilizzato in tutti gli Stati Uniti[44].

A distanza di un decennio dalla nascita dell'analisi predittiva possiamo constatare che il suo utilizzo non è mai diminuito anzi è andato ad aumentare anno dopo anno, ed è oggi presente in molti paesi del mondo.

---

[41] «*seved as the catayst for bringing predictive policing to the forefront*» in *Predictive Policing* Symposiums, *in National Institute of Justice,* 2009, p. 15.

[42] C. Smith, *The controversial crime-fighting program that changed big-city policing forever. Is Compstat's main legacy safe street – or stop and frisk?, cit.*

[43] C. Smith, *The controversial crime-fighting program that changed big-city policing forever. Is Compstat's main legacy safe street – or stop and frisk?, cit.*

[44] S. Brayne, *Predict and Surveil: Data, Discretion, and the Future of Policing, Op. cit., p. 22.*

1.3. Inquadramento tecnico.

Con l'espressione «*Predictive Policing*»[45] si intende l'utilizzo di tecniche analitiche e quantitative, per identificare possibili *target* per l'intervento della polizia, prevenire la commissione di reati futuri e risolvere crimini passati attraverso l'uso di metodi statistici[46].
Tutti i progetti di Polizia Predittiva usano dati storici i quali, se incrociati con le tecnologie avanzate nel modo giusto, possono condurre alla definizione di trend dei comportamenti criminali, facilmente prevedibili ed individuabili.
La previsione si basa sulla rielaborazione probabilistica di una serie di dati investigativi relativi a reati già commessi ed ai loro autori.
Tra questi, si annoverano i dati relativi alle notizie di reati precedentemente commessi, agli spostamenti ed alle attività di soggetti sospettati, ai luoghi teatro di ricorrenti azioni criminali ed alle loro caratteristiche, al periodo dell'anno o alle condizioni atmosferiche maggiormente connesse alla commissione di determinate fattispecie criminose. Talvolta vengono utilizzate anche informazioni che riguardano l'origine etnica, il livello di scolarizzazione, e le condizioni economiche, riconducibili a soggetti appartenenti a determinate categorie criminologiche[47].
Da questi dati elaborati, gli algoritmi dei sistemi di polizia predittiva individuano il tempo ed il luogo in cui saranno commessi determinati reati oppure chi li commetterà; il tutto attraverso il richiamo ai precedenti[48].
Il funzionamento di questi sistemi è basato, anche, su teorie criminologiche ed evidenze empiriche le quali suggeriscono che non tutte le forme di criminalità si verificano in modo casuale nel tempo e nello spazio, ma che sono strettamente collegate alle circostanze del luogo in cui vengono poste in essere ed al loro autore[49].

---

[45] «Polizia Predittiva». In italiano il verbo «predire» rappresenta la traduzione più comune del termine inglese «*to forecast*» rispetto a «*to predict*», entrambi con significati molto simili. Ma vi è una differenza: mentre «*to forecast*» fa riferimento ad una previsione oggettiva, scientifica e libera da distorsioni o errori, «*to predict*» ha un'accezione più soggettiva, intuitiva, soggetta a distorsioni individuali. Vista questa distinzione nella lingua inglese sarebbe più corretto utilizzare il termine «*forecasting policing*», nella comunità scientifica però è più diffuso il termine «*predictive policing*».
[46] V. Manes, *Intelligenza artificiale e giustizia penale*, Giappichelli Editore, 2021, p. 281.
[47] G. Tavella, *Polizia predittiva e smart city: vecchie e nuove sfide per il diritto penale*, in *Fondazione Leonardo Civiltà delle Macchine Umanesimo Digitale*, 2021, p. 3.
[48] M. Martorana, L. Pinelli, *Polizia e giustizia predittive: cosa sono e come vengono applicate in Italia*, in *Agenda Digitale*, 2021.
[49] G. Hannemyr, S. Seres, I.M. Sunde, *Predictive policing, can data analysis help the police to be in the right place at the right time?*, in *The Norwegian Board of Technology*, Oslo, 2015, p.29.

Quindi per polizia predittiva possiamo intendere l'insieme delle attività rivolte allo studio ed all'applicazione di metodi statistici che hanno l'obbiettivo di "predire" chi potrà commettere un reato, o dove e quando potrà essere commesso, al fine di prevenire la commissione dei reati stessi[50].

Sebbene oggi vi sia un'ampia variazione nella complessità, nei metodi e nell'uso delle analisi predittive da parte della polizia, possiamo individuare alcune caratteristiche comuni:

- Una grande mole di dati. Le analisi statistiche utilizzano un'infinita mole di dati, che non riguardano più esclusivamente informazioni sugli arresti o sui rapporti delle pattuglie. Ma le analisi possono anche attingere ad altre fonti, come i dati metereologici, quelli sociodemografici, le informazioni sulle imprese locali, i fattori ambientali come illuminazione e condizioni del traffico[51].
- Utilizzo di strumenti ICT. L'elaborazione dei dati viene fatta attraverso apparecchiature ICT[52].
- Dipendenza dal luogo e dal tempo. Le analisi predittive mirano a determinare il rischio che certi tipi di crimini si verifichino all'interno di determinate aree e fasce orarie. Le previsioni si riferiscono ad una determinata ora e le analisi vengono aggiornate man mano che si rendono disponibili nuovi dati.
- Supporto criminologico. Le analisi spesso si basano sulla criminologia[53], che stabilisce un legame tra il comportamento criminale e le condizioni ambientali che facilitano il compimento di determinati atti criminali.
- Ancoraggio operativo. Le analisi forniscono una base per il lavoro sia cosiddetto «d'ufficio» che quello «sul campo». Inoltre, influiscono sulla gestione delle risorse. Ad esempio, spesso vengono segnate su una mappa le aree considerate «a

[50] Perry W.L., McInnis B., Price C.C., Smith S.C., Hollywood J.S., «*Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*», Rand Corporation, 2013.
[51] W.L. Perry, B. McInnis, C.C. Price, S.C. Smith, J.S. Hollywood, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, *Op. cit,* p. 44-45.
[52] Da *Enciclopedia Treccani,* «*Information and Communication Technologies*», «Tecnologie riguardanti i sistemi integrati di telecomunicazione (linee di comunicazione cablate e senza fili), i computer, le tecnologie audio-video e relativi *software*, che permettono agli utenti di creare, immagazzinare e scambiare informazioni…»
[53] Da *Enciclopedia Treccani,* online, «Disciplina che studia il delitto nella sua realtà oggettiva e nelle sue cause. Sorta nell'ambito della scuola positiva di diritto penale in seguito agli studi di C. Lombroso e R. Garofalo, la criminologia è divenuta poi scienza interdisciplinare autonoma, riunendo in sé l'antropologia criminale, la psicologia criminale e la sociologia criminale.»

rischio», la mappa viene condivisa con le unità di pattugliamento tramite dispositivi mobili, così che questi si possano distribuire nelle aree «a rischio»[54].

I *software* di polizia predittiva posso dividersi fondamentalmente in due categorie:

2. Sistemi di individuazione degli *hotspots;*
3. Sistemi di *crime linking* [55].

I primi sono quelli che, ispirandosi alle acquisizioni della criminologia ambientale, individuano le c.d. «zone calde o *hotspots*», vale a dire i luoghi che, secondo calcoli statistici, costituiscono il possibile scenario dell'eventuale commissione futura di determinate fattispecie di reato (*crime mapping)*. Queste previsioni permettono quindi di intensificare i controlli proprio sui territori «ad alto rischio»[56].

La Commissione per l'efficienza della giustizia del Consiglio d'Europa, ha evidenziato che «*questi strumenti, hanno tassi di efficacia molto persuasivi, si afferma che abbiano effetti deterrenti sulla commissione dei reati nelle aree circostanti i punti caldi, portando ad un'opinione positiva delle politiche pubbliche*»[57].

Esempi di *software* di questo tipo sono «*Risk Terrain Modeling (RTM)*»[58], un algoritmo che, rielaborando quantità enormi di dati inerenti ai fattori ambientali e spaziali che favoriscono la criminalità, sembrerebbe consentire la previsione della commissione di reati di spaccio di sostanze stupefacenti in determinate aree urbane.

Da annoverare anche «*PredPol*» un software statunitense che analizzeremo in seguito, e il corrispondente italiano X-LAW, sviluppato dalla polizia di Napoli.

La seconda tipologia riguarda i sistemi di «*crime linking*». Questi sistemi si concentrano principalmente sulle caratteristiche e sulle abitudini del reo, basandosi esclusivamente su dati investigativi, raccolti sul luogo dell'accadimento del fatto criminoso[59].

Attraverso la raccolta e l'incrocio di una gran mole di dati, questi software, mettono in atto un vero e proprio meccanismo di profilazione, attraverso il quale sono in grado di

---

[54] G. Hannemyr, S. Seres, I.M. Sunde, *Predictive policing, can data analysis help the police to be in the right place at the right time?,* cit p.31.

[55] F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine,* in *Diritto Penale e Uomo*, 2019, p. 11.

[56] A. Giraldi, *Algorithms and Big Data Towards a crime-preventing groupware,* in *Roma Tre Law Review*, volume three/number two/twenty twenty one, 2021, online, p.7.

[57] Nel 2018 la commissione ha adottato la prima «Carta Etica Europea sull'uso dell'intelligenza artificiale (IA) nei sistemi giudiziari e in ambiti connessi» fissando i principi sostanziali e metodologici applicabili al trattamento automatizzato delle decisioni e dei dati giudiziari, sulla base delle tecniche di Intelligenza Artificiale.

[58] In https://www.riskterrainmodeling.com/.

[59] F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine, cit,* p. 12.

individuare l'autore di un precedente rato o di prevedere dove e quando un determinato soggetto ne commetterà un altro. Questi software si basano sull'idea di fondo che alcune forme di criminalità si manifesterebbero in un arco temporale ed in una zona geografica molto circoscritta (*near repeat crimes*)[60]. Infatti, i risultati forniti da questi sistemi potrebbero essere usati anche per ricostruire la carriera criminale di un soggetto e per avere una traccia di indagine da seguire per imputare, al soggetto profilato, anche i precedenti reati nel caso in cui fossero stati commessi in serie[61].

Tra questi ricordiamo il *software* di origine italiana *Keycrime*, quello tedesco *Precobs* e quello inglese *Harm Assessment Risk Tool.*

[60] Ad esempio, la commissione di una rapina sembrerebbe essere associata ad un elevato rischio di commissione di una nuova rapina, da parte degli stessi autori ed in una zona geografica vicina a quella precedente, entro le successive 48 ore e, con un tasso di rischio decrescente, fino a tutto il mese successivo.
[61] Ferguson A., *Predictive Policing and Reasonable Suspicion*, in *American University Washington College of Law*, 2012, p. 279.

1.4. Sistemi di polizia predittiva in America ed in Europa.

L'uso dell'analisi predittiva è particolarmente diffuso negli Stati uniti, anche se negli ultimi anni i vertici di polizia di altri Paesi hanno iniziato ad utilizzare questo tipo di analisi nel lavoro quotidiano. Attraverso l'uso di questi *software* è possibile scoprire nuove correlazioni tra crimini, presupposti o fattori che possono contribuire a migliorare il lavoro svolto dagli agenti di polizia[62].

Di seguito sono riportati alcuni esempi di polizia predittiva nel mondo, per avere un quadro più ampio ed aggiornato possibile.

1.4.1. PredPol

«PredPol è nato da un progetto di ricerca tra il Dipartimento di Polizia di Los Angeles e l'Università della California di Los Angeles (UCLA). Il capo della polizia dell'epoca, Bill Bratton, voleva trovare un modo per utilizzare i dati CompStat non solo per scopi storici. L'obbiettivo era quello di capire se questi dati potessero fornire raccomandazioni lungimiranti su dove e quando si sarebbero potuti verificare nuovi crimini. Poter anticipare i luoghi e gli orari in cui si verificano i crimini potrebbe consentire alle forze di polizia di dispiegare preventivamente gli agenti e contribuire a prevenirli.

In collaborazione con matematici e scienziati comportamentali dell'UCLA e dell'Università di Santa Clara, il team ha valutato un'ampia gamma di tipologie di dati e di modelli comportamentali e previsionali.

I modelli sono stati ulteriormente perfezionati con gli analisti della criminalità e gli agenti della polizia di Los Angeles e del dipartimento di polizia di Santa Cruz, California. Gli esperti hanno stabilito che tra i dati raccolti dai dipartimenti di polizia, quelli che mostrano informazioni più accurate per le previsioni, sono quelli relativi: al tipo di crimine, al luogo del crimine ed al giorno e la data del crimine.

L'attuale piattaforma di Predpol rappresenta un investimento significativo di oltre settant'anni di ricerca, analisi, modellazione e sviluppo, come si può leggere sul sito di PredPol[63].

---

[62] P. Severino, *Intelligenza artificiale. Politica, economia, diritto, tecnologia*, a cura di P. Severino, *Luiss University Press*, Roma, 2022, p.30 ss.

[63] Traduzione da https://www.predpol.com/about/. «*PredPol grew out of a research project between the Los Angeles Police Department and UCLA. The chief at the time, Bill Bratton, wanted to find a way to use*

Lo schema alla base di PredPol è un modello matematico ispirato alle tecniche di modellizzazione delle scosse di assestamento sismico: così come le scosse di assestamento seguono la scia di un terremoto, anche certi criminali tendono a ripetere nuovi atti nella stessa area, o in aree limitrofe ai reati commessi in precedenza. Si tratta di un programma analitico, che si basa sul sistema di individuazione degli *hotspots,* ed in base al tipo di crimine, al luogo ed al momento, esegue una valutazione del rischio per prevedere dove si verificheranno episodi simili nell'immediato futuro.

Il *software* è estremamente efficiente: funziona tramite un solo algoritmo il *machine learning.* Il *dataset* messo a disposizione per la predizione utilizza dati storici e tre variabili: la data, l'ora ed il luogo del crimine e la tipologia di crimine commesso.

Il programma non utilizza dati sugli arresti o informazioni che possono essere collegate ai singoli individui, poiché si cerca di evitare qualsiasi forma di profilazione ed invasione della sfera personale delle vittime[64].

Attraverso questo sistema, all'interno della mappa della città in cui opera il *software*, vengono mostrate delle aree così dette «a rischio»[65], che vengono condivise con le pattuglie di polizia in tempo reale, tramite dispositivi mobili[66]. Le aree a rischio sono circoscritte in zone di approssimativamente 150 x 150 metri, ed aggiornate ogni dodici ore; questo processo permette una migliore allocazione delle risorse di polizia che si dirigono a colpo sicuro verso zone precise della città[67].

COMPSTAT data for more than just historical purposes. The goal was to understand if this data could provide any forward-looking recommendations as to where and when additional crimes could occur. Being able to anticipate these crime locations and times could allow officers to pre-emptively deploy officers and help prevent these crimes.

Working with mathematicians and behavioral scientists from UCLA and Santa Clara University, the team evaluated a wide variety of data types and behavioral and forecasting models. The models were further refined with crime analysts and officers from LAPD and the Santa Cruz (California) Police Department. They ultimately determined that the three most objective data points collected by police departments provided the most accurate input data for forecasting:

Crime type, Crime location, Crime date and time.

The current PredPol platform represents a significant investment of over 70 research-years of PhD-level analysis, modeling and development. It has undergone over a million hours of officer testing in departments of all sizes around the world».

[64] W. Hardyns, A. Rummens, *Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges*, in *European Journal on Criminal Policy and Research*, 2018, p. 201-218.

[65] Le aree a rischio o *hotspot* vengono identificate sulla mappa con dei riquadri rossi.

[66] Tramite i *tablet* e gli *smarthphone* su cui gli agenti consultano la mappa, è possibile anche ricevere i cambiamenti e gli aggiornamenti di quest'ultima in tempo reale.

[67] J.M. Kamensky, *Fighting Crime in a New Era of Predictive Policing*, in *Governing the future of states and localities*, 2013.

Uno studio condotto presso il Dipartimento di Polizia di Santa Cruz, ha dimostrato che gli agenti in carica da molti anni, quindi considerati esperti, erano in grado di individuare circa la metà delle zone identificate dall'algoritmo, mentre gli agenti più giovani, e con meno esperienza, hanno riconosciuto solo alcune delle aree a rischio. Ciò ha dimostrato che l'intuizione e l'esperienza saranno sempre elementi importanti per il lavoro di agenti di polizia, ma l'analisi predittiva può garantire una migliore diffusione delle conoscenze anche per chi ha alle spalle meno anni di servizio.

Secondo quando si evince dal sito web di PredPol, questo strumento ha apportato una diminuzione della criminalità nelle aree in cui è stato utilizzato[68]. Per esempio, un report effettuato da PredPol afferma che a Los Angeles il tasso di furti con scasso, nell'area adibita all'utilizzo del sistema, è diminuito del 13% rispetto ad un aumento complessivo del 0,4% nelle altre zone della città che non veniva utilizzato l'algoritmo. Possiamo ricordate un esperimento condotta a Los Angeles, che ha confrontato la metodologia di PredPol con quella effettuata da esperti analisti criminali, persone in grado di individuare gli *hotspot* e di fare le previsioni sui reati futuri. Questo esperimento ha effettivamente dimostrato che, in media, l'approccio della polizia predittiva è da 1,4 a 2,2 volte più efficacie rispetto al lavoro svolto dagli esperti[69].

Secondo il Dipartimento di Polizia di Santa Cruz, il sistema ha contribuito ad una diminuzione del 27% del tasso dei furti con scasso, anche se non è un dato certo poiché non sono stati effettuati test controllati da autorità esterne[70].

Anche per questo PredPol è stato ampliamente criticato, non essendo presenti risultati verificati in maniera indipendente che possono quindi dimostrare con certezza l'efficacia di questo *software* di polizia predittiva.

1.4.2. SIMSI

SIMSI è l'unico *software* che fornisce il Risk Terrain Modeling (RTM), in grado di identificare fattispecie di reato e coordinare le risorse per prevenirli[71].

---

[68] *PredPol operetional review – initial findings*, Kent police Corporate Services Analysis Department, 2013, in https://www.statewatch.org/media/documents/docbin/uk-2013-11-kent-police-pp-report.pdf.

[69] W.L. Perry, B. McInnis, C.C. Price, S.C. Smith, J.S. Hollywood, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, *Op. cit*, p. 46.

[70] Secondo quanto affermato da figure interne della società PredPol e quanto detto da Steven Clark, ai vertici della Polizia di Santa Cruz nel 2013, in http://www.predpol.com/results/.

[71] Traduzione «*Simsi provides the only Risk Terrain Modeling software to diagnose crime patterns, prioritize places in need, and coordinate resources for prevention*», tratto da https://simsi.com.

Il Risk Terrain Modeling (RTM) è un modello sviluppato da Joel Caplan e dai suoi associati presso l'Università di Rutgers, in New Jearsey. Si tratta di un algoritmo che valuta i fattori geo spaziali che influiscono sul rischio di criminalità prevedendo in primo luogo una mappatura della zona dividendola in celle. Quindi individua il rischio di reato di una regione in base ai suoi tratti geografici[72].

I ricercatori hanno elaborato questo sistema sottoponendo all'algoritmo RTM una serie di dati inerenti ai fattori ambientali e spaziali che venivano più frequentemente associati alla commissione dei rati. Tra i fattori connessi ricordiamo: la presenza di luminarie stradali non funzionanti, la vicinanza di locali notturni, fermate di mezzi pubblici, stazioni ferroviarie, snodi di strade ad alta percorribilità, bancomat, di compro-oro e di scuole. Questo ha permesso di elaborare una vera e propria mappatura di grandi aree metropolitane, per arrivare all'individuazione di alcune «zone calde» dove risultava più elevato il rischio di spaccio di sostanze stupefacenti, con il conseguente beneficio della polizia per la programmazione e la progettazione di interventi mirati sulla delinquenza locale[73].

Il RTM, invece di analizzare le caratteristiche spazio-temporali delle fattispecie di reato al fine di predirne altri futuri, si riferisce alle caratteristiche geografiche che contribuiscono ad aumentate le probabilità di rischio di una futura azione criminosa.

Questo modello è stato testato in maniera indipendente in molte giurisdizioni, registrate nel Rutgets Center on Public Security. I risultati si confermano essere molto positivi[74].

1.4.3. Crime Anticipation System

Il Crime Anticipation System è un sistema di polizia predittiva sviluppato dal dipartimento di

Polizia di Amsterdam. Inizialmente era volto a concentrarsi principalmente sui crimini ad alto impatto, quei reati che hanno un forte impatto sulle vittime e che sono molto

[72] S. Figini, V. Porta, *Algoritmi anticrimine: tutte le tecnologie in campo*, in *Agenda Digitale*, 2019.
[73] J.M. Caplan, L.W. Kennedy, J.D. Barnum, E.L. Piza, *Crime in Context: Utilizing Risk Terrain Modeling and Conjunctive Analysis of Case Configurations to Explore the Dynamics of Criminogenic Behavior Settings.*, in City University of New York, 2017.
[74] SIMSI, *What is Risk Terrain Modeling?*, 2017, in www.simsi.com.

frequenti,[75] attualmente il suo raggio di operatività è stato ampliato anche a crimini di minore entità.[76]

L'ufficio centrale di Statistica[77] fornisce alla polizia olandese, ogni due settimane, i dati relativi alle variabili demografiche, a quelle socioeconomiche da compararsi con quelle relative alle circostanze che favoriscono il compiersi di attività criminali.

Sono quindi disponibili un'ampia gamma di informazioni che permetto al CAS di effettuare un'analisi predittiva efficacie, tuttavia l'elevato numero di variabili rende difficile valutare il contributo effettivo di ciascuna variabile[78].

Attraverso queste analisi vengono create delle mappe, le aree nelle quali vi è un rischio maggiore che si possano compiere crimini ad alto impatto sono indicate con il colore rosso, quelle con una percentuale leggermente inferiore vengono contrassegnate con il colore arancione, ed infine indicate dal colore giallo le zone dove è meno probabile il verificarsi di una fattispecie di reato.

La novità introdotta dal CAS sono le cosiddette «squadre flessibili» della polizia di Amsterdam. Si tratta di squadre non vincolate ad uno specifico distretto, ma disegnate per poter operare in tutta la città. Per ogni squadra flessibile vi sono due analisti che forniscono le indicazioni basate sulle previsioni del rischio elaborate dall'algoritmo. Anche in questo caso le zone dove si dovranno recare le pattuglie sono molto circoscritte e quindi facili da perlustrare, si tratta di celle gradi 125 x 125 metri[79].

Delle analisi hanno riscontrato che, per esempio, nel periodo che va da ottobre 2013 a luglio 2014, CAS ha predetto in maniera corretta il 15% dei furti in abitazione ed il 36% in maniera quasi corretta. Inoltre, sembrerebbe che le «squadre flessibili», grazie all'algoritmo, siano diventate esponenzialmente più efficienti[80]. Non è ancora chiaro se CAS sia in grado di ottenere un'effettiva diminuzione dei tassi di criminalità poiché gli studi non sono sufficienti, ma all'interno della Polizia di Amsterdam è stato valutato in

[75] Si tratta principalmente di: furti in casa, rapine e scippi.
[76] Come borseggi, furti d'automobili, furti di biciclette, aggressioni…
[77] Da Wikipedia l'enciclopedia libera: «Il *Central Bureau voor de Statistiek* o CBS, è l'organismo ufficiale responsabile per il coordinamento generale dei servizi statistici dei Paesi Bassi». Si tratta della principale agenzia governativa dei Paesi Bassi responsabile della raccolta dei dati sul censimento.
[78] S. Oosterloo, G. Van Schie, *The Politics Biases of the "Crime Anticipation System" of the Dutch Police,* Utrecht Data School, in Utrecht University, 2018, p.3.
[79] S. Osterloo, M.T. Schafer, *Predicting crime trough data: analysis of the data assemblage of the Dutch Crime Anticipation System,* in *New Media and Digital Culture,* Utrecht University, 2020, p. 16.
[80] W. Hardyns, A. Rummens, *Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges,* in Cross Mark, 2017, p. 201-218.

maniera molto positiva, tant'è che ne è prevista l'estensione ad altre città olandesi come Maastricht, Groningen, Eindhoven, Breda e Tilburg.

1.4.4. Precobs

Precobs, acronimo di Pre-Crime Observation System, è un *software* ideato dall'Institute for pattern-based Prediction Technique di Oberhausen, e sviluppato in Germania in grado di anticipare, su base statistica, dove e quando avverrà un furto[81].

Questo sistema prevede dove è più probabile che si possa verificare il prossimo furto con scasso. Si basa su un concetto fondamentale: è noto, agli ideatori di Precobs, che i nuovi furti si verificano spesso sulla scia di un furto andato a buon fine, solitamente poco tempo dopo e nelle zone limitrofe (se non nella stessa zona del precedente). Così la Polizia di Monaco di Baviera e di Zurigo hanno sfruttato queste conoscenze per aiutare nella creazione di Precobs [82].

Questo *software* quindi utilizza quello che viene definito il «*near repeat Phenomenon*», fenomeno che constata che gli eventi criminosi sono spesso seguiti, sia a livello temporale che spaziale, da altri eventi simili. Il fondamento logico di queste affermazioni risiede nell'ipotesi che i ladri agiscano in modo razionale e si comportino in maniera quasi schematica, il che si traduce in modelli che sono in qualche misura prevedibili. Numerosi studi empirici hanno supportato questa osservazione con riguardo ad i furti con scasso in abitazione[83].

Il programma gestisce dati storici di furto con scasso e cerca automaticamente delle correlazioni statistiche tra i diversi elementi dei dati; ad esempio l'ora ed il luogo, se si tratta di un appartamento, di una casa indipendente o di una villa a schiera, se i ladri sono entrati da una porta sul retro oppure da una finestra. In questo modo l'algoritmo elabora grandi volumi di dati e statistiche sui furti con scasso e crea in breve tempo delle correlazioni.

Nel quotidiano invece Precobs necessita di una quantità limitata di dati, quelli registrati dalla polizia quando viene denunciato un furto in abitazione. Molto importante è la

[81] R. Mantovani, *Innovazione Precobs, il computer made in Germany che prevede i crimini*, in *Focus*, 2014.
[82] W. Hardyns, A. Rummens, *Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges*, Op. Cit., p. 201-218.
[83] M. Nobels, J.T. Ward, R. Tillyer, *The Impact of Neighborhood on Spatiotemporal Patterns of Burglary*, in *Journal of Research in Crime and Delinquency*, 2016.

scrupolosità con cui vengono registrati i dati dagli agenti, sono necessari l'indirizzo, la data e l'ora dell'evento iniziale.

Quando vengono trovate delle correlazioni, queste sono immediatamente trasmesse alla polizia locale interessata. Innanzitutto, nel momento in cui viene segnalato il verificarsi di un furto, il software trasmette agli agenti una mappa, delle raccomandazioni per il pattugliamento e le informazioni sull'evento inziale. La raccomandazione principale è che entro sette giorni dal primo furto, nel raggio di 500 m, se ne potrebbe verificare un secondo. L'area di pattugliamento, indicata sulla mappa con dei quadrati rossi di 250 x 250 metri, è chiamata cerchio operativo; al cento del quadrato vi è indicato il luogo del furto che ha fatto scattare l'allarme, l'area limitrofa colorata di rosso sta invece ad indicate il raggio di 500m entro il quale si potrebbe verificare un altro furto. In quest'area si ipotizza quindi un rischio elevato di furti con scasso, prevalentemente entro i sette giorni successivi ala primo[84].

In seguito ad un periodo di prova di un anno, la polizia di Zurigo ha affermato che il tasso di furti è diminuito del 30% nelle aree in cui era stato utilizzato Precobs, anche la polizia di Monaco di Baviera ha riferito che il numero di furti con scasso è diminuito del 42% nelle aree in cui gli agenti di polizia hanno dato seguito all'algoritmo[85].

1.4.5. Harm Assessment Risk Tool

La polizia del Durham[86], in collaborazione con l'università di Cambridge ha messo a punto il sistema HART [87] con l'obbiettivo di promuovere processi decisionali che permettano di realizzare interventi mirati a ridurre il rischio di recidiva. In realtà, più che al genus dei sistemi di polizia predittiva, sarebbe più corretto ricondurre questo sistema ai c.d. *Risk Assessment Tools,* ossia a quegli strumenti computazionali in grado di calcolare se un soggetto si sottrarrà al processo o commetterà ulteriori reati. Si tratta di modelli che operano in una fase successiva rispetto a quella di prevenzione e di indagine.

[84] D. Gerstner, *Using Predictive Policing to Prevent Residential Burglary – Findings from the Pilot Project P4 in Baden-Wurttember, Germany,* Department of Criminology, Max Planck Institute for Foreign and International Criminal Law, Germany, 2015, p. 116.
[85] W. Hardyns, A. Rummens, *Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges,* Op. cit., p. 201-218.
[86] Durham è una città situata nel Nord Est dell'Inghilterra.
[87] Acronimo di «Harm Assessment Risk Tool».

D'altra parte, è inevitabile che queste categorie, dai confini ancora sfocati, possano talvolta sovrapporsi[88].

L'HART è stato utilizzato dal corpo di polizia di Durham a partire dal 2017 al fine di valutare quando una persona possa essere sottoposta ad un programma di riabilitazione, chiamato *Checkpoint,* che costituisce un'alternativa all'esercizio dell'azione penale[89].

Si tratta di uno strumento che svolge dei giudizi predittivi per verificare il rischio che un soggetto arrestato commetta dei reati nei due anni successi al primo. Analizzando il risultato, il reo viene catalogato in base a tre criteri di rischio: alto, moderato o basso.

Sono considerati ad alto rischio, gli autori di determinati crimini; cimini per i quali vi è una probabilità molto elevata per il loro autore di commetterne una altro della stessa portata. Per l'algoritmo sono considerati reati gravi: l'omicidio, il tentato omicidio, violenze varie, la rapina, i reati che riguardano la sfera sessuale e quelli con arma da fuoco.

In secondo luogo, sono categorizzati come soggetti a rischio moderato, coloro che si prevede possano commettere dei crimini nell'arco dei due anni successivi al primo, ma questi si limiteranno a reati non gravi.

Infine, sono identificati come a basso rischio, i soggetti che si prevede non commetteranno nuovi reati nel corso dei successivi due anni dal perpetuarsi del primo[90].

Solo le persone che sono classificate nella categoria del rischio moderato, sono incluse nel programma Checkpoint[91].

In sostanza quindi, il programma Checkpoint cerca di affrontare le motivazioni intrinseche che sono alla base della commissione di un reato e dei problemi comunitari ad esso associati, offrendo un aiuto ad un sottogruppo di soggetti prescelti. L'aiuto offerto si fonda sull'individuazione della causa per cui il reo ha commesso un crimine e di conseguenza sulla scelta di interventi e servizi ad hoc per far si che desista dal commettere nuovamente una fattispecie criminosa[92].

---

[88] M. Oswald, J. Grace, S. Urwin, G.C. Barnes, *Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality,* in *Information & Communications Technology Law*, 2018, p.227.

[89] C. Silkie, *Big Brother Watch defending civil liberties, protecting protecting privacy,* 2019, p.2.

[90] M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificilale: luci e ombre dei risk assessment tools tra stati uniti ed europa*, in *Diritto Penale Contemporaneo*, 2019, p 11.

[91] L'obbiettivo di questo programma è quello di ridurre la recidiva affrontando in motivi per cui un soggetto ha commesso un reto. Per esempio, può trattarsi di problematiche riguardanti l'abuso di alcol, la mancanza di una casa o la salute mentale; tutte aree in cui è possibile intervenire e fornire aiuto.

[92] M. Oswald, J. Grace, S. Urwin, G.C. Barnes, *Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality,* cit, p.229.

HART è stato creato sulla base dell'analisi di circa 104.000 casi avvenuti a Durham in un arco temporale di cinque anni[93]. Inoltre, si fonda su una particolare forma di *machine learning*, chiamata *random forest,* che prende in considerazione numerose variabili, e la maggior parte di queste sono collegate alla storia criminale del soggetto, all'età, al genere ed ai codici postali di residenza. Proprio quest'ultima variabile ha scatenato forti critiche, prevalentemente in termini di *privacy.* Critiche cha hanno portato successivamente la polizia di Durham ad eliminare dal sistema le informazioni che riguardano il codice postale[94].

[93] Dal 2008 al 2012.
[94] M. Burgess, *UK police are using AI to inform custodial decisions – but it could be discriminating against the poor*, in Wired, 2018.

1.5. Sistemi di polizia predittiva in Italia.

Negli ultimi anni anche in Italia i sistemi decisionali automatizzati stanno assumendo sempre più importanza nella società. La previsione del crimine, anche nel nostro paese, è finalmente divenuta una priorità per la comunità scientifica che si impegna a sviluppare modelli statistici sempre più precisi ed efficaci.

Da diverso tempo, alcuni rappresentanti dei servizi di pubblica sicurezza sono impegnati nella progettazione di sistemi di intelligenza artificiale che coadiuvano le forze di polizia nell'opera di prevenzione e controllo del territorio contro i crimini tipici della vita cittadina.

In particolare, sono stati realizzati due *software*, oggi in uso in diverse città, KeyCrime ed Xlaw che adesso andremo ad analizzare.

1.5.1. KeyCrime

KeyCrime è un *software* sviluppatosi all'interno dalla questura di Milano, nell'Ufficio prevenzione generale e soccorso pubblico, in una stanza dove una famosa frase di Sherlock Holmes ricorda ogni giorno agli organi di polizia quale è la chiave per essere un bravo investigatore [95]. È proprio questa la frase che ispirò Mario Venturi nell'intraprendere la ricerca di un qualcosa che riuscisse a facilitare il proprio lavoro.

Lo stesso Mario Venturi racconta «Tornando da un turno di servizio in Volante e dovendo mettermi a compilare la relazione di un intervento che avevamo eseguito per una rapina in farmacia mi misi a dare un'occhiata ai fascicoli cartacei riguardanti quel tipo di reato, e tra un foglio e l'altro, iniziai a vedere che tra i vari eventi criminosi pregressi poteva esserci un *fil rouge* che li collegava, o meglio, che collegava alcuni di questi reati commessi e, in special modo, le rapine a danno di esercizi commerciali, soprattutto farmacie che venivano consumati in città.

Capii che tutti quei dati e quei particolari erano scritti sui fogli che noi poliziotti compilavamo ogni fine turno, potevano e dovevano essere trasposti su un supporto

[95] La frase del 1898 pronunciata da Sherlock Holmes è la seguente: «Dalle unghie di un uomo, dalle maniche della sua giacca, dai suoi stivali, dalle ginocchia dei suoi pantaloni, dai calli sull'indice e sul pollice, dalla sua espressione, dai polsini della sua camicia, dai suoi movimenti, da tutte queste cose si capisce l'occupazione di una persona. È pressoché inconcepibile che, tutte insieme, non riescano ad illuminare un investigatore esperto».

informatico; così iniziai a creare un database in cui anche il minimo particolare aveva la propria casella. In tanti anni di immagazzinamento di dati, quel database assunse proporzioni di un certo rilievo. Serviva qualcosa che analizzasse i dati e li incrociasse tra loro per arrivare a trarre le prime conclusioni. Così iniziai a mettere in capo le conoscenze acquisite nel tempo fino ad elaborare l'embrione di un algoritmo di analisi criminale, che poi sarebbe diventato un modello matematico, cuore del programma che attualmente utilizziamo qui a Milano»[96].

Venturi iniziò a lavorare alla realizzazione di questo *software* nel 2007, durante il suo incarico presso l'Ufficio di prevenzione generale e soccorso pubblico. Dopo aver raccolto i dettagli dei crimini in un rudimentale database, nella cui memoria inizialmente ha inserito le informazioni più generiche rispetto al reato: il quartiere, l'ora, il tipo di negozio preso di mira, poi via via ha inserito quelle più dettagliate legate al comportamento e alle caratteristiche dell'autore, costruendo così il *software*[97].

Keycrime quindi, è un progetto che prende corpo dall'osservazione degli elementi presenti in un atto criminoso e dalla conseguente convinzione, divenuta poi una consapevolezza, che questi, se esaminati correttamente attraverso il supporto di un "elaboratore" dotato di un'elevata capacità di calcolo e valutazione, avrebbero permesso di ottenere una precisa conoscenza delle dinamiche riguardanti i crimini seriali. Sulla base di questa convinzione è stato progettato un modello di analisi basato su principi dettati dalla filosofia analitica trasportati poi su modelli matematici[98].

KeyCrime è un software che, rivoluzionando il concetto di *predictive policing*, mette in campo un approccio innovativo, definibile come *predictive crime analysis.* Si tratta di un'analisi scrupolosa di tutti gli elementi che caratterizzano i fatti criminosi, con il fine di riconoscere ed indicare agli investigatori quali crimini siano stati realizzati dalla stessa mano[99].

I dati analizzati appartengono principalmente a caratteristiche proprie dell'autore del reato, come per esempio l'identificazione come mancino o destrorso, se abbia particolarità fisiche evidenti o la tendenza all'uso di armi.

---

[96] C. Morabito, *La chiave del crimine*, in *Polizia Moderna*, 2015, p.36.
[97] R. Pelliccia, *Polizia Predittiva: il futuro della prevenzione criminale?*, in Cyberlaws, 2019.
[98] M. Venturi, *KeyCrime La chiave del crimine, I profili dell'abuso*, in *Giornale scientifico a cura dell'O.N.A.P. – Osservatorio Nazionale Abusi Psicologici*, 2014.
[99] Sindacato Autonomo di Polizia, *UNO SGUARDO AL FUTURO (SPERIAMO PROSSIMO) KEYCRIME*, 2019, in https://www.sap-nazionale.org/news/uno-sguardo-al-futuro-speriamo-prossimo-key-crime/.

Entrando più nello specifico possiamo dire che il *software* parte dall'osservazione del particolare per arrivare al generale, per poi ridiscendere dal generale al particolare, attuando così una capacità previsionale basata su modelli matematici in grado di predire un'azione futura.

L'analisi iniziale effettuata dal programma è un'analisi induttiva, volta ad identificare aspetti comuni in eventi diversi che permettano di creare delle relazioni tra i singoli fatti che non potrebbero essere accomunati in altro modo. Ciò permette di imputare ad un unico soggetto reati che sono avvenuti in tempi ed in luoghi diversi. Questa procedura è svolta dal sistema attraverso l'analisi del reato nel suo insieme e tramite la valutazione di ogni particolare con un approccio analitico tipico dell'investigazione della Polizia.

Nella seconda fase, viene ad attuarsi un percorso deduttivo che applica delle logiche di osservazione che permettono la previsione di un reato futuro attraverso il modello *KeyCrime*[100].

L'obbiettivo di questa analisi è quello di offrire un supporto adatto per coadiuvare le attività istituzionali della Polizia di Stato.

Veniamo ora a comprendere il funzionamento pratico di questo modello che ha fatto invidia a tutto il mondo. Innanzitutto, i poliziotti raccolgono, come di consueto, le denunce delle rapine che vengono poi depositate all'ufficio preposto alla raccolta e all'analisi dei dati. Questi ultimi vengono inseriti all'interno del sistema KeyCrime[101]. Da questo momento in poi entra in gioco il software, il quale, elaborando ed incrociando tutti i dati raccolti[102], cerca le correlazioni tra le diverse fattispecie criminose e propone al poliziotto una serie di eventi potenzialmente collegabili con quello appena inserito, solo in caso di esito positivo viene dato un possibile nome del colpevole.

Inoltre, l'algoritmo è in grado di prevedere le rapine, poiché sulla base delle informazioni che sono state immagazzinate, calcola gli obbiettivi ritenuti più a rischio in una data area della città, in aggiunta al giorno e l'ora in cui è più probabile che il criminale entri in azione. A questo fine vengono predisposte delle pattuglie della polizia, in borghese, per poter arrestare il reo in flagranza o evitare che ponga in essere la fattispecie[103].

---

[100] C. Morabito, *La chiave del crimine, cit,* p.37.

[101] Spesso in questa fase gli agenti sono soliti riconvocare le vittime con il fine di raccogliere informazioni più dettagliate per permettere all'algoritmo di funzionare al massimo delle sue capacità.

[102] Per esempio: corporatura, abbigliamento modus operandi, orari, luoghi.

[103] Riproduzione riservata, *KeyCrime, l'algoritmo anti-rapine. Incastra i banditi e prevede i colpi*, in *Quotidiano Nazionale,* 2016.

I risultati di KeyCrime sono stati messi al vaglio da una ricerca condotta dall'Università di Essex. Lo studio ha evidenziato un punto di forza di questo programma, che lo fa spiccare tra i competitor. Mentre gli altri *software* di polizia predittiva lavorano esclusivamente su una base statistica, indicando dove, quando e che tipo di crimine sarà commesso, KeyCrime è l'unico che definisce anche "il come", grazie ad un'analisi delle modalità comportamentali dell'autore, ispirato quindi all'idea di *crime linking*[104]. Oltretutto a differenza del *software* americano PredPol, che ha l'obiettivo di indirizzare i pattugliamenti verso una o più zone specifiche della città al fine di intimidire i criminali dal commettere i reati o permettere ai poliziotti di intervenire nel caso in cui il reato si verifichi in quel dato momento. Il *software italiano*, si preoccupa di scoprire, sulla base degli eventi accaduti in precedenza, quale potrebbe essere la prossima mossa di un criminale, che è già stato individuato in precedenza, e coglierlo in flagrante[105].

Giovanni Mastrobuoni[106], sottolinea che, poiché KeyCrime lavora principalmente sulla serialità, la sua efficacia debba essere misurata sui crimini che fanno parte di una sequenza, non su quelli isolati, e che più è lunga la serie, migliore è la capacità di previsione[107].

Per questo i risultati ottenuti da KeyCrime sono notevolmente significativi. Nel 2008, anno antecedente all'introduzione del *software* a Milano, le rapine ai danni di farmacie, negozi e supermercati sono state 664, e nel 74% dei casi l'autore non è stato individuato. Nel 2016, otto anni dopo il primo utilizzo del modello, i numeri si sono invertiti, il 74% delle rapine ha un colpevole noto ed il numero dei colpi messi a segno è sceso a 283[108].

Oltretutto i dati presentati dalla Questura di Milano indicano che la soluzione dei casi trattati con KeyCrime è passata dal 27% dell'anno 2007, primo anno di sperimentazione, al 54% dell'anno 2013. Questi risultati hanno introdotto un elemento di deterrenza riducendo il numero degli eventi[109].

---

[104] G. Mastrobuoni, *Impact: Imagine being able to predict a crime in the future*, in *Research case study dell'Università di Essex*, 2018.
[105] S. Figini, V. Porta, *Algoritmi anti-crimine: tutte le tecnologie in campo*, in *Agenda Digitale*, 2019.
[106] Economista e coordinatore degli studi condotti su KeyCrime da parte dell'Università di Essex.
[107] R. Pelliccia, *Polizia Predittiva: il futuro della prevenzione criminale?, cit.*
[108] Riproduzione riservata, *KeyCrime, l'algoritmo anti-rapine incastra i banditi e prevede i colpi, cit.*
[109] M. Venturi, *KeyCrime La chiave del crimine, I profili dell'abuso, cit.*

Approvato dal Viminale KeyCrime sta per essere presentato ad altre questure e forze di polizia in virtù, non solo del suo alto potenziale innovativo, ma anche della sua poliedricità applicativa.

1.5.2. XLAW

Proprio come KeyCrime, anche il *software* XLAW è stato sviluppato da un rappresentante delle forze dell'ordine, ma in questo caso della Questura di Napoli, Elia Lombardo.

Si tratta di una soluzione digitale in grado di prevedere i crimini predatori, secondo la logica della previsione. Lombardo ha proposto il software, in sperimentazione alla Questura di Napoli, all'Ufficio Generale e Soccorso Pubblico, cedendolo in comodato d'uso[110].

L'ispettore Lombardo in persona ha specificato «Ho dato vita ad un lungo studio criminologico con cui sono riuscito a dimostrare che tra i tanti crimini che può commettere un uomo ve ne sono alcuni prevedibili. E sono i furti, gli scippi, le rapine, i borseggi, le truffe, che tra l'altro sono anche crimini istituzionali da parte del cittadino. Sono partito da un assioma: per prevenire bisogna prevedere. Così ho cercato di capire se questo fosse possibile sperimentando strategie e nuovi metodi. Normalmente le attività di controllo vengono attuate quando si è di fronte ad un crimine ripetuto più volte o quando cresce l'allarme sociale: in questo modo si gioca sempre in rincorsa rispetto al crimine. Così ho capito che bisognava passare ad un'attività di pura prevenzione sperimentando la tecnologia»[111].

L'ispettore della questura di Napoli descrive il *software* come una soluzione, probabilistica e dotata di algoritmi di *machine learning*, per scovare tendenze e pattern negli episodi criminali.

Dopo essere stato fornito in comodato d'uso e validato da due università, la Federico II di Napoli e l'Università Partenopea. Attualmente gli è stato consesso il brevetto per Invenzione Industriale.

Il *software* opera grazie a due livelli di informazioni, innanzitutto in base a quelle collegate alle caratteristiche socioeconomiche del territorio preso in esame, ed in secondo

[110] M. Martorana, L. Pinelli, *Polizia e giustizia predittive: cosa sono e come vengono applicate in Italia*, in *Agenda Digitale*, 2021.
[111] Regione Campagna, *XLAW: L'algoritmo-poliziotto che prevede furti e rapine*, in *Smau Napoli*, 2018.

luogo sulle informazioni riguardanti gli eventi criminosi immagazzinate grazie alle denunce, i social media e le notizie fornite dai media. La novità che ha portato al riconoscimento del brevetto, è che il sistema si sviluppa in tre *step*. Il primo *step* si sviluppa nell'analisi criminologica sui crimini predatori, il secondo riguarda l'istruzione della macchina per far si che faccia scattare l'allarme predittivo, ed il terzo riguarda l'aspetto predittivo propriamente detto[112].

La logica alla base del suo funzionamento è quella delle «riserve di caccia», modello di individuazione dei reati che parte dall'assunto che i reati predatori siano crimini ciclici e stanziali. Ciò comporta la possibilità di dedurre il modo in cui si manifesteranno i comportamenti criminosi prima che vengano posti in essere, grazie ad un'analisi algoritmica della storia criminale di un luogo nel tempo[113].

Questo *software* sembra ispirarsi ad un sistema di individuazione degli *hotspot*, che fa leva su un algoritmo capace di rielaborare una mole enorme di dati estrapolati dalle denunce inoltrate alla Polizia di Stato. Tale rielaborazione consente di fare emergere fattori ricorrenti o fattori coincidenti[114]. Questo consente al sistema di tracciare una mappa del territorio dove vengono segnate le zone a più alto rischio fino a raggiungere il livello massimo in determinati orari, così consentendo, nelle zone evidenziate, la predisposizione delle forze dell'ordine per impedire la commissione di tali reati e per cogliere in flagranza i potenziali autori degli stessi[115].

Il sistema XLAW può quindi essere utilizzato per allertare le forze dell'ordine di polizia ed inviare pattuglie sulla scena del crimine, prima che questo venga compiuto, ed al contempo fornisce agli agenti precisi dettagli sui potenziali sospettati.

Il modello in questione si basa su un metodo di analisi innovativo, e la sperimentazione da parte di più strutture di sicurezza ha permesso si stabilire che basando le attività sulla selettività e sequenzialità dei controlli in virtù degli allarmi predittivi, elaborati secondo

---

[112] C. Morelli, *XLAW, il brevetto italiano di polizia predittiva*, in Altalex, 2022.

[113] F. Chiusi, S. Fischer, N. Kayser-Brill, M. Spielkamp, *Automating Society Report 2020*, in *AlgorithmWatch gGmbh*, Berlino, Germania, 2020, p. 49, tratto da https://automatingsociety.algorithmwatch.org/wp-content/uploads/2020/11/Automating-Society-Report-2020-Edizione-italiana.pdf.

[114] Come per esempio la ripetuta commissione di rapine negli stessi luoghi, da parte di persone con lo stesso tipo di casco, e con analoghe modalità.

[115] F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine, in Diritto Penale e Uomo*, Fascicolo 10/2019, 2019, p.12.

il modello di intelligenza artificiale, si ottiene un netto stravolgimento del metodo di lavoro normalmente basato sul pronto intervento.

Il sistema è già stato adottato, oltre che nella città di Napoli, anche a Modena, Prato, Salerno, Livorno, Trieste, Trento e Venezia, per permetterne una sperimentazione indipendente in diverse città italiane. L'obbiettivo è quello di migliorare l'attività di prevenzione dei crimini nelle aree urbane. Risulta che il supporto operativo dell'intelligenza artificiale, abbia permesso agli operatori maggiore consapevolezza del rischio e capacità decisionale direttamente nello scenario operativo.

Gli studi fin qui realizzati[116], hanno dimostrato come sia possibile un'accuratezza di previsione del comportamento delinquenziale al 90%[117].

A Napoli i crimini predatori sono diminuiti del 22%, mentre denunce ed arresti in flagranza di reato sono aumentati del 24%[118].

In generale, risulta che il supporto operativo dell'intelligenza artificiale, abbia permesso agli operatori maggiore consapevolezza del rischio e capacità decisionale direttamente nello scenario operativo.

Sul sito di XLAW viene infatti riportato un elenco di obbiettivi raggiunti dal *software* che è bene riportare:

- Efficacia operativa: sono diminuiti scippi, rapine, furti e borseggi in misura maggiore rispetto alla media nazione. Oltretutto è stata dimostrata la maggiore efficacia del metodo previsionale rispetto a quello tradizionale.
- Valorizzazione del capitale umano: sono migliorate la motivazione, la partecipazione e la capacità di prendere decisioni strategiche per raggiungere gli obbiettivi a breve e medio termine da parte degli operatori di controllo del territorio e la percome operativa all'interno dell'organizzazione.
- Risparmio sui costi di gestione della sicurezza per la collettività: sono stati razionalizzati gli interventi e ridotti i chilometri di percorrenza delle pattuglie, il consumo di carburante e lo stress di uomini e mezzi. In aggiunta al risparmio per la collettività in base alla diminuzione dei delitti.

[116] Quello del Professore Giacomo di Gennaro, docente di sociologia e direttore del Master in criminologia dell'Università Federico II di Napoli, a cui si aggiungono gli spunti offerti dall'antropologo culturale Daniele Vazquez Pizzi nel suo libro *la fine della città post-moderna,* Mimesis, 2013.

[117] R. Thomas, *La criminalistica e l'algoritmo XLAW che prevede i reati,* in *Polizia Penitenziaria.it*

[118] Regione Campania, *XLAW: L'algoritmo-poliziotto che prevede furti e rapine*, *cit.*

- Ulteriori implicazioni: un'integrazione operativa con le forze dell'ordine, il miglioramento della percezione di sicurezza e fiducia nell'istituzione da parte del cittadino, il miglioramento della reputazione professionale da parte degli operatori, il contenimento dei fattori di rischio e stress degli operatori, la definizione su base scientifica della sicurezza reale e percepita, ed infine la favorevole accettazione da parte dei media, del mondo accademico e di quello giuridico[119].

Emergono dei dubbi sull'esattezza dei risultati prodotti da questi sistemi e del loro impatto nella lotta al crimine, essendo queste analisi fornite dai fondatori del sistema stesso e non essendo presente nessuna ricerca portata avanti da autorità indipendenti ed esterne.

[119] Citazione dal sito: https://www.xlaw.it/presentazione/.

1.6. Quadro normativo

In un primo momento gli strumenti di polizia predittiva non sono stati regolamentati da una disciplina ad hoc, rimettendo le modalità e le condizioni del loro utilizzo all'esclusiva iniziativa degli operatori di polizia ed alla prassi.

Il Consiglio d'Europa, a seguito dell'irrefrenabile diffusione degli strumenti digitali e dell'intelligenza artificiale in tutti i settori istituzionali e giudiziari, nel dicembre 2017 ha pubblicato uno studio dal titolo *Algorithms and Human Rights,* nel quale un gruppo di esperti ha approfondito la portata dei diritti umani in relazione alle tecniche di trattamento automatizzato dei dati, le possibili implicazioni normative e le preoccupazioni del Consiglio d'Europa[120].

La fattispecie in esame è stata per la prima volta oggetto di specifica disciplina nel dicembre 2018 con l'adozione della Carta Etica Europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e nei relativi ambienti da parte della Commissione europea per l'efficacia della giustizia del Consiglio d'Europa (CEPEJ)[121]. Innanzitutto, bisogna chiarire che viene riconosciuta c come urgente e necessaria la necessita di regolamentare gli strumenti informatici. Infatti, per la commissione, l'impiego di metodi computazionali per il rafforzamento dell0efficacia della giustizia deve essere incoraggiato. Questo documento cristallizza cinque principi che devono rappresentare il fondamento per qualsiasi disciplina riguardante la materia in esame: il rispetto dei diritti fondamentali, facendo particolare attenzione al diritto di accesso alla giurisdizione e al diritto di equo processo; il principio di non discriminazione, il principio di qualità e sicurezza nell'analisi dei dati e delle decisioni giudiziarie, il principio di trasparenza ed imparzialità, declinato nelle forme di accessibilità, comprensibilità e verificabilità esterna dei processi computazionali, e l'inderogabile possibilità di controllo da parte dell'utente[122].

---

[120] Comitato di esperti sugli intermediari di Internet (MSI-NET), *Algorithms and Human Rights,* Consiglio d'Europa, 2017, in https://rm.coe.int/algorithms-and-human-rights-study-on-the-human-rights-dimension-of-aut/1680796d10.

[121] La Commissione Europea per l'efficacia della giustizia venne istituita nel 2002 per iniziativa del Comitato dei Ministri del Consiglio d'Europa, con lo scopo di monitorare e misurare la qualità dei sistemi giudiziari dei Paesi membri.

[122] S. Quattrocolo, *Intelligenza Artificiale e Giustizia: nella cornice della Carta Etica Europea, gli spunti per un'urgente discussione tra scienze penali e informatiche,* in *Legislazione Penale*, 2018, p.3.

La Commissione Europea, nell'aprile del 2021, ha pubblicato una proposta di Regolamento del Parlamento Europeo e del Consiglio che si concentra sulla gestione ed il controllo dei rischi connessi all'uso dell'intelligenza artificiale[123]. Nella proposta non viene regolamentata l'intelligenza artificiale in quanto tale, ma il suo ingresso nel mercato, la messa in uso e l0utilizzo dell'ambito dell'Unione Europea dei sistemi che contengono tale tecnologia.

La proposta classifica i Sistemi di Intelligenza Artificiale in base al rischio di impatto negativo sui diritti fondamentali: più il prodotto è suscettibile di mettere in pericolo questi diritti, più necessita di misure maggiormente severe per eliminare o mitigare l'impatto, fino ad arrivare a vietare determinati prodotti considerati incompatibili[124].

In particolare, il regolamento identifica SIA proibiti, SIA as alto rischio e SIA con specifichi rischi. di manipolazione. Una serie di sia vengono proibiti quando i rischi legati a questi vengono considerati inaccettabili. Questi comprendono pratiche in grado di manipolare le persone attraverso tecniche subliminali o di sfruttare la vulnerabilità di specifici gruppi, per distorcere i loro comportamenti. Per quanto riguarda la giustizia penale, ricordiamo che sono vietati i sistemi a tempo reale di identificazione biometrica da remoto di spazi pubblici per funzioni di polizia, se con fini di sorveglianza indiscriminata [125] . Rientrano in questa categoria anche alcune fattispecie del riconoscimento facciale, soprattutto quando viene utilizzato da parte di un'autorità pubblica.

I SIA ad alto rischio sono invece quelli che dipendo dallo scopo a cui sono adibiti, dalla severità dei danni potenziali, e dalla probabilità della loro occorrenza. Questi non sono proibiti in quanto tali, ma sono soggetti a requisiti ed obblighi aggiuntivi. Ricadono in questa categoria, per esempio, quelli usati per l'identificazione biometrica e la categorizzazione di individui, e quelli utilizzati dalle forze di polizia e nell'amministrazione della giustizia. Si tratta della categoria più comune.

---

[123] All'interno del regolamento viene attribuita, per la prima volta, una definizione di SIA. «Per sistema di intelligenza artificiale si intende un *software* sviluppato con una o più delle tecniche degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono». Art. 3 Regolamento.

[124] G. Tavella, *Polizia predittiva e smart city: vecchie e nuove sfide per il diritto penale,* in *Fondazione Leonardo, Civiltà delle macchine,* 2022, p.7.

[125] Sono però previste varie eccezioni che ammettono, in parte, il loro utilizzo e che si basano su parametri di valutazione "caso per caso", prendendo in considerazione la natura della situazione, le conseguenze dell'uso del SIA, e i criteri di proporzionalità.

Infine, vi sono i SIA che potrebbero essere soggetti a manipolazione, si tratta di un rischio medio, per questi sono previsti controlli finalizzati ad evitare problemi di trasparenza[126]
Per quanto riguarda la gestione e la protezione de dati necessari per l'utilizzo dei *software* di polizia predittiva deve farsi riferimento al *Data protection reform package*, costituito dal Regolamento 2016/679/UE (GDPR) e dalla Direttiva 2016/680/UE[127]. Nello specifico, la Direttiva 2016/680/UE, mira a stabilire norme minime relative alla «protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte di autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzioni di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica»[128].
A livello nazionale, la Direttiva in questione è stata attuata con D.lgs. 18 maggio 2018, n.51. Bisogna ricordare l'artico 8 del D.lgs. che stabilisce il divieto di decisioni basate unicamente su trattamenti automatizzati, affermando il criterio di non esclusività del dato algoritmico[129].
Quindi possiamo affermare che l'utilizzo di questi *software*, se utilizzati per l'individuazione di una responsabilità penale, non potranno mai essere l'unico elemento sul quale fondare la decisione in sede di giudizio, proprio perché si tratta della libertà personale dell'imputato. Nessuna limitazione invece, nel caso in cui siano limitati all'allocazione delle forze di polizia sul territorio.

[126] A. Lavogna, G. Suffia, *La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale*, in *Giustizia penale e nuove tecnologie*, *Diritto penale contemporaneo*, 2021, p. 92-94.
[127] P. de Hert, V. Papakonstantinu, *The New Police and Criminal Justice Data Protection Directive: A First Analysis*, in *New Journal of European Criminal Law*, 2016, p.7
[128] Art 1, Par 1, Direttiva 2016/680/UE.
[129] G. Tavella, *Polizia predittiva e smart city: vecchie e nuove sfide per il diritto penale, cit*, p. 8.

2. Nuove tecnologie nella funzione di Pubblica Sicurezza

2.1. Scurezza pubblica

La sicurezza pubblica è «il complesso dei compiti attribuiti alle autorità preposte al mantenimento dell'ordine pubblico, alla sicurezza e alla incolumità dei cittadini, alla tutela della proprietà, al controllo e all'osservanza delle leggi e dei regolamenti»[130]. Dunque, è quindi una condizione oggettiva che permette agli individui di svolgere tranquillamente le proprie attività di qualsiasi genere, purché lecite.

Nella nostra Carta costituzionale all'articolo 117, comma secondo, lettera h), ed al terzo comma dell'articolo 118 si parla di sicurezza pubblica, la quale viene definita come funzione che consente agli individui di vivere in modo tranquillo all'interno di una comunità e di agire all'interno della stessa, per mantenere la propria individualità e per soddisfare i propri interessi.

L'esigenza sociale della sicurezza pubblica è, da sempre, legata all'esistenza dello Stato, inteso come soggetto di diritto, il quale ha la competenza esclusiva in materia[131].

La *ratio* di questa ripartizione della competenza legislativa trova fondamento nell'interpretazione materiale del concetto di sicurezza pubblica.

La nozione di pubblica sicurezza è stata oggetto di numerose ricostruzioni dottrinarie volte a distinguerne i confini rispetto al concetto di «ordine pubblico», al quale è tradizionalmente e normativamente abbinato[132].

L'oggetto della sicurezza pubblica è dunque l'ordine pubblico, cioè «l'insieme dei principi etici e politici, la cui osservanza ed attuazione sono ritenute indispensabili all'esistenza di tale ordinamento, ed al conseguimento dei suoi fini essenziali»[133].

Questo è stato definito anche «il buon assetto o il regolare andamento del vivere civile, a cui corrispondono, nella collettività, l'opinione e il senso della tranquillità e della sicurezza»[134].

---

[130] «Sicurezza pubblica», *Dizionario Giuridico,* in *Brocardi.it.*
[131] Ai sensi dell'articolo 117 comma 1 lettera d) della Costituzione.
[132] F. Paolozzi, *Focus sulla giurisprudenza costituzionale in materia di sicurezza pubblica,* in *Osservatorio Regionale*, 2012, p. 887.
[133] F. Famiglietti, *La polizia di sicurezza, Manuale di diritto di pubblica sicurezza,* Roma, 2014, p. 20.
[134] M. Pellissero, M. Riverditi, *Reati contro la personalità dello stato e l'ordine pubblico,* Torino, 2014, p.33.

Se si condivide questa interpretazione la pubblica sicurezza deve intendersi come un mezzo attraverso il quale godere di altri diritti, relativi all'integrità fisica, morale e patrimoniale dei privati. Quindi le condotte che ledono uno o più soggetti, nuoceranno anche la sicurezza pubblica e di conseguenza la società.

Questo orientamento è confermato all'articolo 159 comma secondo del d.lgs. 112/1998, dove l'ordine pubblico è nuovamente definito come: «il complesso dei beni giuridici fondamentali e degli interessi pubblici primari sui quali si regge l'ordinata e civile convivenza nella comunità nazionale, nonché alla sicurezza delle Istituzioni, dei cittadini e dei loro beni» e la sicurezza pubblica come «l'insieme delle misure preventive e repressive dirette al mantenimento dell'ordine pubblico»[135].

In conclusione, da questo breve quadro si evince che ordine pubblico e sicurezza pubblica costituiscono una endiadi, in quanto si riferiscono allo stesso ambito concettuale e sono tra loro complementari. Questo è stato confermato da alcune sentenze della giurisprudenza costituzionale: la prima è la sentenza n.77 del 1987, attraverso la quale la Corte costituzionale ha definito la sicurezza pubblica come «la funzione inerente alla prevenzione dei reati o al mantenimento dell'ordine pubblico»[136]; definizione che è richiamata anche nella sentenza n. 218 del 1988 che traccia una prima distinzione tra "polizia amministrativa" e "pubblica sicurezza", definendo la prima come «le attività di prevenzione o repressione dirette ad evitare danni o pregiudizi che possono essere arrecati alle persone o alle cose nello svolgimento di attività ricomprese nelle materie sulle quali si esercitano le competenze regionali, senza che ne risultino lesi o messi in pericolo i beni o gli interessi tutelati in nome dell'ordine pubblico» e la seconda come «l'insieme delle misure preventive e repressive dirette al mantenimento dell'ordine pubblico»[137].

Queste definizioni sono state poi riprese e specificate dalla Corte con la sentenza n.115 del 1995, dove si dispone che la polizia di sicurezza ricomprenda «le misure preventive e repressive dirette al mantenimento dell'ordine pubblico, da intendersi quale complesso dei beni giuridici fondamentali o degli interessi pubblici primari sui quali si fonda l'ordinata convivenza civile dei consociati», e la polizia amministrativa ricomprende «le misure preventive e repressive dirette ad evitare danni o pregiudizi che possono derivare

[135] Rubricato: *Conferimento di funzioni e compiti amministrativi dello Stato alle regioni ed agli enti locali, in attuazione del capo I della legge 15 margo 1997, n.59* (G.U. n.92 del 21 aprile 1998, s.o. n.77/L).
[136] Corte Costituzionale, 27 marzo 1987, n. 77, in https://www.giurcost.org/decisioni/1987/0077s-87.html.
[137] M. Bombi, *Polizia amministrativa e pubblica sicurezza*, in *Diritto.it*, 2008.

alle persone e alle cose nello svolgimento di attività riconducibili alle materie sulle quali vengono esercitate competenze statali o regionali, senza che ne risultino giudicati o messi in pericolo gli interessi tutelati in nome dell'ordine pubblico»[138].

Questi concetti sono stati poi trasferiti nelle definizioni delle funzioni e dei compiti di Polizia amministrativa regionale-locale e nelle funzioni e compiti relativi all'ordine pubblico e alla sicurezza disciplinate nel già citato articolo 159 del d.lgs. 112/1988[139].

L'articolo 117 della nostra Carta Costituzionale, al comma secondo, lettera h), ha confermato allo Stato la competenza legislativa in materia di "ordine pubblico e sicurezza" escludendo esplicitamente la "polizia amministrativa locale" che, per l'operatività della clausola residuale contenuta nel quarto comma del medesimo articolo, è da ricomprendere tra le materie di competenza legislativa regionale. L'art. 118 invece prevede la possibilità di disciplinare con legge statale forme di coordinamento tra Stato e Regioni nelle materie "ordine pubblico e sicurezza" e "immigrazione".

Il quadro normativo cambia a seguito della riforma costituzionale del 2001, la quale ribalta la competenza esclusiva statale in materia di "ordine pubblico e sicurezza" e fa rientrare tra le materie di competenza legislativa regionale residuale, la "polizia amministrativa locale".

L'esclusione della materia "polizia amministrativa locale" e la conseguente collocazione tra quelle di competenza regionale residuale, hanno consentito alle Regioni di adottare delle proprie leggi di disciplina per le funzioni di polizia amministrativa e per le strutture di polizia locale deputate al loro esercizio[140].

Infatti, nel periodo seguente all'approvazione della riforma costituzionale, vengono approvate numerose leggi organiche a livello regionale, di riforma della polizia locale.

Inoltre, prendendo atto dell'interpretazione restrittiva del concetto di "sicurezza pubblica", molte delle leggi regionali approvate disciplinano, insieme alle funzioni di polizia amministrativa locale, anche l'istituzione di un "sistema integrato di sicurezza", al quale si possono ricondurre interventi in numerosi settori: la riqualificazione delle aree urbane degradate; la prevenzione di situazioni di disagio sociale; l'assistenza alle vittime

---

[138] F. Paolozzi, *Focus sulla Giurisprudenza Costituzionale in materia di Sicurezza Pubblica*, in *Servizio Affari legislativi e qualità dei processi normativi della giunta regionale,* Regione Emilia-Romagna, 2011, p.888

[139] F. Paolozzi, *Focus sulla Giurisprudenza Costituzionale in materia di Sicurezza Pubblica*, cit, *Ivi,* p.889.

[140] F. Paolozzi, *Focus sulla Giurisprudenza Costituzionale in materia di Sicurezza Pubblica*, cit, *Ivi,* p.890.

di reato e le azioni di supporto a controllo del territorio tra cui l'utilizzo di strumenti tecnologici.

La giurisprudenza costituzionale, a seguito della riforma del 2001, si è orientata verso un inquadramento della materia "ordine pubblico e sicurezza" con riferimento ai solo interventi finalizzati alla prevenzione dei reati e al mantenimento dell'ordine pubblico.

2.1.1. Smart City

Il crescente sviluppo di innovativi strumenti tecnologici ha portato anche ad un'innovazione, in termini generali, del concetto di sicurezza pubblica[141].

Una comunità non può progredire collettivamente finché non le verrà garantito un grado elevato di sicurezza fisica, assicurato in maniera sempre maggiore anche grazie all'introduzione dell'intelligenza artificiale e dei *software* predittivi[142].

Obbiettivo che è stato in parte raggiunto attraverso la creazione di *Smart City*, città che utilizzano le tecnologie ed i dati digitali per supportare le decisioni e migliorare la qualità della vita dei singoli individui. Queste città sono caratterizzate dall'integrazione tra strutture e mezzi tecnologicamente avanzati, proiettata verso politiche di crescita sostenibile al fine di ottenere un miglioramento degli standard qualitativi della vita umana[143].

Per realizzare una città intelligente è necessario tutelare e garantire la fruibilità dei servizi per la collettività e per il cittadino attraverso i migliori strumenti scientifici e tecnologici disponibili.

Perciò risulta adeguato alle nuove esigenze di questa comunità, un sistema integrato di sicurezza attraverso il quale si possano gestire e interconnettere tutti i settori pubblici e privati che condividono la gestione di beni e servizi essenziali per i cittadini.

Pertanto, sarebbe auspicabile puntare sulla gestione condivisa di diversi servizi con l'interconnessione su un'unica piattaforma digitale in grado di elaborare le informazioni

---

[141] Seagate, *L'intelligenza artificiale migliora le attività operative della pubblica sicurezza nelle città smart,* in *SEAGATE*, 2020.

[142] A tal proposito nel 2015, l'International Development Research Center ha chiesto ad un Gruppo di ricercatori di tutto il mondo «cosa rende sicura una città?». Un delegato della Repubblica Democratica del Congo ha affermato che «una città sicura è un luogo in cui le persone hanno l'opportunità di realizzare il loro potenziale, dove possono affermare di vivere in pace e di muoversi liberamente». Un delegato dell'India ha aggiunto che «la presenza della paura nella vita di una persona a volte può essere più destabilizzante dei casi di reale violenza».

[143] E. Ferrero, *Le Smart City nell'ordinamento giuridico,* in *Il Piemonte delle Autonome rivista quadrimestrale di scienze dell'Amministrazione,* 2014.

trasmesse dai sensori per soddisfare, non solo i bisogni dei cittadini, contribuendo a migliorarne la qualità di vita, ma anche le esigenze di controllo e di sicurezza del territorio[144].

In un contesto così innovativo ed in costante sviluppo come quello delle città intelligenti, sembrerebbe ancora più appropriato parlare di polizia predittiva.

Appare quindi sempre più evidente l'importanza crescente di migliorare le infrastrutture urbane attraverso sistemi di intelligenza artificiale e altre innovazioni tecnologiche.

[144] G. Cinque, *La sicurezza delle comunità connesse dev'essere «integrata»: ecco come realizzarla,* in *Agenzia Digitale*, 2022.

2.2. Le diverse funzioni di polizia.

Lo Stato tutela l'ordine e la legalità servendosi di quattro corpi di polizia:

- la Polizia di Stato,
- l'Arma dei Carabinieri,
- la Guardia di Finanza
- ed il Corpo di Polizia Penitenziaria.

I contenuti delle funzioni di polizia e l'assetto delle forze di polizia risentono di una tradizione legislativa italiana che comporta la presenza di più funzioni di polizia che possono essere svolte da una pluralità di corpi di polizia statali e locali, in ragione della quale si attuano varie forme di coordinamento[145].

Poiché la Costituzione non individua il contenuto delle singole funzioni di polizia, spetta al legislatore identificarle[146].

Le funzioni di polizia sono quella amministrativa e quella giudiziaria.

La polizia amministrativa si occupa dell'osservanza della legge e dei regolamenti amministrativi, per esplicare i compiti propri del potere esecutivo. Questa si distingue in molte qualificazioni, quali ad esempio: la polizia tributaria, la polizia sanitaria e la polizia di sicurezza[147].

Per quanto concerne la polizia di sicurezza, il professore emerito di Diritto processuale penale dell'Università di Firenze, Paolo Tonini, afferma che «La polizia di sicurezza ha come compito la tutela della collettività contro i pericoli e le turbative a interessi esistenziali per la vita di una società civile quali sono l'ordine pubblico (inteso come assenza di reati) e la sicurezza delle persone. In definitiva, la polizia di sicurezza è quella funzione che tende a prevenire il compimento di reati».

Questa è regolamentata nell'art 1 del testo unico delle leggi di pubblica sicurezza (TULPS) (R.D. 18 giugno 1931, n.773), il quale dispone che «L'autorità di pubblica sicurezza veglia al mantenimento dell'ordine pubblico, alla sicurezza dei cittadini alla loro incolumità e alla tutela della proprietà; cura l'osservanza delle leggi e dei regolamenti

[145] P. Bonetti, *Funzioni e corpi di polizia: problemi giuridici e prospettive per un riordino costituzionalmente orientato*, in *ASTRID*, 2009, p. 1.

[146] La sola forma di coordinamento costituzionalmente prevista è quella tra Stato e Regioni in materia di ordine pubblico e sicurezza.

[147] P. Tonini, *Manuale di procedura penale, G*iuffrè Francis Lefebvre, Milano, 2019, p. 126.

generali e speciali dello Stato, delle provincie e dei comuni, nonché delle ordinanze delle autorità; presta soccorso nel caso di pubblici e privati infortuni.
Per mezzo dei suoi ufficiali, ed a richiesta delle parti, provvede alla bonaria composizione dei dissidi privati.
L'autorità di pubblica sicurezza è provinciale e locale.
Le attribuzioni dell'autorità provinciale di pubblica sicurezza sono esercitate dal prefetto e dal questore, quelle dell'autorità locale dal capo dell'ufficio di pubblica sicurezza del luogo o, in mancanza, dal Podestà»[148].
Nell'ordinamento italiano la polizia di sicurezza ha quindi la funzione di prevenire non solo i reati, ma anche le cause generali di turbamento dell'ordine pubblico[149], essa ha carattere preventivo in quanto è tesa ad impedire qualunque violazione dell'ordine sociale.
La funzione di polizia giudiziaria invece, trova la sua definizione dell'articolo 55 del codice di procedura penale. Questo dispone che «La polizia giudiziaria deve, anche di propria iniziativa, prendere notizia dei reati, impedire che vengano portati a conseguenze ulteriori, ricercarne gli autori, compiere gli atti necessari per assicurarne le fonti di prova e raccogliere quant'altro possa servire per l'applicazione della legge penale.
Svolge ogni indagine e attività disposta o delegata dall'autorità giudiziaria.
Le funzioni indicate nei commi primo e secondo sono svolte dagli ufficiali e dagli agenti di polizia giudiziaria».
Il codice del 1988 colloca la polizia giudiziaria tra i soggetti del procedimento affidandogli un'attività prettamente investigativa, che consiste nella raccolta di tutti gli elementi necessari per accertare il reato e per rendere possibile lo svolgimento del processo penale.
Quindi la differenza tra la polizia di sicurezza e giudiziaria sta nella contrapposizione tra "prevenzione dei reati" e "repressione di un reato".
Questa distinzione ha finalità prettamente garantistiche. Quando svolge la funzione di prevenzione dei reati, la polizia non gode di poteri coercitivi, cioè non può direttamente

[148] R.D., 18 giugno 1931, n.773, in https://www.brocardi.it/testo-unico-pubblica-sicurezza/titolo-i/capo-i/art1.html.
[149] Tale attività, di norma, non dovrebbe comportare attività limitative di libertà costituzionalmente garantite da riserva di giurisdizione, per questo la funzione di polizia di sicurezza dipende funzionalmente da autorità di indirizzo politico amministrativo, con particolare riguardo per il Ministro dell'Interno, a cui compete in generale la tutela dell'ordine e della sicurezza pubblica, ed il coordinamento delle forze di polizia.

limitare le libertà fondamentali. Invece, quando giunge la notizia della commissione di un reato, viene posta in essere la funzione di polizia giudiziaria con l'utilizzo annesso dei poteri coercitivi.

In situazioni di necessità ed urgenza la polizia giudiziaria procede all'arresto in flagranza o al fermo di una persona gravemente indiziata; inoltre in caso di flagranza può perquisire persone o luoghi.

Le funzioni di polizia di sicurezza e giudiziaria sono poste sotto una differente dipendenza. La funzione di polizia di sicurezza è diretta da un organo unitario, il Ministro dell'Interno; in sede locale la direzione spetta al prefetto e al questore. Mentre la funzione di polizia giudiziaria è svolta sotto la direzione del Pubblico Ministero e sotto la sorveglianza del procuratore generale presso la Corte d'Appello[150].

[150] P. Tonini, *Op. cit.*, p.127.

2.3. Polizia Predittiva e Pubblica Sicurezza

L'autorità di pubblica sicurezza è quindi chiamata ad occuparsi di ordine pubblico e sicurezza pubblica per garantire la pace sociale. È mossa dall'intento di evitare o ridurre la possibilità che si verifichino fatti penalmente rilevanti, a tal fine, prevede i fattori che possano potenzialmente minacciarla e si adopera per annientare gli stati di turbativa già in essere.

L'attività di polizia di sicurezza non impone il rispetto di rigorosi criteri di acquisizione della prova, ma si focalizza sull'individuazione dei soggetti che potenzialmente stanno per commettere uno o più reati. Lo strumento tecnologico della polizia predittiva, parte dall'analisi dei dati, acquisiti dalle fonti più disparate, attraverso l'elaborazione dei quali tenta di prevenire e di rispondere al contenimento della consumazione di probabili attività illecite[151].

Quindi le forze dell'ordine, che agiscono nella funzione di pubblica sicurezza, possono utilizzare sistemi di polizia predittiva per affiancare il loro operato. Infatti, come abbiamo visto, in Italia, sono stati i funzionari di polizia stessi ad ideare i sistemi predittivi come KeyCrime ed XLAW.

Nel nostro ordinamento lo sfruttamento di un'intelligenza artificiale in questo campo non trova un limite delineato da disposizioni procedurali, ma piuttosto incontra un limite riguardante l'acquisizione di dati e d'informazioni che devono essere elaborati per l'utilizzo dei software in questione[152].

Sul piano prettamente teorico il meccanismo è semplice, ma il livello di efficacia di un *software* di questo tipo non può che dipendere dalla qualità, quantità e tempestività delle informazioni che dovranno essere analizzate.

Il quesito che bisogna porsi è se esistono o meno dei rischi di un'elaborazione informatica nelle prospettive sopra descritte[153].

Per quanto concerne l'attività della polizia di sicurezza, non sembrano esserci rischi oggettivi. La qualità di quest'ultima si misura sul numero di episodi di reato che riesce a

[151] L. Bennett Moses, J. Chan, *Algorithmic prediction in policing: assumptions, evaluation, and accountability*, in *Taylor & Francis Online*, 2016.

[152] C. Cath, S. Wachter, B. Mittelstadt, M. Taddeo, *Artificial Intelligence and the Good Society: the US, EU and UK approach*, Springer, 2018, p. 12.

[153] Argomento che è approfondito al paragrafo 2.4 del capitolo 2, riguardo alla polizia di sicurezza, ed al capitolo 3, riguardo a quella giudiziaria.

prevenire: una valutazione di efficacia facilmente oggettivabile, e come tale valutabile in termini trasparenti[154].

Le forze dell'ordine, nella funzione di pubblica sicurezza, applicano i metodi di polizia predittiva per distribuire le loro risorse in modo più efficiente ed efficacie all'interno del territorio.

In primo luogo, dai dati raccolti possiamo affermare che tra i benefici apportati da questi *software* vi è sicuramente la possibilità, per le risorse di polizia, di essere distribuite in modo più accurato nello spazio e nel tempo[155].

Inoltre, attraverso l'analisi dei dati storici criminali e quella delle informazioni recuperate attraverso il *data miming*[156], la polizia predittiva è in grado di individuare aree in cui vi è un rischio maggiore di una futura commissione di un reato[157].

Oltre all'individuazione del momento in cui l'attività criminale è maggiore in una specifica area geografica, attraverso l'attività di polizia predittiva, è possibile individuare ipotesi di ripetizione ravvicinata dei crimini. Teoria secondo la quale è più probabile che i crimini futuri avvengano in prossimità del momento e del luogo in cui sono avvenuti quelli attuali.

Quindi l'analisi di dati temporali e spaziali costituisce la base per la distribuzione delle risorse delle forze dell'ordine[158].

In secondo luogo, le tecniche di polizia predittiva aiutano ad identificare individui che potrebbero essere potenzialmente coinvolti in un atto criminale, sia come vittime sia come autori, attraverso attività di *profiling*[159].

L'obbiettivo di questa tecnologia è quindi quella di facilitare l'attività degli investigatori in termini di operatività, efficacia e rapidità. Ad oggi gli unici dati che ci sono stati forniti con riguardo all'efficacia concreta di questi *software* provengono dagli ideatori stessi.

Analizzando l'esperienza italiana sappiamo che la sperimentazione del software XLAW è avvenuta con successo nelle città di Napoli, Prato, Salerno e Venezia. Per esempio, a

---

[154] C. Parodi, V. Sellaroli, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco,* in *Diritto Penale Contemporaneo,* 2019, p. 55

[155] A. Meijer, M. Wessels, *Predictive Policing: Review of Benefits and Drawbacks,* in *Taylor & Francis Online,* 2019, p. 1031-1039.

[156] Sono dati che non hanno una rilevanza immediata ma che possono potenzialmente aiutare a prevenire e prevedere il verificarsi dei reati.

[157] Si riferisce alla *hot spot analysis* e alla *risk terrain analysis*.

[158] A. Meijer, M. Wessels, *Predictive Policing: Review of Benefits and Drawbacks,* cit, p. 1031-1039.

[159] La profilazione non si ferma ad un'analisi sulle caratteristiche demografiche degli individui, ma può consistere anche in individuazione di modelli comportamentali e sociali.

Napoli i crimini predatori sono diminuiti del 22%, mentre denunce ed arresti in flagranza di reato sono aumentati del 24%[160].

Inoltre, gli studi del Professore Giacomo di Gennaro[161] e Daniele Vasquez Pizzi[162] hanno dimostrato che attraverso questo sistema, è possibile un'accuratezza di previsione al 90% del comportamento delinquenziale. Anche i risultati forniti dalla Questura di Milano sul software KeyCrime sono significativi, poiché dimostrano che la soluzione dei casi effettuati attraverso questo meccanismo è passata dal 27%, nell'anno 2007 primo anno di sperimentazione, al 54% nell'anno 2013[163].

Anche lo stesso Mario Venturini, ideatore di *KeyCrime,* afferma che le rapine ai supermercati, ai negozi e alle farmacie sono calate del 57% da quando a Milano si utilizza l'algoritmo[164].

Sull'efficacia della polizia predittiva possiamo ricordare anche lo studio condotto dall'Università della California che segnala come nelle città in cui viene utilizzato il *software PredPol,* i crimini si siano ridotti in media del 7,4% con punte del 30%[165]. Il problema, già esaminato in precedenza, è che questo studio è stato condotto dagli ideatori stessi del sistema analizzante.

L'utilizzo di algoritmi di *predictive policing* volti alla prevenzione dei reati non consiste quindi in un'attività nuova di polizia. Le forze dell'ordine utilizzano da sempre strumenti di mappatura del crimine per indirizzare la propria attività di prevenzione. Ciò che oggi differisce è l'utilizzo combinato di strumenti di Intelligenza artificiale e di *Big Data.*

Purtroppo, ad oggi, non sono stati ancora condotti studi da parte di autorità esterne che possano confermare in maniera concreta e precisa i benefici apportati dai sistemi di polizia predittiva, all'interno delle città nelle quali vengono utilizzati. Ma possiamo affermare che l'impiego di questo software ha consentito di fare un salto di qualità nelle attività di polizia di sicurezza, anche solo per la possibilità dell'acquisizione e rielaborazione di una mole enorme di dati, scoprendo connessioni prima difficilmente individuabili dall'operatore umano.

---

[160] Regione Campania, *XLAW: L'algoritmo-poliziotto che prevede furti e rapine*, *cit.*

[161] Docente di sociologia e direttore del Master in criminologia dell'Università Federico II di Napoli.

[162] Antropologo culturale la cui ricerca è contenuta nel suo libro, *la fine della città post-moderna,* Mimesis, 2013.

[163] M. Venturi, *KeyCrime La chiave del crimine, I profili dell'abuso*, *cit.*

[164] A. D. Signorelli, *Quando l'algoritmo diventa sbirro: pro e contro della polizia predittiva,* in *vice*, 2016.

[165] R. Pelliccia, *Polizia predittiva: il futuro della prevenzione criminale?,* cit.

2.4. Limiti

I sistemi di polizia predittiva descritti possono indubbiamente apportare grandi benefici nella prevenzione almeno di alcune fattispecie di reato, ma il loro utilizzo suscita più d'una perplessità.

Le incertezze di questi *software* non riguardano solo i risultati effettivi, ma anche il modo in cui i dati vengono raccolti ed utilizzati.

In primo luogo, bisogna interrogarsi sull'opportuna ampiezza che il controllo umano deve assumere su tali applicazioni, soprattutto nel caso in cui esse utilizzino sistemi di intelligenza artificiale che ne assicurino ampi margini di autonomia: il controllo dell'uomo si deve limitare alla scelta degli obbiettivi, al monitoraggio, o deve essere un controllo più intenso, esercitato anche a costo di compromettere le prestazioni del software?

In secondo luogo, le preoccupazioni maggiori concernono le implicazioni che l'utilizzo di tali strumenti possono avere sull'individuo e sulla *privacy*. In considerazione della gran mole di dati che queste applicazioni possono acquisire in relazione alla vita, anche privata, dei cittadini: dati che, peraltro, potrebbero essere manipolati abusivamente, sottratti, deformati, con grave pregiudizio per le persone cui essi si riferiscono. L'individuazione delle modalità di raccolta dei dati nonché il funzionamento dell'algoritmo utilizzato, non è sempre facile e ciò potrebbe comportare la violazione dei diritti del cittadino. L'utilizzo dei dati personali che vengono raccolti da internet, come gli account sui social media e i filmati delle telecamere a circuito chiuso, pone seri rischi in materia di tutela della libertà personale.

Un altro fenomeno da analizzare è la profilazione, che oltre a compromettere la protezione dei dati personali della collettività rischia di tradursi in un ulteriore fattore di discriminazione. Si guardi in proposito all'esperienza americana con il software PredPol. Alcuni studi hanno evidenziato come il sistema risenta dei pregiudizi delle forze di polizia[166], ed anche per questo, in alcuni software, sono state escluse dal database le informazioni relative all'etnia[167].

---

[166] I. Ainora, *Polizia predittiva: la nuova frontiera dell'investigazione,* in *Informare, magazine di libera informazione*, 2022.

[167] Sono stati riscontrati problemi con il divieto di discriminazione, nella misura in cui, ad esempio, identificano fattori di pericolosità connessi a determinate caratteristiche etiche, religiose o sociali.

Un ulteriore limite da osservare è quello riguardante la mancanza di precisione, poiché l'affidabilità della polizia predittiva dipende dalla qualità dei dati e dall'integrità dei suoi esecutori ed utenti[168].

Oltretutto ci si chiede se non sarebbe il caso che, algoritmi con compiti di tale responsabilità e che maneggiano informazioni così delicate, fossero trasparenti ed analizzabili dall'opinione pubblica[169]. Non si deve infatti trascurare il fatto che la maggior parte di questi software sono coperti da brevetti depositati da aziende private, i cui detentori sono, giustamente, gelosi dei relativi segreti industriali e commerciali, sicché non si può disporre di una piena comprensione dei meccanismi e del loro funzionamento, con evidente pregiudizio delle esigenze di trasparenza, di verificazione indipendente della qualità e affidabilità dei risultati da essi prodotti[170].

Inoltre, la diminuzione dei reati per merito di questi programmi non deve far dimenticare che, compito della società non è solo quello di reprimere il crimine, ma anche di lavorare sulle cause socioeconomiche che hanno portato alla criminalità[171].

Da ultimo, occorre considerare che alcune di queste applicazioni sono equipaggiate con armi non letali o addirittura letali, ciò crea indubbiamente preoccupazioni in ordine al tasso di fallibilità di queste applicazioni e quindi in ordine all'individuazione del responsabile di eventuali uccisioni o lesioni commesse per errore, nonché in ordine alla presumibile assenza, in capo a questi dispositivi, di doti tipicamente umane[172], la cui presenza, in operatori di polizia è sempre auspicabile[173].

2.4.1. Tutela dei dati personali ai sensi della Direttiva (UE) 2016/680

La preoccupazione maggiore in relazione alla polizia predittiva attiene alla tutela del diritto alla *privacy* del cittadino.

Se da un lato è importate tutelare le informazioni personali dei singoli, dall'altro bisogna abbracciare e utilizzare in maniera efficace e tempestiva i risultati dell'evoluzione tecnologica in atto.

---

[168] A. Norga, *4 vantaggi e 4 svataggi della polizia predittiva,* in *Liberties*, 2021.
[169] A.D. Signorelli, *Il software italiano che ha cambiato il mondo della polizia predittiva*, in *wired,* 2019.
[170] F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi d'indagine,* cit, p. 14.
[171] A.D. Signorelli, *Quando l'algoritmo diventa sbirro: pro e contro della polizia predittiva*, cit.
[172] Doti come la pietà, la capacità di improvvisare, il senso comune, l'intuito.
[173] F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi d'indagine,* cit, p. 9-10.

La tutela della *privacy* è un diritto fondamentale dell'individuo alla protezione dei dati personali, riconosciuto dall'articolo 8 della Convenzione Europea dei Diritti dell'Uomo (CEDU). Rubricato con il titolo «Diritto al rispetto della vita privata e familiare», dispone che: «ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui»[174]. L'articolo in questione prevede che questo diritto può essere limitato solo nei casi previsti espressamente dalla legge e per il perseguimento di uno scopo legittimo, richiedendo quindi un bilanciamento tra interessi pubblici e privati[175].

Anche la Carta dei Diritti Fondamentali dell'Unione Europea (Carta di Nizza), all'articolo 8 riconosce la tutela dei dati personali, statuendo che: «Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente»[176].

Quindi il diritto alla protezione dei dati personali non è un diritto assoluto, e può essere oggetto di limitazioni per tutelare diritti e libertà altrui o per un interesse generale. Infatti, l'articolo 52 della Carta di Nizza, dispone che: «Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e

[174] Corte Europea dei Diritti dell'Uomo, *Guida all'articolo 8 della Convenzione europea sui diritti dell'uomo,* in https://www.echr.coe.int/documents/guide_art_8_ita.pdf, p.7.

[176] Carta dei Diritti Fondamentali dell'Unione Europea, *Articolo 8 – protezione dei dati di carattere personale*, in https://fra.europa.eu/it/eu-charter/article/8-protezione-dei-dati-di-carattere-personale.

rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere diritti e libertà altrui»[177].

In Italia il diritto alla tutela dei dati personali è disciplinato dal "pacchetto protezione dati" composto dal GDPR e dalla Direttiva (UE) 2016/680 sul trattamento dei dati personali in ambito penale, recepita in Italia con il d.lgs. 18 Maggio 2018, n.51[178].

Il GDPR all'articolo 2, n.2, lett. d, esclude dall'ambito applicativo del regolamento il trattamento dei dati personali effettuati dalle autorità competenti per finalità di «prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse». Queste finalità sono affermate anche dall'articolo 1 della Direttiva 2016/680[179].

Inoltre, la Direttiva disciplina il trattamento dei dati personali raccolti dalle autorità competenti nello svolgimento di attività di prevenzione, e nella verifica, indagine e perseguimento dei reati[180].

Il quadro così delineato può far evincere una distribuzione limpida dell'ambito di applicabilità del Regolamento e della Direttiva. In realtà non è così. In primo luogo, risulta necessario che il titolare del trattamento sia un'autorità di pubblica sicurezza e che le finalità di trattamento rientrino nell'ambito del GDPR o della Direttiva. Non è però semplice inquadrare le finalità del trattamento ed applicare la disciplina corretta.

---

[177] Carta dei Diritti Fondamentali dell'Unione Europea, *Articolo 52 – Portata e interpretazione dei diritti e dei principi*, in https://fra.europa.eu/it/eu-charter/article/52-portata-e-interpretazione-dei-diritti-e-dei-principi.

[178] Il d.lgs. n.51 del 2018 riproduce testualmente il testo della Direttiva 2016/680. Per questo motivo, al fine del seguente lavoro viene fatto riferimento alla Direttiva 2016/680.

[179] «La presente direttiva stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica».

[180] Direttiva 2016/680, *considerando n.12* «Le attività svolte dalla polizia o da altre autorità preposte all'applicazione della legge vertono principalmente sulla prevenzione, l'indagine, l'accertamento o il perseguimento di rati, comprese le attività di polizia condotte senza previa conoscenza della rilevanza penale di un fatto. Tali attività possono comprendere anche l'esercizio di poteri mediante l'adozione di misure coercitive quali le attività di polizia in occasione di manifestazioni, grandi eventi sportivi e sommosse. Esse comprendono anche il mantenimento dell'ordine pubblico quale compito conferito alla polizia o ad altre autorità incaricate nell'applicazione della legge ove necessario per la salvaguardia contro la prevenzione di minacce alla sicurezza pubblica e agli interessi fondamentali della società tutelati dalla legge che possono dar luogo a reati. Gli Stati membri possono conferire alle autorità competenti altri compiti che non siano necessariamente svolti a fini di prevenzione, indagine, accertamento o perseguimento di rati, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, cosicché il trattamento dei dati personali per tali altre finali altre finalità, nella misura in cui ricada nell'ambito di applicazione del diritto dell'Unione, rientra nell'abito di applicazione del regolamento (UE) 2016/679», in *Gazzetta ufficiale dell'Unione Europea, 2016, p. 2-3.*

Per poter comprendere appieno la disciplina sulla tutela dei dati personali, bisogna avere ben chiaro il concetto di dato personale. Per dato personale si intende «qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato)»[181]. Non sono annoverabili tra i dati personali i dati anonimi[182].

Un dato personale si definisce tale in quanto è in grado di identificare un soggetto, ma la sua portata cambia ogni volta che muta il soggetto titolare del trattamento. Per cogliere l'applicabilità della Direttiva 2016/680 alla fruizione di sistemi predittivi, occorre delimitare l'estensione dell'accezione di dato personale.

Il gruppo di lavoro per la protezione dei dati personali Articolo 29[183], afferma che l'utilizzo dell'espressione «qualsiasi informazione» ricalca la volontà del legislatore di ampliare il concetto di dato personale. Nozione all'interno della quale deve includersi qualsiasi informazione sia oggettiva che soggettiva, in qualsiasi formato, senza la necessità che sia constatata la veridicità dell'informazione, purché l'interessato abbia la possibilità di accedervi[184].

I sistemi di polizia predittiva si basano sull'elaborazione di diverse tipologie di dati, che possono essere definiti come personali, proprio grazie a questa interpretazione estensiva. Quindi risulta in modo chiaro che i dati trattati da questi *software* hanno il carattere di dati personali, poiché contengono informazioni su soggetti che devono essere identificati o riguardanti gruppi di individui[185].

A tal fine, si auspica ad un sempre più efficacie bilanciamento tra il diritto alla protezione dei dati personali, con l'interesse generale alle attività di prevenzione, indagine, accertamento e perseguimento dei reati.

---

[181] Direttiva (UE) 2016/680, articolo 3, n.1 e Regolamento (UE) 2016/679 (GDPR), articolo 4, n.1.

[182] Si definiscono come dati anonimi, quei dati che in origine, o a seguito di un trattamento, non possono essere associati ad un interessato identificato o identificabile. Sul punto M. Massimini, *Automatizzazione dei dati personali: significato, benefici e dubbi in ottica GDPR,* in *Privacy.it,* 2021.

[183] Il Gruppo di lavoro Articolo 29 era il gruppo di lavoro europeo indipendente che, fino al 25 maggio del 2018, entrata in vigore del RGPD, aveva lo scopo di occuparsi di questioni relative alla protezione della vita privata e dei dati personali.

[184] M. Lamanuzzi, *Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento 2017/679/UE e nuove responsabilità per gli enti*, in *vita e pensiero Jus,* 2017.

[185] O. Lynskey, *Criminal justice profiling and EU data protection law: precarious protection from predictive policing,* Cambridge University Press, 2019, p. 171.

2.4.2. Qualità, liceità e correttezza.

L'affidabilità della polizia predittiva dipende dalla qualità dei dati e dall'integrità dei suoi esecutori ed utenti.

Per poter assicurare la correttezza dei risultati proposti dall'algoritmo, è necessario che sia assicurata la qualità dei dati, anche a garanzia dei diritti fondamentali dell'individuo.

La qualità dei dati è tutelata dall'articolo 4, lett. d, della Direttiva (UE) 2016/680 la quale dispone che: «Gli stati membri dispongono che i dati personali siano esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati». Inoltre, l'articolo 7 della Direttiva (UE) 2016/680 distingue i dati in diverse categorie in base al grado di esattezza o di affidabilità, differenziando tra dati fondati su fatti, opinioni e valutazioni personali[186].

L'articolo 4 della Direttiva (UE) 2016/680 disciplina anche il trattamento dei dati personali, svolto dalle autorità di pubblica sicurezza o di qualsiasi altro organismo o entità del diritto dello Stato, che deve avvenire nel rispetto dei principi di liceità e correttezza[187].

In linea generale l'articolo 5 del GDPR disciplina i principi applicabili al trattamento dei dati personali, affermando che: «1. I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (liceità, correttezza e trasparenza); b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non si incompatibile con tali finalità; un ulteriore trattamento dei dati personali ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali (limitazione delle finalità); c) adeguati, preminenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattai (esattezza); e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano

[186] Direttiva (UE) 2016/680, articolo 3, n.1 «Gli Stati membri dispongono che i dati personali fondati su fatti siano differenziati, nella misura del possibile da quelli fondati su valutazioni personali».

[187] Direttiva (UE) 2016/680, articolo 4, n.1. lettera a) «Gli stati membri dispongono che i dati personali siano: trattati in modo lecito e corretto».

trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato (limitazione della conservazione); f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e della perdita, della distruzione o dal danno accidentali (integrità e riservatezza). 2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo (responsabilizzazione)»[188].

I principi disposti nel suddetto articolo sono attenuati se i dati personali vengono trattati dalle forze dell'ordine al fine di analisi di tipo predittivo o per altre finalità. Oltretutto a questi non viene applicato il principio di trasparenza poiché incompatibile con le finalità del trattamento stesso.

In questo caso non è neanche chiesto il consenso dell'interessato affinché il trattamento sia lecito, ma viene richiesto che esso sia necessario per l'esecuzione di un compito di un'autorità competente per le finalità di cui all'articolo 1 della Direttiva e si basi sul diritto dell'Unione o dello Stato membro.

Per quanto riguarda la correttezza, si deve guardare alla relazione che si viene a creare tra interessato e titolare del trattamento e all'obbligo del titolare di dimostrare la conformità del trattamento alla normativa. A tal fine, l'articolo 13 della Direttiva dispone che «Gli stati membri dispongono che il titolare del trattamento metta a disposizione dell'interessato almeno le seguenti informazioni: a) l'identità e i dati di contatto del titolare del trattamento; b) i dati di contatto del responsabile alla protezione dei dati, se del caso; c) le finalità del trattamento cui sono destinati i dati personali; d) il diritto di proporre reclamo a un'autorità di controllo e i dati di contatto di detta autorità; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati e la rettifica o cancellazione dei dati personali e la limitazione del trattamento dei dati personali che lo riguardano». Aggiungendo che in casi specifici il titolare del trattamento deve fornire all'interessato ulteriori informazioni riguardanti: «a) la base giuridica per il trattamento; b) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; c) se del caso, le categorie di destinatari dei

[188] Articolo 5 GDPR – Direttiva (UE) 2016/679, in *altalex.*

dati personali, anche in paesi terzi o in seno a organizzazioni internazionali; d) se necessario, ulteriori informazioni, in particolare nel caso in cui i dati personali siano raccolti all'insaputa dell'interessato»[189].

Per quanto concerne la finalità del trattamento, l'articolo 4 della Direttiva (UE) 680/2016, dispone che i dati devono essere raccolti per finalità determinate, esplicite e legittime e trattati in modo non incompatibile con tali finalità[190]. Ciò comporta che la finalità del trattamento sia determinata prima del trattamento e che qualsiasi altra operazione sia conforme alla finalità inizialmente definita.

Il suddetto articolo dispone che i dati raccolti potranno essere utilizzati dallo stesso o da altro titolare per qualsiasi attività di cui all'articolo 1 della Direttiva 680/2016 a condizione che: «il titolare del trattamento è autorizzato a trattare tali dati personali per detta finalità conformemente al diritto dell'Unione e dello Stato membro; e che il trattamento sia necessario e proporzionato a tale finalità conformemente al diritto dell'Unione o dello Stato membro», diversamente il trattamento per finalità differenti è vietato.

Conseguenza di detti principi è il diritto di accesso, rettifica e cancellazione dei dati personali in capo all'interessato.

L'articolo 15 del GDPR e l'articolo 8 della Carta di Nizza prevedono che l'interessato ha il diritto all'accesso dei dati personali che lo interessano. Se però il trattamento dei dati avviene secondo la Direttiva (UE) 680/2016, il diritto di accesso può essere limitato in virtù del bilanciamento tra il diritto del singolo e l'interesse degli stati membri in ordine al corretto svolgimento delle indagini, all'accertamento e al perseguimento di reati, all'esecuzione di sanzioni penali, alla tutela della sicurezza pubblica, e della tutela dei diritti e libertà altrui. Inoltre, l'interessato ha diritto alla rettifica dei dati inesatti e all'integrazione dei dati incompleti.

2.4.3. Controllo umano e mancanza di precisione.

La circostanza che i *software* predittivi si edificano sulla fruizione di *big data* e su approcci basati esclusivamente su informazioni, può avere importanti implicazioni sul

[189] Direttiva (UE) 2016/680 del Parlamento Europeo e del Consiglio dell'Unione Europea, in *Gazzetta ufficiale dell'Unione europea.*

[190] Direttiva (UE) 2016/680, Articolo 4, *lettera b) e c).*

modo in qui questi vengono utilizzati e avere come conseguenza negativa un'eccessiva enfasi sulle correlazioni tra questi, anzi che sulla casualità.

L'interferenza causale o ragionamento causale è oggi assente nei meccanismi di *machine learning* presi in considerazione dagli esperti di intelligenza artificiale, eppure essa è l'interferenza più rappresentativa dell'intelligenza umana poiché implica la previsione degli effetti delle proprie azioni. Il nostro mondo non è costituto da puri dati, piuttosto, i fatti sono uniti da un intricata rete di causa effetto. La maggior parte della nostra conoscenza è composta da spiegazioni causali, non da pure nozioni. Per questo le previsioni che derivano unicamente da algoritmi, poiché costitute esclusivamente sulla base di dati, risultano opache e difficili da interpretare. Perciò se i modelli predittivi esistenti non vengono esaminati e valutati con l'uso di istruzioni pratiche, questi saranno considerati obsoleti e per questo presenteranno un'immagine distorta della realtà. Ciò rafforza l'ipotesi secondo la quale, i modelli predittivi non possono mai essere utilizzati da soli senza ulteriori istruzioni da impartire agli agenti di polizia[191].

Attualmente i *software* predittivi non forniscono sufficienti raccomandazioni sul modo corretto di interagire con gli autori di un determinato reato, e neppure sulle modalità di utilizzo del sistema stesso.

A tal proposito, l'Unione Europea, investita della tematica, chiede che gli algoritmi siano in chiaro. Il che significa che l'utente, che sia il poliziotto o lo stato, deve sapere quale è il percorso analitico di un algoritmo.

Oltretutto i *software* di polizia predittiva utilizzano database che sono costituiti dalle informazioni raccolte dalla polizia stessa, tale connessione determina una componente soggettiva all'interno di questi, che non sono quindi slegati da pregiudizi. In virtù di ciò si evidenzia che la registrazione dei crimini non potrà mai essere obbiettiva e completa poiché si basa sui rapporti e sulle relazioni effettuate dagli agenti stessi. In questo senso può registrarsi una mancanza di precisione nelle informazioni raccolte e di conseguenza nei risultati ottenuti. Per esempio, le statistiche sul crimine collezionate sulla base di pregiudizi razziali, creeranno previsioni razziste, portando ad un eccesso di sorveglianza che continuerà a generare dati fuorvianti e previsioni a loro volta razziste. E proprio perché si tratta di sistemi che in una certa misura si auto-alimentano attraverso i dati prodotti dal loro stesso utilizzo, si prospetta il rischio di innescare un altro tipo di

[191] A. Meijer, M. Wessels, *Predictive Policing: Review of Benefits and Drawbacks,* cit, p. 1031-1039.

malfunzionamento: il fenomeno della "profezia che si auto-avvera". Ad esempio se un sistema predittivo individua una determinata "zona calda", i controlli ed il pattugliamento della polizia in quella zona si intensificano, con una conseguente crescita del tasso dei dati rilevati dalla polizia in quella zona, che diventerà, quindi, ancora più "calda", mentre altre zone, inizialmente non ricondotte nelle "zone calde", e quindi non presediate dalla polizia, rischiano di rimanere, o di diventare, per anni "zone fredde", dove la commissione di reati non viene adeguatamente monitorata[192].

2.4.4. Profilazione

Considerata l'evoluzione tecnologica in atto e, di conseguenza, l'aumento dei *Big Data*, il legislatore ha avvertito l'esigenza di disciplinare in maniera specifica la fattispecie della profilazione.

La profilazione è una tecnica di trattamento valutativo automatico che consiste nell'elaborazione mediante algoritmi di grandi quantità di dati riguardanti diversi individui, il tutto al fine di delineare per ciascuno di essi un "profilo". Si tratta di quelle attività di raccolta ed elaborazione dei dati collegati agli utenti di un servizio, al fine di suddividerli in gruppi a seconda del loro comportamento[193].

All'articolo 3 della Direttiva (UE) 2016/680, questa tecnica viene definita come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

In sintesi, si ha profilazione in presenza di tre elementi: un trattamento automatizzato; eseguito su dati personali; con lo scopo di valutare aspetti personali della persona fisica.

L'elaborazione automatica di dei dati personali può quindi costituire la base perché l'identità dell'individuo venga classificata e analizzata, le sue condotte valutate, le sue scelte previste e influenzate senza che egli se ne renda conto[194].

---

[192] F. Basile, *Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione*, in *il sistema penale ai confini delle hard sciences. Percorsi epistemologici tra neuroscienze e intelligenza artificiale*, Pacini Giuridica, 2021, p.6.

[193] B. Saetta, *Profilazione e processi decisionali automatizzati,* in *Protezione dati personali,* 2018.

[194] A. Punzi, *Diritto certezza e sicurezza,* G. Giappichelli editore – Torino, 2017, p.17.

Per aversi profilazione non basta il mero tracciamento dell'interessato che naviga online, o la classificazione dello stesso, occorre che si tratti di analisi per carpire decisioni riferite al soggetto o per prevederne le preferenze e i comportamenti. Si è in presenza di un processo decisionale automatizzato, quando vengono poste in essere decisioni impiegando mezzi tecnologici senza coinvolgimento umano. L'uso dei mezzi tecnologici ed il convincimento umano non sono necessariamente in un rapporto di dipendenza l'uno dall'altro, ma spesso le due cose tendono a coincidere[195].

L'utilizzo della profilazione "automatizzata", oggi sti sta diffondendo in molti settori.

I rischi a danno dell'individuo riguardano la poca chiarezza dei processi e meccanismi utilizzati ed il dislivello informativo che potrebbe sorgere tra il titolare del trattamento e l'interessato.

L'articolo 11 della direttiva (UE) 2016/680 disciplina il processo decisionale automatizzato relativo alle persone fisiche, disponendo che: «Gli stati membri dispongo che una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici negativi o incida significativamente sull'interessato sia vietata 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». Il d.lgs. n. 51 del 2018, nel recepimento della Direttiva 2016/680, prevede all'articolo 8 che «sono vietate le decisioni basate unicamente su un trattamento automatizzato, compresa la profilazione, che producono effetti negativi nei confronti dell'interessato, salvo che siano autorizzate dal diritto dell'Unione europea o da specifiche disposizioni di legge».

Quindi le decisioni basate esclusivamente sul trattamento automatizzato dei dati sono vietate.

A tal proposito il Considerando n. 38 della Direttiva (UE) 2016/680 dispone che «L'interessato dovrebbe avere il diritto di non essere oggetto di una decisione che valuta aspetti personali che lo concernono basata esclusivamente su un trattamento automatizzato e che produca effetti giuridici negativi nei suoi confronti o incida significativamente sulla sua persona. In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, compresi il rilascio di specifiche informazioni

[195] B. Saetta, *Profilazione e processi decisionali automatizzati*, cit.

all'interessato e il diritto di ottenere l'intervento umano, in particolare di esprimere la propria opinione, di ottenere una spiegazione della decisione raggiunta dopo tale valutazione e di impugnare la decisione. La profilazione che porti alla discriminazione di persone fisiche sulla base di dati personali che, per loro natura sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali dovrebbe essere vietata dalle condizioni stabilite negli articoli 21 e 52 della carta».

Alla luce di ciò, possiamo affermare che i sistemi di *predictive policing* sono sistemi di profilazione in quanto trattano dati personali al fine di prevenire il compimento di reati predicendo comportamenti di persone fisiche[196]. Per questo è necessario che nel processo risolutivo vi sia un contributo umano che verifichi la decisone proposta dall'algoritmo andando ad integrarla ovvero a convalidarla o confutarla.

Tuttavia, nonostante la Direttiva sancisca il divieto al trattamento automatizzato dei dati, tale tutela non risulta efficacie e soprattutto non risulta adeguata ad offrire la giusta protezione ai diritti dell'interessato.

Ciò che risulta essere particolarmente controverso è la definizione di quando la decisione si possa considerare «basata esclusivamente su un trattamento automatizzato»[197] e di conseguenza vietata.

Per questo si evince che gli strumenti offerti dalla Direttiva a tutela degli individui dal trattamento dei dati personali ai fini delle attività predittive, non risultano essere completamente esaustivi, o comunque risultano delineati e spiegati in maniera non sufficientemente adeguata[198].

Prova di questa incompletezza è appunto l'obbligo assegnato al titolare del trattamento, dall'articolo 12 della Direttiva, di fornire all'interessato le informazioni relative al trattamento dei dati, regolate dal successivo articolo 13[199]. L'adempimento di tale obbligo

---

[196] O. Lynskey, *Criminal justice profiling and EU data protection law,* cit., p.172.

[197] Articolo 11, Direttiva (UE) 2016/680.

[198] S. Wacher, B. Mittelstradt, L. Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation,* in *International Data Privacy Law, Oxford academic*, 2017, p.80.

[199] L'articolo 13 della Direttiva (UE) 2016/280, dispone che: «1. Gli stati membri dispongono che il titolare del trattamento metta a disposizione dell'interessato almeno le seguenti informazioni: a)l'identità e i dati di contatto del titolare del trattamento; b)i dati di contatto del responsabile della protezione dei dati, se del caso; c)le finalità del trattamento cui sono destinati i dati personali; d)il diritto di proporre reclamo a un'autorità di controllo e i dati di contatto di detta autorità; e)l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati e la rettifica o la cancellazione dei dati personali e la limitazione del trattamento dei dati personali che lo riguardano. 2. In aggiunta alle informazioni di cui al paragrafo 1. Gli stati membri dispongono per legge che il titolare del trattamento fornisca all'interessato, in casi specifici, le seguenti ulteriori informazioni per consentire l'esercizio dei diritti dell'interessato: a)la

risulta impossibile, poiché i software e gli algoritmi utilizzati sono quasi sempre coperti dal segreto commerciale, dal diritto d'autore e dalla tutela commerciale.

2.4.5. Dati biometrici

Importante è anche sottolineare la possibilità di utilizzazione del dato biometrico per il compimento di attività di profilazione e nello specifico per attività predittive.

«Il dato biometrico è un dato personale relativo alle caratteristiche fisiche, fisiologiche o comportamentali di un individuo mediante il quale ne consente l'identificazione univoca»[200].

Può essere definito come il risultato dell'applicazione della matematica biologica. Il dato biometrico rientra nelle categorie particolari di dati disciplinati dall'articolo 9 del GDPR, il quale prevede un elenco di dati definiti «particolari»[201], disponendo che: «1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le condizioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. 2. Il paragrafo 1 non si applica nei seguenti casi: a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi

base giuridica per il trattamento; b)il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzabili per determinare tale periodo; c) se del caso, le categorie di destinatati dei dati personali, anche in paesi terzi o in seno a organizzazioni internazionali; d)se necessario, ulteriori informazioni, in particolare nel caso in cui i dati personali siano raccolti all'insaputa dell'interessato. 3. Gli stati membri possono adottare misure legislative intese a ritardate, limitare o escludere la comunicazione di informazioni all'interessato ai sensi del paragrafo 2 nella misura e per il tempo in cui ciò costituisca una misura necessaria e proporzionata in una società democratica, tenuto conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata al fine di: a) non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari; b) non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali; c) proteggere la sicurezza pubblica; d) proteggere la sicurezza nazionale; e) proteggere i diritti e le libertà altrui. 4. Gli stati membri possono adottare misure legislative al fine di determinare le categorie di trattamenti cui può applicarsi, in tutto o in parte, una delle lettere del paragrafo 3».

[200] G. Ziccardi, P. Perri, *Dizionario Legal tech*, Giuffrè Francis Lefebvre, 2020, p. 314.

[201] Dati che venivano definiti dal codice della Codice Privacy come «sensibili».

del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali; g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato».

Quindi si tratta di dati che per loro natura richiedono maggiori garanzie. Per questi è previsto un divieto generale di trattamento, al quale fanno eccezione le ipotesi previste dall'articolo 9 del GDPR.

La Direttiva (UE) 2016/680 invece, non pone un divieto assoluto di trattamento di questa tipologia di dati. All'articolo 10 è previsto che il trattamento dei dati particolari è consentito «solo se strettamente necessario, soggetto a garanzie adeguate per i diritti e le libertà dell'interessato». È ovviamente necessario che il trattamento venga autorizzato dal diritto dell'Unione e dello Stato membro, che sia volto alla salvaguardia di un interesse vitale dell'interessato e che i dati particolari trattati siano resi pubblici dall'interessato stesso[202].

In sostanza la biometria si basa su sistemi informatici in grado di riconoscere ed identificare le persone sulla base di alcune caratteristiche biologiche come impronte digitali, altezza, sagoma della mano, colore e dimensione dell'iride. Sicuramente il riconoscimento biometrico può semplificare molte azioni della vita quotidiana, come lo sblocco del cellulare o l'accesso al conto in banca, ma diviene oggetto di molti interrogativi in tema di privacy.

A tal fine, la rivista inglese *Comparitech* ha stilato una graduatoria dei paesi in cui la sorveglianza, basata su raccolta di dati biometrici, è più stretta. L'Italia si colloca nella parte intermedia della classifica proprio a causa dei database della polizia. In cima alla classifica si trova invece la Cina, dove lo stato fa un uso talmente invasivo della biometria da permettere di parlare di «sorveglianza biometrica»[203]. Il sistema biometrico a Pechino è già usato nei passaporti, nelle carte d'identità e nei conti bancari, adesso si sta espandendo per arrivare alla creazione di un database nazionale che include il Dna. Secondo questa ricerca, la Cina fa un uso altamente invasivo della tecnologia di riconoscimento facciale nelle telecamere a circuito chiuso, che si calcolano cento telecamere ogni mille abitanti, e questo fa delle città cinesi le più sorvegliate al mondo[204]. Pechino ha introdotto il riconoscimento facciale anche per chi acquista una nuova Sim telefonica per il cellulare. Inoltre, le aziende sono state autorizzate a monitorare le onde celebrali dei dipendenti per verificarne la produttività mentre sono al lavoro.

[202] Articolo 4, Direttiva (UE) 2016/680.
[203] A. Mac, *Dati biometrici, la mappa della sorveglianza paese per paese,* in *Sole 24 ore,* 2019.
[204] A. Fonderi, *La pericolosa passione della Cina per i dati biometrici,* in *Wired,* 2020.

Problemi di sorveglianza si presentano anche per chi deve visitare, in qualità di turista, Pechino, infatti il visto per entrarvi viene rilasciato solo dopo aver rilevato le impronte digitali dei soggetti stranieri.

Oltretutto le autorità cinesi adottano, già da diversi anni, il sistema di «credito sociale» con il quale la popolazione viene categorizzata e valutata in base al proprio comportamento pubblico e al rispetto dei valori condivisi dal regime autocratico di Pechino.

Nel 2017 la NGO di New York è venuta in possesso di un App usata dalla polizia cinese per controllare e profilare una minoranza etnica[205], la cui analisi, condotta con il metodo del *reverse engineering*, ha svelato alcune zone d'ombra sulla sorveglianza messa in atto in tutti questi anni dal governo cinese. Il sistema è volto a sorvegliare circa dodici milioni di Uiguri. L'App in questione dispone di tre funzioni principali per collezionare dati informativi da vari sensori, riportare i dati di situazione e richiedere l'intervento degli investigatori con un segnale di allerta inviato automaticamente dal sistema[206]. Il controllo è basato su una piattaforma operativa integrata, in grado di acquisire dati da molteplici sensori come videocamere dotate di riconoscimento facciale e visione notturna. Inoltre, attraverso questo sistema, gli agenti di polizia riescono ad identificare i dispositivi telefonici dei cittadini e tracciarne le attività[207].

In aggiunta, il governo cinese, attraverso una piattaforma che porta il nome di *City Brain*, è in grado monitorare le condizioni del traffico, rileva incidenti stradali, regola i semafori per ridurre i tempi di viaggio e persino i tempi di risposta dei veicoli di emergenza. L'intelligenza artificiale di *City Brain*, asservita alle velleità del governo, è solo una delle tante applicazioni in grado di controllare i veicoli di un'intera città. Grandi quantità di dati biometrici vengono raccolte, elaborate da algoritmi, reinserite nei sistemi della citta e resi poi disponibili all'autorità. In Cina l'interesse pubblico prevale su quello del singolo, il controllo della società e le esigenze di pubblica sicurezza si impongono sui diritti degli individui[208].

---

[205] Si tratta degli Uiguri dello Xinjiang. Sono un'etnia turcofono di religione islamica che vive nel nord-ovest della Cina.

[206] A. Vecchio, *Xinjianf, Cina: sorveglianza e analisi predittiva si fanno con lo smartphone*, in *Difesa online*, 2019.

[207] *Ibidem*

[208] B. Calderini, *Sorveglianza di massa, la Cina è un sistema a "diritti affievoliti": perché lo tolleriamo e cosa rischiamo*, in *Agenzia Digitale*, 2022.

In conclusione, quello tra l'occidente e la Cina non è quindi un rapporto di sole relazioni tra governi, ma una connessione tra le diverse percezioni che i rispettivi cittadini hanno su temi divisivi, come può esserlo quello dei diritti fondamentali. La necessità di pensare in modo critico e consapevole sui sistemi di sorveglianza ed in generale sull'intelligenza artificiale risulta evidente. Se da una parte la strategia cinese mira al controllo totalitario della propria società e al predominio scientifico, dall'altra negli stati occidentali si è venuta a creare una biforcazione tra settore pubblico e privato, dove i privati mirano alla mercificazione delle opportunità tecnologiche e il pubblico cerca di sorvegliare e regolare il loro utilizzo.

2.4.6. Discriminazione

L'utilizzo di *software* predittivi potrebbe comportare problematiche che riguardano la discriminazione e la parità di trattamento.

Per discriminazione si intende il trattamento differenziato di individui appartenenti, regolarmente o apparentemente, a specifici gruppi sociali[209].

Come anticipato nei capitoli precedenti il rischio è generato dal fatto che gli algoritmi predittivi si ergono sulla base di dati espressivi di una scelta discrezionale delle forze dell'ordine. I dati vengono infatti raccolti dalle forze dell'ordine stesse, secondo criteri e modalità da questi regolate, ciò comporta che il modello di criminalità ottenuto spesso è diverso da quello realmente posto in essere[210]. Poiché la polizia predittiva si basa sul *machine learning*, un modello statistico il cui funzionamento è presieduto anche da decisioni umane, risulta intuitivo osservare che se i dati con cui viene istruita sono viziati, vi è un elevata possibilità che lo siano anche le previsioni che ne risultano[211].

Un esempio esplicativo di un software affetto da questo tipo di vizi è l'americano PredPol. A causa dei dati inesatti inseriti dalle forze dell'ordine, la conseguenza è stata una presenza massiccia di polizia nei quartieri che erano già storicamente sorvegliati in maniera sufficiente e l'inesatta copertura di molte altre zone della città. A tal proposito decenni di ricerca criminologica hanno mostrato che i dati riguardanti arresti e denunce

[209] K. Lippert-Rasmussen, *Born free and equal? A philosophical inquiry into the nature of discrimination,* in *Oxford University Press*, 2014, p.111.
[210] M. Martona, L. Pinelli, *Algoritmi di polizia predittiva: la discriminazione è alla fonte,* cit.
[211] E. Tulumello, *Se prevedere il crimine discrimina, polizia predittiva, algoritmi che discriminano. La matematiche rimane neutrale?,* in *Monnalisa bytes,* 2020.

non costituiscono un campione statistico rappresentativo dell'attività criminale. Al contrario, i crimini registrati raffigurano una percentuale inferiore rispetto a quelli che vengono effettivamente commessi, facendo evincere una discriminazione sistematica verso specifici gruppi etnici, prevalentemente verso neri e latini, e specifici quartieri, si tratta di quelli più poveri e con meno servizi per i cittadini.

Influente è anche il rapporto che le varie comunità hanno con la polizia stessa, quando si è disposti a chiamarla in aiuto o quando ci si sente, invece, da essa minacciati.

Numerosi dati e fatti di cronaca dimostrano che, negli Stati Uniti, l'utilizzo della forza da parte degli agenti di polizia nei confronti di persone nere è molto diffuso, tanto da essere realmente preoccupante.

Uno studio effettuato nel 2016 da Kristian Lum e William Isaac, due statisti dello H*uman Rights Data Analysis Group*[212], ha confermato che i dati in possesso della polizia sono affetti da pregiudizi, di conseguenza se il *software* PredPol viene istruito con tali informazioni, è altamente probabile che generi predizioni che rinforzano quei pregiudizi.

Innanzitutto, i ricercatori hanno messo a confronto i dati relativi all'uso illegale di droga raccolti dalla polizia di Oakland, California, con quelli provenienti dall'indagine nazionale sull'uso di droga e salute, relativi ad uno specifico anno. Lo studio ha dimostrato che i dati provenienti da queste due fonti raffigurano un quadro completamente differente. Innanzitutto, si evince che i dati provenienti dall'indagine nazionale, quindi pubblici, suggeriscono una distribuzione uniforme dall'uso illegale di droga, con un'equivalenza tra le zone più ricche ed abitate prevalentemente da bianchi e quello più periferiche. Gli arresti legati a questo tema però sono concentrati in quartieri della città notoriamente frequentati da persone di carnagione non bianca ed appartenenti ad una fascia di reddito molto bassa. In queste zone si registrano fino a duecento arresti un più rispetto alle zone centrali.

Infine, Kristian Lum e William Isaac hanno istruito l'algoritmo Pred Pol con i dati dell'indagine nazionale, ed hanno contato quante volte, per ogni giorno dell'anno, l'algoritmo predicesse il verificarsi di un crimine all'interno di una determinata zona della città. Piuttosto che mitigare il bias, PredPol lo ha rinforzato, ha infatti indicato come zone a rischio quelle già soggette ad una sorveglianza più elevata. Dalla suddetta analisi è emerso che, a fronte di un uso di droga proporzionalmente uguale tra cittadini bianche e

[212] K. Lum, W. Isaac, *To predict and serve?,* in *Royal Statistical Society,* 2016, p. 14-19.

neri, PredPol avrebbe indicato come target la comunità nera il doppio delle volte di quella bianca. Questa predizione indica come la discriminazione contenuta nei dati, e quindi radicata all'interno di essi, possa essere riproposta e rinfornata attraverso le previsioni dell'algoritmo.

Ugualmente, l'*American Civil Liberties Union*[213] ha criticato questa pratica poiché tendente a perpetrare il *profiling* razziale; se alimentato con dati distorti, l'algoritmo ingrandisce i pregiudizi che emergono dai processi convenzionali, intensificandone ulteriormente le discrepanze ingiustificate nell'applicazione[214]. Oltretutto questa dinamica, a livello sistematico potrebbe minare gli obbiettivi vitali della polizia, tra cui la costruzione della fiducia della comunità.

Anche il parlamento europeo si è pronunziato al riguardo, attraverso la Risoluzione sull'Intelligenza Artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia in ambito penale. Tramite questa risoluzione, adottata nel 2021, il Parlamento ha evidenziato gli aspetti positivi dell'Intelligenza Artificiale in molti degli ambiti in cui opera, ma anche come allo stesso tempo l'applicazione di quest'ultima violi diritti fondamentali e porti spesso a risultati discriminatori [215].

Al punto n. 8 la Risoluzione sottolinea come «l'uso di applicazioni basate sull'intelligenza artificiale come l'apprendimento automatico, compresi gli algoritmi sui quali sono basate tali applicazioni, potrebbero comportare distorsioni e discriminazioni;…ricorda che il risultato fornito dalle applicazioni di IA p necessariamente influenzato dalla qualità dei dati utilizzati e che tali questioni distorsioni intrinseche sono destinate ad aumentare gradualmente quindi a perpetuare e amplificare

[213] L'unione Americana per le Libertà Civili è un'organizzazione non governativa orientata a difendere i diritti civili e le libertà individuali negli Stati Uniti.

[214] A. Norga, *4 vantaggi e 4 svantaggi della polizia predittiva,* cit.

[215] Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia giudiziaria in ambito penale (2020/2016 (INI), Lettera A "considerando che le tecnologie digitali in genere e la diffusione del trattamento e analisi dei dati dovuta all'intelligenza artificiale (IA) in particolare portano con sé promesse e rischi straordinari; che lo sviluppo dell'IA ha compiuto un notevole balzo in avanti in anni recenti che la rende una delle tecnologie strategiche del XXI secolo, con il potenziale di generare notevoli benefici in termini di efficienza europea, ma comporta anche rischi enormi per i diritti fondamentali e le democrazie basate sullo Stato di diritti; che l'IA non dovrebbe essere vista come fine a se stessa, ma come uno strumento al servizio delle persone, con lo scopo ultimo di accrescere il benessere degli esseri umani, le capacità umane e la sicurezza".

le discriminazioni esistenti, in particolare nei confronti delle persone che appartengono a determinate minoranze o comunità razziali;»[216].

Inoltre, al punto n.8 il Parlamento «osserva che se gli esseri umani fanno affidamento unicamente sui dati, i profili e le raccomandazioni generati dalle macchine, non saranno in grado di condurre una valutazione indipendente; evidenzia le ripercussioni negative potenzialmente gravi, in particolare nel settore delle attività di contrasto e della giustizia, qualora le persone ripongano eccessiva fiducia nella natura apparentemente oggettiva e scientifica degli strumenti di IA e non considerino la possibilità che tali strumenti conducano a risultati errati, incompleti, non pertinenti o discriminatori;»[217].

In aggiunta, al punto n.24, la Risoluzione: «osserva che la polizia predittiva è tra le applicazioni di IA utilizzate nell'ambito delle attività di contrasto ma avverte che se da un lato la polizia predittiva può analizzare gli insieme di dati forniti per l'identificazione di modelli e correlazioni, essa non può dare una risposta alla questione della causalità, non può fare previsioni sui comportamenti degli individui e pertanto non può costituire l'unica base per un intervento; sottolinea che diverse città degli Stati Uniti hanno interrotto l'uso dei sistemi di polizia predittiva in seguito agli audit; ricorda che durante la missione della commissione LIBE negli Stati Uniti nel febbraio 2020, i membri sono stati informati dai dipartimenti di polizia di New York City e Cambridge, Massachusetts, che avevano eliminato gradualmente i loro programmi di polizia predittiva a seguito della loto inefficacia, nell'impatto discriminatorio e dell'insuccesso pratico ed erano tronati a sistemi di polizia di quartiere; osserva che ciò ha portato a una riduzione del tasso di criminalità; si oppone, peraltro, all'utilizzo dell'IA da parte delle autorità di contrasto per fare previsioni sui comportamenti degli individui o di gruppi sulla base di dati storici e condotte precedenti, all0appartenenza a un gruppo, l'ubicazione o qualunque altra caratteristica al fine di identificare le persone che potrebbero commettere un reato;».

Essa, premesso che il fatto che i dati utilizzati al fine della polizia predittiva rispecchiano quelle che sono le priorità della sorveglianza delle forze dell'ordine e che questo aumenti il rischio di trattamenti discriminatori, evidenzia l'importanza che vi siano gruppo

[216] Risoluzione del Parlamento europeo sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia in ambito penale, in https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_IT.html.

[217] Risoluzione del Parlamento europeo sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia in ambito penale, in https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_IT.html.

interdisciplinari di progettazione, sviluppo e manutenzione dei sistemi di IA per attività di contrasto e giudiziarie, che i decisori abbiano competenze tecniche adeguate e professionali adeguate che consentano loro di individuare eventuali distorsioni e discriminazioni e che gli stati membri adottino politiche di contrasto alla discriminazione e piani nazionali contro il razzismo nell'ambito delle attività di polizia e nel sistema giudiziario[218].

Il Parlamento europeo riconosce quindi che i risultati forniti dai sistemi di intelligenza artificiale sono necessariamente influenzati dalla qualità dei dati utilizzati e che tali pregiudizi intrinseci sono inclini ad aumentare gradualmente quindi a perpetuare e amplificare le discriminazioni esistenti, in particolare per le persone appartenenti a determinati gruppi etnici o comunque «ratealizzate». Si nota, altresì, che molte tecnologie di identificazione guidate da algoritmi attualmente in uso identificano e classificano erroneamente in modo sproporzionato e quindi causano danni alle suddette persone ratealizzate, agli individui appartenenti a determinate comunità etniche, alle persone LGBT, ai bambini e agli anziani, nonché alle donne[219].

2.4.7. Trasparenza

Un altro limite che appartiene all'utilizzo dei *software* di polizia predittiva riguarda la mancanza di trasparenza dell'algoritmo stesso.

La mancanza di conoscenza del processo decisionale posto in essere da parte dell'algoritmo genera molte preoccupazioni, soprattutto perché ciò potrebbe comportare il conseguimento di risultati discriminatori.

Per "trasparenza" si intende la disponibilità di rendere accessibili all'utente informazioni circa il processo decisionale dell'algoritmo[220].

[218] Risoluzione del Parlamento europeo sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia in ambito penale, punto 22, 2021, in https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_IT.html.

[219] M. Martorana, *Intelligenza Artificiale e diritto penale, la risoluzione del Parlamento europeo,* in *Altalex,* 2021.

[220] B. Perego, *Predictive policing: trasparenza degli algoritmi, impatto sulla privacy e risvolti discriminatori,* in *BioLaw Journal Rivista di Biodiritto,* 2020.

La trasparenza dell'algoritmo, ovvero il «diritto alla decifrazione dei trattamenti decisionali automatizzati» rappresenta un punto di partenza fondamentale per le applicazioni dell'IA[221].

La trasparenza è generalmente definita rispetto alla «disponibilità di informazioni, le condizioni di accessibilità e come le informazioni… possono supportare in modo pragmatico o epistemico il processo decisionale dell'utente»[222]. Il valore della trasparenza per il controllo predittivo si rivela estremamente significativo, affinché questi *software* vengano utilizzati in modo efficacie, legale ed etico.

La trasparenza algoritmica consente di individuare la dinamica dei flussi di dati che vengono utilizzati dal sistema e permettere di ragionare sul motivo per il quale, ad esempio, una decisione elaborata dal sistema di IA possa essere considerata errata, inoltre consente di introdurre presidi correttivi funzionali alla prevenzione della reiterazione futura dell'errore.[223]

L'articolo 20 della Direttiva (UE) 2016/680 afferma infatti che: «gli stati membri dispongono che il titolare del trattamento, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità di trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituitisi dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, metta in atto misure tecniche e organizzative adeguate, quali la pseudo minimizzazione, volte ad attuare in modo efficacie principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti della presente direttiva tutelare i diritti degli interessati».

Aggiungendo che «Gli stati membri dispongono che il titolare del trattamento metta in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la qualità dei dati personali raccolti, la portata del

---

[221] M. Bonafe, C. Trevisi, *Intelligenza artificiale, l'algoritmo "trasparente": un rebus ancora da sciogliere,* in *Agenda Digitale*, 2019.

[222] Parlamento Europeo, *Report on foundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement,* 2017, in https://www.europarl.europa.eu/doceo/document/A-8-2017-0044_EN.html,

[223] M. Bonafe, C. Trevisi, *Intelligenza artificiale, l'algoritmo "trasparente": un rebus ancora da sciogliere,* cit.

trattamento, il periodo di conservazione e l'accessibilità. In particolare, tali misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica»[224]. Questo articolo riconosce all'individuo un diritto alla trasparenza dell'algoritmo, imponendo la trasparenza come elemento necessario nella formulazione dell'algoritmo e nell'elaborazione automatizzata di dati, prevedendo una serie di doveri in capo al titolare del trattamento.

Per quanto concerne la polizia predittiva, allo stato attuale delle tecnologie impiegate vi è una mancanza di trasparenza a tutti i livelli[225]. Quindi senza investimenti significativi volti a comunicare i metodi di raccolta dei dati, e senza un uguale investimento nella comprensione delle sfide associate all'inserimento e all'analisi dei dati, l'intero sistema corre il rischio di essere costruito su database sconosciuti e non conoscibili.

Nell'aprile del 2021 è stata presentata una proposta di Regolamento del Parlamento Europeo e del Consiglio alla Commissione europea, per disciplinare ed armonizzare le regole in materia di Intelligenza artificiale. L'intento di questo regolamento è quello di evitare una frammentazione normativa tra stati membri e creare un mercato unico in materia di IA in Europa.

L'Artificial Intellicence Act si applicherà a fornitori, importatori e distributori, sia pubblici che privati, che immettono sistemi di IA nel territorio dell'Unione anche se gli stessi sono stabiliti in un paese terzo. Uno dei doveri previsti da questo regolamento è quello della trasparenza. All'articolo 13 è sancito un esplicito obbligo di trasparenza per gli sviluppatori di software di IA ad alto rischio, imponendo che gli stessi siano «progettati e sviluppati in modo tale da consentire agli utenti di interpretare l'output del sistema e utilizzarlo adeguatamente». I fornitori devono inoltre «garantire istruzioni d'uso che riportino informazioni circa l'identità e i contatti del fornitore, le caratteristiche, le capacità e i limiti della prestazione del sistema di IA, le possibili modifiche e del suo funzionamento nonché gli eventuali interventi di manutenzione necessari»[226].

---

[224] Direttiva (UE) 2016/680, Articolo 20.

[225] J.F. Gilsinan, *The Numbers Dilemma: The Chimera of Modern Police Accountability System,* in *St. Luis University Public Law Review,* 2012.

[226] Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'Intelligenza Artificiale) e modifica alcuni atti legislativi dell'Unione, Articolo 13, par. 2 e 3, in https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0206&from=IT.

Tali obblighi rapprenderebbero un buon punto di parenza al fine di limitare quanto più possibile i rischi che l'opacità degli algoritmi comportano. Tuttavia, è necessario che siano indicate line guida con esempi concreti sulle misure specifiche richieste al fine di non lasciare margini di libera interpretazione al fornitore del sistema.

Anche la Corte di Cassazione si è pronunciata in tema di trasparenza dell'algoritmo[227]. L'associazione Mavaluate Onlus ha chiesto al Tribunale di Roma l'annullamento del provvedimento del Garante per la protezione dei dati personali. Questa associazione, costituita nel 2013, offre un servizio volto a misurare e dare valore alla reputazione reale di persone, aziende ed enti. La società detiene la proprietà intellettuale del *Rating Reputazionale* e di tutto il Sistema Digitale di Qualificazione Reputazionale ed è strutturata per poter operare in tutti il mondo attraverso organizzazioni locali[228]. Nel 2016 il garante pe la protezione dei dati personali ha dichiarato l'associazione illecita a causa della forte incidenza del servizio sulla dignità dei soggetti interessati e ha disposto il divieto di qualsiasi tipo di trattamento dei dati personali in quanto la stessa aveva violato gli articoli 2,3,11,23,24,26 del codice Privacy[229].

Il Tribunale di Roma ha accolto il ricorso presentato dalla società, annullando con sentenza il provvedimento del Garante per la protezione dei dati personali, affermando la competenza del mercato nello «stabile l'efficacia e la bontà del risultato presentato»[230]. In seguito, la Corte di Cassazione, attraverso l'ordinanza 14282/2021, ha stabilito che la motivazione data dal tribunale di Roma non è condivisibile in quanto il problema non è «confinabile nel perimetro della risposta del "mercato", bensì attiene alla validità del consenso che si presume prestato al momento dell'adesione».

In conclusione, la corte di cassazione ha stabilito che il tribunale di Roma dovrà procedere ad un nuovo giudizio uniformandosi al dispositivo principio di diritto il quale precisa che in tema di trattamento di dati personali, il consenso è validamente prestato solo se espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato. Quindi nel caso di una piattaforma web che sia preordinata all'elaborazione di profili reputazionali di singole persone fisiche o giuridiche, e incentrata su un sistema di calcolo con alla base un algoritmo finalizzato a stabilire i punteggi di affidabilità, il

[227] Attraverso l'Ordinanza 14282/2021.
[228] Gruppo Meacaluate, Mevaluate Holding Ltd, in Cropnews, 2018.
[229] M. Iaselli, *Sistemi automatizzati per il consenso serve la trasparenza dell'algoritmo,* in *Altalex*, 2021.
[230] Corte di Cassazione, Sezione I Civile, Ordinanza n.14382/2021, punto VII.

requisito di consapevolezza non può considerarsi soddisfatto ove lo schema esecutivo dell'algoritmo e gli elementi di cui si compone risultino ignoti o non conoscibili da parte degli interessati. Secondo tale principio di diritto, per trasparenza di deve quindi intendere ancora una volta la conoscibilità dello schema esecutivo e degli elementi di cui l'algoritmo è composto.

Essere espliciti sulle scelte e sulle decisioni che riguardano le fonti, i dati, i processi di sviluppo e le parti interessate, può contrapporsi ad un'altra esigenza: la protezione dei segreti industriali.

Se da un lato, alcune aziende rivendicano il diritto di mantenere il codice sorgente per sé stesse, trattando i loro algoritmi come segreti commerciali[231]. Dall'altro, la ragione tecnica di tale mancanza di trasparenza è legata al fenomeno della scatola nera (*back box*) e quindi, in molti casi in cui vengono impiegate tecnologie basate su algoritmi, gli agenti di polizia coinvolti nel funzionamento dei programmi non avranno alcuna comprensione di come lavora l'algoritmo.

Se quindi da un lato, il segreto industriale consente, oltre alla tutela degli investimenti economici connessi al regime di protezione, di scongiurare il rischio di manipolazione degli algoritmi, dall'altro, tale protezione ma si concilia con i principi di trasparenza e comprensibilità algoritmica.

Quindi la trasparenza può aiutare a prevenire la discriminazione e la stigmatizzazione (ad esempio attraverso la scelta delle variabili da parte del programmatore e i metodi di raccolta dei dati), ma è anche improbabile che corregga il difetto di applicazione. Al fine di prevenire conseguenze dannose per i diritti individuali, è necessario che i programmi di polizia predittiva siano attuati in modo trasparente ma ciò non è sufficiente: se non porta alla correzione di distorsioni codificate nei dati o all'uso di informazioni sporche, la trasparenza risulta piuttosto vuota come principio istituzionale.

[231] E. E. Joh, *The Undue Influence of survelliance Tecnology companies on Policing,* in *New York University Law Review Online,* 2017.

3. Nuove tecnologie nella funzione di polizia giudiziaria

3.1. Polizia giudiziaria e giustizia predittiva

Le funzioni di polizia sono quella amministrativa e quella giudiziaria, come esposto nel Capitolo 2, al paragrafo 2.

In questa sede occorre chiarificare il ruolo della polizia giudiziaria, per comprendere al meglio il concetto di giustizia predittiva. La funzione di polizia giudiziaria trova la sua definizione nell'articolo 55 del codice di procedura penale, il quale dispone che: «La polizia giudiziaria deve, anche di propria iniziativa, prendere notizia dei reati, impedire vengano portati a conseguenze ulteriori, ricercarne gli autori, compiere gli atti necessari per assicurare le fonti di prova e raccogliere quant'altro possa servire per l'applicazione della legge penale». A differenza della polizia di sicurezza, che si occupa della "prevenzione dei reati", quella giudiziaria si impegna alla "repressione di un reato", ossia alla raccolta di tutti gli elementi necessari per accertare il reato e per rendere possibile lo svolgersi del processo penale. Di conseguenza, quando giunge la notizia della commissione di un reato, viene posta in essere la funzione di polizia giudiziaria con il successivo utilizzo dei poteri coercitivi[232]. In aggiunta, in situazioni di necessità ed urgenza, quest'ultima può procedere all'arresto in flagranza o al fermo di una persona gravemente indiziata, inoltre, in caso di flagranza può perquisire persone o luoghi.

L'articolo 55 del c.p.p. aggiunge che: «svolge ogni indagine e attività disposta o delegata dall'autorità giudiziaria. Le funzioni indicate dai commi precedenti sono svolte dagli ufficiali e dagli agenti di polizia giudiziaria»[233].

Il professore emerito Paolo Tonini afferma: «la polizia giudiziaria è svolta sotto la direzione del pubblico ministero e sotto la sorveglianza del procuratore generale presso la corte d'appello», aggiungendo che «colui che svolge funzioni di polizia giudiziaria dipende funzionalmente dal pubblico ministero e organicamente dal potere esecutivo. Per tale motivo vi è il pericolo che le direttive dell'autorità giudiziaria siano ostacolate da direttive in senso contrario provenienti dagli organi del potere esecutivo. In concreto, vi

[232] L'esercizio di poteri coercitivi avviene in relazione al successivo svolgersi di un procedimento penale, con la garanzia del diritto di difesa e sotto il controllo del pubblico ministero e del giudice.
[233] Codice di Procedura Penale, articolo 55.

è il rischio che, in relazione a determinati reati, non siano ricercate le fonti di prova e non siano eseguite con la dovuta solerzia le direttive dell'autorità giudiziaria»[234].

La polizia giudiziaria dipende quindi dall'autorità giudiziaria, il codice[235] distingue tre strutture che svolgono funzioni di polizia giudiziaria, pur restando i singoli agenti ed ufficiali sotto la dipendenza "organica" del corpo di appartenenza. Le strutture si caratterizzano per il diverso grado di dipendenza funzionale dall'autorità giudiziaria[236].

In primo luogo, come disposto dalla lettera *b* dell'articolo 56 c.p.p., il maggior grado di dipendenza è riconosciuto «alle sezioni di polizia giudiziaria istituite presso ogni procura della Repubblica e composte con personale dei servizi di polizia giudiziaria».

In secondo luogo, come disposto dalla lettera *a* dell'articolo 56 c.p.p., un minor grado di dipendenza funzionale è riscontrabile nei «servizi di polizia giudiziaria previsti dalla legge». Questi sono costituiti presso i corpi di appartenenza.

Infine, gli organi di polizia giudiziaria che non sono ricompresi nelle sezioni o nei servizi restano, comunque, sotto la dipendenza funzionale della magistratura. «gli ufficiali e gli agenti di polizia giudiziaria sono tenuti ad eseguire i compiti a essi affidati dall'autorità giudiziaria»[237].

Alla luce di ciò, possiamo affermare che la polizia giudiziaria assume un duplice significato, condizionato dal rapporto che quest'ultima ha con la magistratura requirente. Da un lato si intende l'insieme dei soggetti che esercitano una specifica funzione[238], dall'altro l'attività stessa. Una funzione che si caratterizza come non preventiva, specialmente quando diretta ad assicurare efficacia al momento repressivo[239].

Per quanto concerne il rapporto che intercorre tra la polizia giudiziaria e i sistemi di IA, occorre segnalare alcune precisazioni.

L'attività svolta dai *software* di polizia predittiva non impone il rispetto di rigorosi criteri di acquisizione della prova, privilegiando l'aspetto di concreta individuazione di soggetti che potenzialmente potrebbero commettere uno o più reati. Questi sistemi dipendono dalla quantità, qualità e tempestività delle informazioni che dovranno essere elaborate.

---

[234] P. Tonini, *Op. cit.*, p.127-128.
[235] Codice di Procedura Penale, articolo 56.
[236] P. Tonini, *Op. cit.*, p.128.
[237] Codice di Procedura Penale, Articolo 56, lett. *c*.
[238] Consistente nell'individuazione delle condotte penalmente rilevanti, nell'identificazione dei responsabili delle stesse e nella raccolta delle prove.
[239] C. Parodi, V. Sellaroli, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Diritto Penale Contemporaneo*, 2019, p.55 ss.

Questa base cognitiva può coincidere con quella di un applicativo funzionale alla raccolta, catalogazione e individuazione di correlazioni tra elementi oggettivi per ricostruire responsabilità penali[240] anche se la differente finalità consente di calibrare implicazioni e termini differenti.

Bisogna valutare se esistono dei rischi correlati alla polizia predittiva nella funzione di polizia giudiziaria. L'interrogativo da prosi è in che termini l'insieme degli elementi raccolti dal database dei *software* di polizia predittiva possono porsi a fondamento di un'annotazione della polizia giudiziaria finalizzata ad una richiesta di misura cautelare, di intercettazione o quale elemento di prova dell'esercizio dell'azione penale. Ed in che modo potranno essere utilizzati tali elementi in sede dibattimentale[241].

Per verificare ciò è innanzitutto indispensabile che tutti gli elementi inseriti nel *database* siano stati acquisiti con riguardo alle indicazioni codicistiche, sia per quanto concerne le forme che per i termini temporali. Quindi, solo gli elementi acquisiti in maniera conforme alla disciplina procedurale potranno essere correttamente utilizzati.

Oltretutto, gli elementi storici posti alla base delle comparazioni e della ricerca di correlazioni, devono poter essere singolarmente ed autonomamente portati all'attenzione del tribunale o del giudice per le indagini preliminari. Se così fosse occorre capire in base a quali principi sia compiuta la comparazione che ha portato ad evidenziare una serie di relazioni che si assumono significative sul piano della ricostruzione della responsabilità; e in base a quali principi l'insieme delle comparazioni e relazioni evidenziate può essere considerato in grado di costituire il fondamento di responsabilità penali.

In aggiunta ai sistemi di polizia predittiva, i recenti sviluppi dell'IA hanno reso possibile l'adattamento di detti strumenti al sistema penale. L'utilizzo dell'IA nel procedimento penale, e più in generale nel sistema penale, deve essere incoraggiato in quanto comporta «numerosi vantaggi quali, ad esempio, la notevole riduzione della tempistica procedimentale per operazioni meramente ripetitive e prive di discrezionalità, l'esclusione di interferenze dovute a negligenza (o peggio a dolo) del funzionario e la conseguente maggior garanzia di imparzialità della decisione automatizzata»[242].

[240] Ossia di polizia giudiziaria.
[241] C. Parodi, V. Sellaroli, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco,* cit, p. 58 ss.
[242] Come riportato dal Consiglio di Stato, sez VI, 4 febbraio 2020, n.881.

Il dibattito tra sistema penale ed intelligenza artificiale si focalizza principalmente su quattro argomentazioni:

- la prima riguarda l'attività di polizia e la già analizzata polizia predittiva;
- la seconda concerne gli algoritmi di giustizia predittiva, i c.d. «*risck assesment tools*», in grado di computare il rischio di recidiva dell'imputato e più in generale la sua pericolosità sociale ed essere quindi strumento d'aiuto per il giudice nella determinazione della pena o nell'applicazione di altri istituti;
- la terza riguarda la prova fondata sull'IA, nella cui analisi rientra l'utilizzo dei captatori informatici e dei c.d. «*facial recognition systems*»*;*
- infine, il tema della responsabilità penale dei c.d. "sistemi intelligenti", il quale si incentra principalmente sulla necessità della modifica delle classiche norme incriminatrici previste dal sistema penale e sull'introduzione di nuove fattispecie.

3.2. Giustizia predittiva

Le tecnologie basate sull'intelligenza artificiale non esauriscono quindi il loro utilizzo al campo investigativo e probatorio ma sono destinati anche ad applicazioni che riguardano direttamente il momento "decisorio".

Il termine giustizia predittiva rischia di condensare in sé fenomeni diversi e di affrontare in modo unitario problematiche tecniche tra loro eterogenee. Una prima categoria di strumenti cha ha attirato l'interesse degli avvocati è quella dei sistemi di *judge profiling*, ossia di previsione della decisione del giudice. In ambito civile sono stati sviluppati strumenti in grado di valutare le possibilità di successo di una controversia. In ambito penale, invece, si è discusso molto dei *risk assassment tools* e delle problematiche rispetto al diritto di difesa[243].

Tra le decisioni che queste tipologie di algoritmi sono in grado di assumere vi sono, ovviamente, anche decisioni volte a comporre, ovvero prevenire, liti ed a risolvere controversie.

Grazie alla possibilità di usufruire di un ampio spettro di dati, provenienti da fonti autorevoli[244], sono in circolazione algoritmi molto sofisticati in grado di impiegare una metodologia che i soggetti coinvolti percepiscono come oggettiva e priva di pregiudizi[245].

Le caratteristiche principali di questi metodi alternativi di risoluzione delle controversie è l'apportare una significativa riduzione dei tempi ed una notevole riduzione dei costi, rispetto ai sistemi tradizionali, poiché sono gestiti esclusivamente *online*.

In concreto, la giustizia predittiva è un sistema che consente di prevedere il possibile esito di una controversia sulla base di soluzioni statuite per casi analoghi o simili. Benché mascherata e innovata dall'utilizzo della tecnologia, la giustizia predittiva può suscitare il timore di un ritorno ad una visione meccanicistica del ruolo del giudice. Timori che sono stati rappresentati ed esplicati dal Report della XIII Assemblea Nazionale degli Osservatori sulla giustizia civile, nel quale si legge che: «si è considerato che la "giustizia predittiva" incarna il mito illuminista del giudice bocca della legge, svelato ormai da gran tempo come tale nella manualistica della filosofia giuridica. E si sono evidenziate le anomalie di una giustizia siffatta: all'imparzialità del giudice, per darne attuazione in una

[243] E. Barbujani, *La giustizia predittiva e l'incalcolabile*, in *Cassa forense*, 2020.
[244] Quali banche dati giurisprudenziali, banche dati legislative, raccolte di precedenti.
[245] J. Kaplan, *Intelligenza artificiale, Guida al futuro prossimo*, Luiss *University Press*, 2018, p.137 ss.

declinazione mitologica, impossibile e distorta, si sostituisce l'incorporeità e la a-storicità di una macchina che *ius dicit* al di fuori della storia, cioè lo spazio abitato dagli umani e cioè dai loro corpi. Ci troviamo forse di fronte al recupero in chiave tecnocratica di una teocratica "Giustizia Eterna"? O forse solo a un alibi de-responsabilizzante? Comunque, un giudizio che è specchio della profonda alienazione di un Uomo che delega il giudizio su un altro uomo a qualcosa di non umano. Rimane, per ora, la clausola di garanzia finale recata dalla norma sopra indicata, ma limitata: è garantito l'intervento umano, non chiare le sue modalità e la certa sua decisività. Ma rimane anche il problema ampiamente evidenziato, del rapporto tra la decisione del giudice e quella della macchina, tutto da verificare e scoprire, anche a livello di legittimazione diffusa nelle decisioni.

Sono dunque ammissibili apporti dell'elaborazione informatica di dati, ma in campi limitati e circoscritti, connotati da ampia discrezionalità giudiziale ma anche da immediata misurabilità, dunque nei quali è essenziale, proprio ai fini di prevedibilità delle decisioni, ottenere sintesi di innumerevoli e disparate decisioni, ma dove l'interferenza con l'attuazione di regole e di valori è evitata perché la stessa valutazione quantitativa è già stata operata dal giudice a monte: così, ad esempio, per la verifica della qualificazione delle somme spettanti a vario titolo nelle procedure di separazione coniugale e scioglimento del vincolo matrimoniale; per la qualificazione del danno biologico, ecc.»[246].

Il tratto che accomuna la decisione umana e quella, per così dire, "robotica"[247] è da ricercare nello sforzo incessante della disciplina processualistica verso una maggiore oggettivizzazione della giustizia, che attiene alla necessità di garantire, in uno Stato di diritto, una decisione che sia il più possibile equa, imparziale, razionale e auspicabilmente incontestabile. In questo senso, il concetto di giustizia predittiva, intesa strettamente come la possibilità di «prevedere la probabile sentenza, relativa ad uno specifico caso,

[246] S. Alecci, E. Bertacchini, M. Bove, G. Buffone, T. Caradonio, C.M. Cea, P. Cendon, G. Cesari, C. Chiaravalloti, B. Ciaccia, L. Circelli, V. Corasaniti, M. Delia, L. Delli Priscoli, P. Di Marzio, F. Elefante, A. Fasano, C. Ferri, F. Fimmanò, E. Forgillo, M. Giorgetti, G. Ianni, F. Lupia, G. Marseglia, R. Martino, F. Proietti, S. Ruscica, P. Sandulli, S. Schirò, B. Spagna Musso, P. Spaziani, A. Stilo, A. Uricchio, A. Vlitutti, A. Zaccaria, *Prevedibilità, predittività e umanità del giudicare (XIII Assemblea Nazionale degli Osservatori sulla Giustizia Civile),* in *Rivista scientifica di Diritto Processuale Civile,* 2018, p. 7-8.

[247] La dottrina giuridica si sta negli ultimi anni seriamente domandando se, in un futuro più o meno lontano, possa aversi nella realtà giudiziaria una decisione prodotta dalla sola applicazione di un sistema algoritmico. Sul punto discute A. Carratta, *Decisione robotica e valori del processo,* in *Rivista di diritto processuale*, 2020, p.491 ss.

attraverso l'ausilio di algoritmi»[248], è correlato in maniera evidente all'esigenza di prevedibilità cui è orientato il sistema penale nel suo complesso.

Dapprima, la prevedibilità va letta come la necessità di poter prevedere, sul piano giuridico, le conseguenze delle proprie azioni e quindi come una diretta applicabilità del principio di legalità espresso dal comma 2 dell'articolo 25 della Costituzione[249], assioma che governa il diritto penale e garantisce la piena autodeterminazione in ordine ai comportamenti sociali[250].

Per altro verso, la prevedibilità consiste nella possibilità di avere effettiva contezza dell'esito di un processo. Essendo la finalità quella di poter prevedere i risultati delle proprie azioni, conseguenza è che tale scopo non può dirsi realizzato se non eliminando le tracce di arbitrarietà che possono contaminare una vicenda giudiziaria. Per essere pienamente attuato tale principio, il soggetto deve essere in grado di conoscere cosa aspettarsi dall'apparato giudiziario, per capire a quali conseguenze andrà incontro. In questo senso la prevedibilità della norma penale diventa prevedibilità della decisione giudiziale[251].

Inoltre, la possibilità di una diffusione di decisioni giudiziarie algoritmiche anche in materia penale, ha richiamato l'attenzione del Consiglio d'Europa, il quale, tramite la propria commissione per l'efficacia della giustizia (CEPEJ), ha adottato la «Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e nei relativi ambienti»[252]. Come già evidenziato nel capitolo precedente, si tratta di un documento di eccezionale rilevanza il quale individua alcune fondamentali linee guida alle quali dovranno attenersi i soggetti pubblici e privati responsabili del progetto e sviluppo degli strumenti e dei sevizi di IA[253]. Il documento dispone che: «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,

[248] L. Viola, Giustizia Predittiva, in *Enciclopedia Giuridica Treccani – Diritto online.*

[249] «nessuno può essere punito se non in forza di una legge che sia entrata in vigore prima del fatto commesso».

[250] G. Padua, *Intelligenza artificiale e giudizio penale: scenari limiti e prospettive,* in *Giappichelli*, 2018.

[251] F. Viganò, *Il principio di prevedibilità della decisione giudiziale in materia penale,* in Diritto *Penale Contemporaneo,* 2016, p.3.

[252] La presente Carta è stata adottata il 4 dicembre 2018.

[253] S. Quattroloco, *Intelligenza artificiale e giustizia: nella cornice della carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche,* in *La legislazione penale*, 2018.

avvocati e privati»[254], evidenziando poi che l'utilizzo di tali algoritmi è meritevole di essere preso in considerazione «nel campo della giustizia civile, commerciale e amministrativa al fine di una risoluzione precontenziosa *online* delle controversie, purché un ricorso successivo al giudice rimanga possibile»[255]. Per quanto riguarda i procedimenti penali, invece, la Carta dispone che «anche se non sono specificatemene progettati per essere discriminatori, l'uso di algoritmi basati sull'IA ha mostrato il rischio di favorire la rinascita di teorie deterministiche a scapito delle teorie dell'individualizzazione della pena»[256].

Sicché, l'utilizzo di algoritmi di giustizia predittiva nell'abito penale risulta essere maggiormente problematico. Innanzitutto, essendo la testimonianza il mezzo di prova più utilizzato ai fini dell'accertamento dei fatti, vi è un evidente impossibilità per un algoritmo di giudicare tale mezzo di prova in modo soddisfacente e completa, non essendo in grado di giudicare emozioni e circostanze riguardanti l'imputato. In secondo luogo, all'interno del processo penale i criteri di valutazione della prova sono plurimi e non predeterminati, motivo per il quale risulta difficile per un algoritmo stabilire se determinati indizi possono essere considerati «gravi, precisi e concordanti» ai sensi dell'articolo 192, comma 2, c.p.p.[257] Infine, il procedimento penale è improntato sulla regola di giudizio basata sull' «oltre ogni ragionevole dubbio»[258], principio che non può essere seguito da un *software,* per definizione incapace di esprimere valutazioni, riservate esclusivamente all'esperienza umana[259].

---

[254] «*The use of artificial intelligence in European judicial systems remains primarily a private-sector commercial initiative aimed at insurance companies, legal departments, lawyers and individuals*», da *European ethical Charter on the use of Artificial Intelligence in judicial system and their environment,* 2018, p.16.

[255] «*Their application in the field of civil, commercial and administrative justice is to be considered for the creation of scales or the pre-litigation resolution of disputes online, when a later appeal to the judge remains possible*», da *European ethical Charter on the use of Artificial Intelligence in judicial system and their environment,* 2018, p.41.

[256] «*Even they are not specifically designed to be discriminatory, the use of statistics and AI in criminal proceedings has shown a risk of prompting the resurgence of deterministic doctrines to the detriment of individualization of the sanction, which have been widely acquired since 1945 in most European judicial systems*» da *European ethical Charter on the use of Artificial Intelligence in judicial system and their environment,* 2018, p.48.

[257] F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine,* cit, p. 15-16.

[258] Articolo 533, comma 1, c.p.p.

[259] *Ibidem.*

3.2.1. *Risk assessment tools*

I *Risk assessment tools* sono strumenti di valutazione del rischio, capaci di effettuare valutazioni attuariali, rielaborando quantità enormi di dati al fine di far emergere relazioni, coincidenze, correlazione, che consentono di profilare una persona e prevederne i successivi comportamenti, anche di rilevanza penale[260]. In particolare, questi strumenti permettono di valutare la probabilità che un individuo posso commettere un reato in futuro sulla base di dati comportamentali e fattori di rischio individuati.

Nel sistema penale, uno dei compiti principali del giudice è quello di valutare il comportamento futuro di un individuo e la sua pericolosità sociale, valutazione prognostica basata su un ragionamento di tipo intuitivo-esperienziale, che tiene conto di una serie di elementi aggregati. La valutazione del rischio individuale di recidiva, quindi, consiste nel calcolo della probabilità di verificazione di un evento futuro ed incerto[261].

I *risk assasment tools* hanno lo scopo di automatizzare l'attività di valutazione sul futuro comportamento dell'imputato, attività attualmente già compiuta dal giudice al fine della valutazione della pena o per l'applicazione di altri istituti ai sensi delle numerose norme del codice penale, del codice di rito e di leggi speciali. Per ricordare alcune fattispecie il codice penale, all'articolo 133, fornisce un elenco di criteri oggettivi e soggettivi che il giudice deve tenere in considerazione per scegliere la pena da applicare in maniera discrezionale. Oltre alla gravità del reato, il giudice deve tenere conto «della capacità a delinquere del colpevole, desunta: 1) dai motivi a delinquere e dal carattere del reo; 2) dai precedenti penali e giudiziari, e, in genere, dalla condotta e dalla vita del reo, antecedente al reato; 3) dalla condotta contemporaneo o susseguente al reato; 4) dalle condizioni di vita individuale, familiare e sociale del reo».

L'articolo 163 del codice penale, invece, disciplina l'istituto della sospensione condizionale della pena, concessa all'imputato in seguito ad una valutazione discrezionale operata dal giudice, all'interno della quale non deve tenere in considerazione solo la gravità del reato ma anche il comportamento del reo[262].

---

[260] L. Castelletti, G. Rivellini, E. Straticò, *Efficacia degli strumenti di Violence Risk Assessment e possibili ambiti applicativi nella psichiatria forense e generale italiana,* in *Journal of Psychopathology,* 2014, p.153 ss.

[261] F. Basile, *Esiste una nozione ontologicamente unitaria di pericolosità sociale? Spunti di riflessione, con particolare riguardo alle misure di sicurezza e alle misure di prevenzione,* in *Rivista italiana diritto processuale penale,* 2018, p.644 ss.

[262] Articolo 163, Codice penale.

Inoltre, l'articolo 203 del codice penale, riguardante l'applicabilità delle misure di sicurezza, richiede che il fatto sia previsto dalla legge come reato e aggiunge che l'imputato debba essere una «persona socialmente pericolosa»[263], definita come una persona incline a commettere nuovi reati. Nel Codice di rito, una valutazione prognostica simile è richiesta per determinare la sussistenza di uno dei tre *pericula libertatis* richiesti per disporre una misura cautelare. In particolare, l'articolo 274 del Codice di procedura penale, alla lettera *c*, prevede che le misure cautelari si possono applicare quando vi sia un pericolo di reiterazione del reato, desumibile, oltre che dalle modalità e dalle circostanze del fatto, anche dalla «personalità della persona sottoposta alle indagini o dell'imputato, desunta da comportamenti o atti concreti o dai suoi precedenti penali»[264].
Questi sono solo alcuni esempi di ipotesi previste nel sistema penale in cui al giudice è richiesto di compiere una valutazione prognostica che potrebbe essere sostituita da algoritmi predittivi, quali non andrebbero a rivoluzionare processi cognitivi volti a determinare l'applicabilità di uno specifico istituto, ma ad automatizzarli[265].
L'approccio alla valutazione della pericolosità sociale si integra facilmente nello scenario della giustizia predittiva, offrendo un'ulteriore prospettiva applicativa dell'intelligenza artificiale. In questa prospettiva, il sistema giudiziario può avvalersi di un giudizio basato su parametri oggettivi e concretamente apprezzabili[266], basato su evidenze statistiche e fattori individuali, noti come fattori di rischio[267]. Si tratta del modello di qualificazione del rischio, noto come *risk assessment*, che dalla combinazione di elementi e parametri intende arrivare alla misura della probabilità che un evento si verifichi.
I *risk assessment tools* sono *software* predittivi il cui fine è quello di computare il rischio che un imputato commetta nuovamente un fatto di reato. Questa previsione viene posta in essere attraverso l'analisi dei dati comportamentali del reo e la successiva comparazione con quelli relativi ad altri individui precedentemente arrestati o condannati.

[263] Definizione attribuibile ad un soggetto quanto è probabile che commetta nuovi fatti preveduti dalla legge come reati.
[264] Articolo 274, lettera c, Codice di procedura penale.
[265]A. Giraldi, L. Grossi, A. Massaro, L. Notaro, P. Sorbello, *Intelligenza artificiale e giustizia penale*, in *Dipartimento di giurisprudenza Università Roma Tre*, 2020, p.93 ss.
[266] C.d. "*evidence based*".
[267] G. Zara, *Tra il probabile e il certo. La valutazione del rischio di violenza e di recidiva criminale*, in Diritto *Penale Contemporaneo*, 2016, p.12 ss.

L'algoritmo, dunque, elabora una valutazione della probabilità di recidiva e della sua pericolosità sociale[268].

Tali sistemi vengono costruiti a partire da una combinazione di elementi e parametri che permettono di misurare la probabilità che un evento si verifichi. La valutazione del rischio prevede, innanzitutto, un momento in cui vengono individuati i fattori di rischio che possono essere direttamente coinvolti nel comportamento criminoso, come l'età, il sesso, l'origine etnica, il livello di scolarizzazione, la situazione familiare e lavorativa, la posizione sociale, i precedenti penali, le precedenti esperienze carcerarie, la presenza di un certo tasso di criminalità nella cerchia familiare o nella rete di conoscenze, l'uso di sostanze stupefacenti o alcoliche ed il grado di controllo degli impulsi[269].

Successivamente, ciascuno di questi fattori viene convenzionalmente etichettato e viene attribuito un punteggio che indica il grado di significatività della loro correlazione con il rischio di recidiva, sulla base delle statistiche disponibili fino a quel momento. In questo modo, si può calcolare in termini probabilistici il rischio individuale di recidiva, in base ai fattori di rischio presenti nel caso specifico.

Gli strumenti di valutazione del rischio possono quindi fornire una valutazione oggettiva e concretamente apprezzabile del rischio che un individuo possa commettere in futuro un reato. Tuttavia, è importante sottolineare che l'utilizzo di questi strumenti non deve essere considerato come un'alternativa al giudizio del giudice, ma piuttosto come strumento di supporto della sua decisione. Inoltre, è fondamentale garantire che l'utilizzo di questi strumenti sia sempre guidato da principi etici e che sia rispettoso dei diritti fondamentali delle persone coinvolte.

3.2.2. Algoritmi di giustizia predittiva negli Stati Uniti

Negli stati Uniti già da una decina d'anni sono in fase di diffusione algoritmi predittivi della pericolosità criminale.

L'algoritmo di giustizia predittiva più noto è sicuramente il *software* americano COMPAS (*Correctional Offender Management Profiling for Alternative Sanction*)[270].

---

[268] P. Severino, *Intelligenza artificiale e diritto penale,* in *Intelligenza artificiale: il diritto, i diritti e l'etica,* a cura di U. Ruffolo, *Giuffrè Francis Lefebvre,* Milano, 2020, p. 542.

[269] G. Padua, *Intelligenza artificiale e giudizio penale: scenari limiti e prospettive,* cit.

[270] Software già citato nel capitolo 1, prodotto nel 1998 dalla società Northpointe (da gennaio 2017 rinominata Equivant).

Il sistema identifica il rischio di recidiva dell'imputato sotto tre distinti aspetti: *pretrial risk*, *general recidivism*, *violent recidi*vism. Inoltre, accanto a questa funzione più strettamente predittiva, l'algoritmo elabora anche una *need scale* per definire il profilo dell'autore e le esigenze di riabilitazione del medesimo[271].

I dati di imput sono formati da informazioni rese dall'imputato, attraverso un questionario, e da informazioni raccolte dal suo fascicolo. Il questionario utilizzato da COMPAS consta di 137 domande, riguardanti informazioni sulla vita e sul casellario giudiziario dell'imputato.

Questi dati vengono confrontati con quelli di profili simili già presenti del *dataset* dell'algoritmo, il quale elabora un *output*. Quest'ultimo consta, innanzitutto di un numero decimale al quale corrisponde il grado di rischio di reiterazione del reato, ed in secondo luogo elabora il *need scale*[272], una scala che va da 1 a 10, che indica il livello di pericolosità dell'imputato rispetto ad altri criminali della stessa categoria[273].

Il procedimento attraverso cui si giunge a questa valutazione è però ignoto, la società ha omesso di svelare il contenuto del procedimento, sicuramente per ragioni di proprietà intellettuale[274]. Le perplessità che riguardano questa mancanza di trasparenza vengono esplicate in modo chiaro nel caso *State v. Loomis,* da cui conviene prendere le mosse per evidenziare le criticità che si nascondono dietro l'uso indiscriminato di questi algoritmi.

Eric Loomis è un cittadino americano che nel 2013 viene fermato dalla polizia alla guida di un'autovettura coinvolta in una sparatoria. Per determinare la pena da attribuirgli, la Corte chiede il *Presentece Investigation Report*, un rapporto preparato su richiesta del tribunale, da un funzionario incaricato della libertà vigilata, volto a scoprire la storia, criminale, familiare e sociale di una persona condannata per un determinato crimine. In

---

[271] Tratto da *Practitioner's Guide to COMPAS Core, in* www.equivant.com, 2019, «*the need scales are not meant to be predictive but aim simply and accurately to describe the offender along dimensions relevant for correctional practice. Research findings indicate that individuals involved in the criminal justice system often have problems and deficits in the domains of education, housing, employment, substance abuse, relationships, and cognition. The need scales should be valid and reliable measures of constructs in these domains and other aspects of the person-in-environment that represent potential targets for interventions. The need scales guide individualized decisions for case planning, including identifying targets and choosing inventions*».

[272] A. Giraldi, L. Grossi, A. Massaro, L. Notaro, P. Sorbello, *Intelligenza artificiale e giustizia penale*, cit, p.173 ss.

[273] Dove un punteggio da 1 a 4 indica un basso rischio di recidiva; da 4 a 7 un rischio medio e da 8 a 9 un rischio elevato. Da *Practitioner's Guide to COMPAS Core,* cit.

[274] G. Contissa, G. Lasagni, G. Sartor, *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Pacini Giuridica*, 2019, p.619 ss.

questo rapporto vengono inclusi anche i risultati ottenuti attraverso COMPAS, risultati che in questo caso hanno mostrato un rischio di recidiva molto alto[275].

Dagli esiti del rapporto, la Corte ha emesso una sentenza di condanna per i reati contestati particolarmente severa.

Successivamente, Loomis ha impugnato la decisione innanzi alla Corte Suprema del Wisconsin[276]. Sede nella quale l'imputato ha lamentato la violazione del suo diritto costituzionale ad un giusto processo[277]. In questa circostanza COMPAS è stato contesto per la sua predisposizione a seguire pregiudizi basati sul genere e sulla razza, nonché per il difetto di trasparenza relativo al suo meccanismo di funzionamento[278].

La Corte Suprema del Wisconsin ha formulato, quindi, un *warning* in relazione all'uso di COMPAS, nel quale ha evidenziato: in primo luogo, data la segretezza dei procedimenti che caratterizzano l'algoritmo, derivanti dal segreto industriale, la corte ha affermato l'invalidità della divulgazione e della comprensione delle informazioni che riguardano il suo metodo di funzionamento; in secondo luogo, le valutazioni effettuate dall'algoritmo sono valutazioni di gruppo e non su base individuale; in terzo luogo, l'elevato pericolo di una sovrastima del rischio di commissione di reati a carico di alcune minoranze etniche.

Nonostante ciò, la Corte ha respinto il ricorso di Loomis, poiché le valutazioni di COMPAS non erano da considerarsi decisive, in quanto sottoposte al controllo ed alla validazione di un giudice "umano"[279].

Un altro *risk assessment tool* diffuso degli Stati Uniti è il *Public Safety Assessment (PSA)*. Introdotto da un'organizzazione *non profit*[280], nell'intento di riformare il sistema del "*parole"*[281], fornendo ai giudici che devono formulare una prognosi criminale indicazioni scientifiche ed imparziali.

---

[275] A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro della libertà,* in *Rivista di BioDiritto*, 2019, p.78-79.

[276] S. Quattrocolo, *Quesiti nuovi e soluzioni antiche?*, cit, p.1751 ss.

[277] I motivi di doglianza della sentenza sono tre: violazione del proprio diritto ad essere condannato sulla base di informazioni accurate, violazione del proprio diritto a una pena individuale, lo strumento, nella definizione del rischio di recidiva, aveva utilizzato in maniera controversa il dato di genere.

[278] S. Carrer, *Se l'amicus curiae è un algoritmo: il chicchierato caso Loomis alla Corte Suprema del Wisconsin*, in *Giurisprudenza Penale Web*, 2019.

[279] *Ibidem.*

[280] L'organizzazione "Laura and John Arnold Foundation".

[281] Il "*parole system*" è un sistema giudiziario americano che prevede la condanna dei criminali ad una pena minima obbligatoria, solitamente per reati violenti o legati alla droga. Questo sistema è stato introdotto in diversi stati degli Stati Uniti a partire dagli anni '70 e '80 come risposta alla crescente criminalità, con l'obbiettivo di garantire la certezza della pena e scoraggiare la recidiva. Tuttavia, il sistema ha ricevuto

Il PSA è volto ad attuare una correlazione tra i fattori di rischio del soggetto, che deve essere valutato attraverso un *database* di 1,5 milioni di casi, ed in base alle informazioni a disposizione attribuisce a questo un punteggio[282]. In questo caso tra i fattori di misurazione che vengono presi in esame, non vi è la razza, l'origine etnica e geografica[283]. Tale sistema è stato adottato nello Stato del New Jersey, ed ha contribuito ad aumentare il numero delle persone rilasciate su *parole* e senza il pagamento di cauzione. I dati hanno infatti mostrato come questo algoritmo abbia favorito le persone non abbienti e non pericolose.

3.2.3. Algoritmi di giustizia predittiva in Europa

Il nostro ordinamento giuridico consente l'utilizzo di *software* di giustizia predittiva quali strumenti ausiliari per il giudice, ma solo se questi non costituiscono l'unico elemento su cui si fonda la decisione.

Infatti, l'articolo 8 del D.lgs. 51/2018 vieta le decisioni «basate esclusivamente su un trattamento automatizzato», incluse quelle che utilizzano la profilazione.

Inoltre, l'articolo 220 del codice di procedura penale prevede un divieto di perizia psicologica e criminologica, disponendo che non sono ammesse indagini penali volte a «stabilire l'abitualità o la professionalità del reato, la tendenza a delinquere, il carattere e la personalità dell'imputato e in genere le qualità psichiche indipendenti da cause patologiche», sancendo così un limite invalicabile per l'uso di strumenti di giustizia predittiva.

Dunque, si evince il possibile utilizzo di algoritmi di giustizia predittiva come uno dei tanti elementi che possono poi essere valutati in sede di condanna[284]. Utilizzo che non è esente da critiche, infatti tali strumenti possono essere basati su dati di formazione discriminatoria, che portano ad una polarizzazione delle decisioni giudiziarie, creando disuguaglianze nella giustizia. Inoltre, l'uso di tali strumenti potrebbe portare ad una riduzione del ruolo del giudice e della sua discrezionalità nella decisione finale, ponendo

molte critiche per i suoi effetti sul sovraffollamento carcerario, la disuguaglianza razziale nella sua applicazione e la mancanza di flessibilità nella valutazione dei casi individuali.

[282] G. Zara, *Tra il probabile e il certo. La valutazione del rischio di violenza e di recidiva criminale,* cit, p.14 ss.

[283] Persistono invece fattori quali l'età, i precedenti penali, le passate apparizioni in tribunale e le denunce ricevute in casi precedenti.

[284] M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra stati uniti ed europa,* cit, p.74 ss.

dubbi sulla corretta applicazione dei principi costituzionali che reggono il procedimento penale[285].

A tal riguardo, possiamo riportare le parola di Andrea Natale, il quale riflettendo sull'utilizzo di algoritmi predittivi in sede giudiziaria, svolge le seguenti, condivisibili, considerazioni: «il risultato fornito dagli algoritmi predittivi è necessariamente influenzato dalla qualità dei dati che vengono posti come *input*; ne discende che è indispensabile prevedere meccanismi che assicurino: (a1) la qualità del dato; (a.2) l'indipendenza della fonte da cui provengono i dati; (a.3) l'indipendenza dell'autorità che raccoglie i dati; (a.4) l'accessibilità a tutti dei dati posti come *imput* dell'algoritmo;

(b) è necessario scongiurare il rischio che l'algoritmo possa avere esito discriminatorio fondato su dati personali sensibili, tra cui la razza e l'estrazione sociale.

(c) la verificabilità o meno della struttura dell'algoritmo; nel concepire l'architettura di un algoritmo, il programmatore fa delle scelte che, necessariamente, influenzano il risultato dell'operazione computazionale; il programmatore può fare degli errori di progettazione; un algoritmo la cui struttura sia protetta da diritti di proprietà intellettuale e non *open source* è sottratto dalla possibilità di controllo, verifica e confutazione da parte della parte processuale e , più in generale, dalla comunità degli utenti; ciò comporta non pochi problemi, tanto sotto il profilo della validazione dell'affidabilità scientifica del risultato che l'algoritmo restituisce, quanto sotto il profilo del diritto di difesa; si ritiene, pertanto, indispensabile che – laddove si voglia davvero fare un uso processuale di algoritmi predittivi da parte del sistema giudiziario (che è un sistema per natura pubblico) – nessun segreto possa essere posto sull'architettura degli algoritmi e dei dati che lo alimentano; si deve poi elaborare un meccanismo che assicuri l'indipendenza di chi ha elaborato l'algoritmo (che senso ha costituzionalizzare l'indipendenza del giudice e la sua soggezione solo alla legge se non si coltiva l'analoga pretesa di chi elabora uno strumento decisorio di simile portata?);

(d) l'algoritmo – anche ove usato non come strumento decisorio esclusivo, ma come mero supporto alla decisione del giudice – richiede formazione; è dunque indispensabile formare il personale giudiziario che potrebbe doversene avvalere;

(e) l'algoritmo predittivo – muovendo da una elaborazione della giurisprudenza e dei casi precedenti- può indicare non il "risultato" esatto di una certa controversia, ma il suo

[285] *Ibidem*

possibile esito, evidenziando quali siano le linee giurisprudenziali prevalenti e quali gli esiti concreti che si sono dati in casi simili; ciò, però, comporta più di un rischio; (e.1) l'algoritmo non è in grado di "riconoscere" che quello a lui sottoposto non è un caso simile; vi sono delle singolarità che un decisore umano, forse rileverebbe e che porterebbero ad operare un *distinguishing*; l'algoritmo on è progettato per prevedere questa evoluzione; (e.2) per la stessa ragione, l'algoritmo può favorire quello che Garapon chiama come effetto *moutonnier* (effetto pecora nel gregge): non è corretto, in altri termini, il rischio di indurre il giudice pigro ad agitarsi sulla proposta dell'algoritmo senza assumere su di sé l'autentica responsabilità del giudizio che egli emette; (e.3) per la stessa ragione, l'uso di algoritmi può favorire una cristallizzazione della giurisprudenza, rendendola meno sensibile ai cambiamenti sociali (e, di fatto, rendendoli meno probabili)»[286]

Anche il Parlamento Europeo, dispone che: «la diffusione dell'IA nel settore delle attività di contrasto e nel settore giudiziario non dovrebbe essere considerata una mera questione di realizzabilità tecnica ma piuttosto una decisione politica riguardante la progettazione e gli obbiettivi dei sistemi di attività di contrasto e di giustizia penale; che il moderno diritto penale si basa sull'idea che le autorità reagiscono a un reato dopo che è stato commesso, senza supporre che le persone siano pericolose e debbano essere sorvegliate costantemente per prevenire possibili illeciti; che le tecniche di sorveglianza basate sull'IA mettono in dubbio profondamente tale approccio e impongono ai legislatori in tutto il mondo di valutare con attenzione le conseguenze derivanti dalla diffusione delle tecnologie che riducono il ruolo dell'essere umano nelle attività di contrasto e di giudizio»[287].

In questo contesto, l'ingresso di tali strumenti nel procedimento penale deve essere disciplinato da una normativa specifica, che tuteli gli interessi collettivi dei singoli, nel rispetto dei principi costituzionali che regolano il procedimento penale. In altre parole, l'uso dell'IA nella giustizia penale dovrebbe essere regolamentato in modo tale da garantire che le decisioni giudiziarie siano sempre basate su un'analisi completa ed equilibrata dei dati, evitando qualsiasi discriminazione o pregiudizio basato su fattori automatici o algoritmici. Ciò richiede un approccio olistico, che prenda in considerazione

[286] A. Natale, *Una giustizia (im)prevedibile?*, in *questione di giustizia*, fascicolo 4/2018, p.3.
[287] Risoluzione del Parlamento Europeo sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità giudiziarie in ambito penale (2021/2016) (INI), 6 ottobre 2016, Considerando Q.

non solo l'efficacia tecnica dei sistemi di IA, ma anche i loro effetti sulle libertà individuali, la giustizia e l'uguaglianza. Solo in questo modo, infatti, si può garantire che l'intelligenza artificiale sia un alleato della giustizia e non un fattore di rischio per i diritti fondamentali degli individui[288].

In Europa, l'accesso degli algoritmi di giustizia predittiva all'interno del sistema penale è stato precluso dall'art 15 della direttiva 95/46/CE, confluito nell'art 22 del nuovo regolamento europeo in materia di protezione dei dati personali, entrato in vigore il 25 maggio 2018. Questo articolo stabilisce il diritto delle persone di non essere sottoposte a decisioni basate esclusivamente su un «trattamento automatizzato di dati destinati a valutare la sua personalità»[289]. Articolo che mira a proteggere i diritti individuali e la privacy dei cittadini europei. Inoltre, la risoluzione del parlamento europeo sulla robotica del 2017 ha sottolineato l'importanza del principio di trasparenza nella decisione presa con l'aiuto dell'IA, affermando la necessità che risulti sempre possibile indicare la logica alla base di ogni decisione presa con l'ausilio dell'intelligenza artificiale, qualora tale decisione possa avere un impatto rilevante sulla vita di più persone.

L'uso di tecnologie di IA nel sistema di giustizia penale è una questione delicata che richiede un approccio equilibrato. Soprattutto perché l'adozione di tali tecnologie potrebbe aiutare a migliorare l'efficienza e l'efficacia del sistema giudiziario, ad esempio, prevedendo crimini e riducendo gli errori giudiziari. Pertanto, è importante trovare un equilibrio tra l'uso delle tecnologie di IA e la protezione dei diritti individuali, soprattutto perché il sistema giudiziario deve essere guidato dal principio della presunzione di innocenza e dalla necessità di rispettare i diritti delle persone coinvolte nel processo penale.

[288] P. Severino, *Op. cit,* p. 545.

[289] Articolo 22, Regolamento generale sulla protezione dei dati, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, aggiornato alle rettifiche pubblicate sulla Gazzetta Ufficiale dell'unione europea 127 del 23 maggio 2018, in https://www.garanteprivacy.it/documents/10160/0/Regolamento+UE+2016+679.+Arricchito+con+riferimenti+ai+Considerando+Aggiornato+alle+rettifiche+pubblicate+sulla+Gazzetta+Ufficiale++dell%27Unione+europea+127+del+23+maggio+2018.

3.3. Valutazione della prova e responsabilità

A differenza degli algoritmi di giustizia predittiva, l'uso di prove digitali e c.d. *machine evidence* all'interno dei procedimenti penali sta diventando sempre più comune grazie alla diffusione dell'*Internet of things.* Pensiamo, ad esempio, alle scatole nere che vengono inserite nelle automobili e che possono essere utilizzate per dimostrare l'alibi di un imputato; pensiamo anche alla domotica che è in grado di fornire informazioni sulla configurazione di un ambiente e sui soggetti presenti[290].

Per dare una collocazione e questo tipo di prova, possiamo partire dalla considerazione che la prova scientifica è un insieme di prove in cui «l'inferenza probatoria che è alla base dell'accertamento del fatto non può essere articolata sulla base di conoscenze ordinarie o del sapere diffuso» [291]. All'interno della prova scientifica, c'è un sottoinsieme che comprende la prova digitale, e all'interno di questa, c'è la prova strettamente fondata sull'IA.

È importante notare che le prove digitali non vengono acquisite necessariamente come prove atipiche[292], ma come declinazioni di prove tipiche, poiché sono un sottoinsieme della prova scientifica.

Attualmente non esiste una normativa specifica che regoli l'uso dell'IA nella prova processuale all'interno del sistema giudiziario italiano. Tuttavia, l'articolo 111 della Costituzione sancisce il principio di uguaglianza delle parti e il diritto di difesa nel processo, diritti che potrebbero essere compromessi se l'uso di tecnologie avanzate fosse permesso senza una regolamentazione adeguata. Inoltre, l'articolo 190 del c.p.p. stabilisce che «la prova deve essere acquisita con le forme e nei vari modi previsti dalla legge», il che potrebbe richiedere una normativa specifica per l'uso dell'IA come mezzo di prova. Al momento, quindi, l'uso dell'IA nella prova processuale dipende dall'interpretazione dei principi costituzionali e del codice di procedura penale da parte dei giudici.

D'altronde, non è possibile acquisire la prova basata sull'IA nel procedimento penale tramite l'articolo 189 c.p.p., poiché la mancanza di conoscenza del codice sorgente e

[290] A. Zilordi, *Intelligenza artificiale e processo penale tra norme, prassi e prospettive,* in *Questione di Giustizia*, 2019.
[291] Cassazione Penale, Sez. 4, 13 dicembre 2010, n.43786, Sentenza Cozzini.
[292] Ai sensi dell'articolo 189 c.p.p.

quindi la mancanza di trasparenza dell'algoritmo non consentono di assicurare l'accertamento dei fatti, che è un requisito espresso della norma[293]. Inoltre, la segretezza del codice sorgente renderebbe la prova fondata sull'IA incompatibile con il principio del contraddittorio nella formazione della prova previsto dall'articolo 111 della Costituzione, che prevede la possibilità di verificare l'affidabilità della prova stessa, rendendola inutilizzabile nella fase decisoria.

Per garantire il rispetto dei principi fondamentali dell'ordinamento giuridico italiano, sarebbe opportuno regolamentare l'uso generale della prova basata sull'IA, prevedendo dei criteri valutativi per l'effettiva attendibilità della stessa da applicare nei casi specifici. In questo modo, sarebbe possibile utilizzare al meglio le tecnologie emergenti assicurando al contempo la protezione dei diritti fondamentali dei cittadini.

Per quanto concerne la valutazione delle prove, bisogna sottolineare l'importanza del giudizio umano, che rappresenta e deve rappresentare il valore aggiunto rispetto ad un giudizio espresso da una macchina. Il giudizio umano può essere influenzato da emozioni e sentimenti, ma la formazione e l'etica del magistrato dovrebbero prevenire tali forme di fallibilità. Tuttavia, se vogliamo un giudizio che consideri la complessità dell'agire umano e le molte variabili che lo condizionano, solo un giudizio espresso da una mente umana può soddisfare questa esigenza. Una macchina non potrebbe adeguarsi a questo tipo di complessità e di conseguenza la sua valutazione sarebbe meno accurata rispetto a quella del giudice "umano"[294].

Questa conclusione si evince anche dalle norme fondamentali del codice di procedura penale. Innanzitutto, l'articolo 533 c.p.p. precisa che «il giudice pronuncia sentenza di condanna se l'imputato risulta colpevole del reato contestatogli al di là di ogni ragionevole dubbio». Sebbene un'applicazione di intelligenza artificiale possa quantificare le percentuali di criticità o dubbi sulla responsabilità dell'imputato, la connotazione di ragionevolezza è difficile da incorporare in un algoritmo.

Analogamente, si deve ricordare l'articolo 192 c.p.p. il quale dispone che «il giudice valuta la prova dando conto nella motivazione dei risultati acquisiti e dei criteri adottati. L'esistenza di un fatto non può essere desunta da indizi a meno che questi siano gravi, precisi e concordati». Anche in questo caso il requisito della gravità non può essere

[293] M. Gialuz, *Giurisdizione penale, intelligenza artificiale ed etica del giudizio, Giuffrè Fracis Lefebvre,* 2016, p.52 ss.
[294] G. Canzio, *Il dubbio e la legge,* in *Diritto Penale Contemporaneo,* 2018, p.2.

ricondotto solo a principi generali ed astratti ma è intenzionalmente aperto ad un insieme di interconnessioni delineato nella norma nel suo insieme.

Anche in relazione all'articolo 133 c.p., possiamo affermare che la valutazione degli effetti della pena può essere fatta in modo oggettivo dal giudice al fine di applicare una pena adeguata alla gravità del reato. Tuttavia, è difficile far rientrare in questa categoria l'intensità del dolo, il grado della colpa, i motivi per delinquere e il carattere del reo.

Pertanto, una serie di fattori come la ricerca, la verifica e il confronto tra dati e informazioni a disposizione del pubblico ministero, insieme all'applicazione di principi scientifici ed esperienziali, potrebbero essere di grande aiuto nell'attività dei giudici e, prima ancora, dei magistrati che presentano le accuse. Anche se ogni prova potrebbe fornire un contributo, la sintesi finale e la valutazione sulla personalità del reo deve essere frutto di una "metabolizzazione" su parametri di giudizio umani e non, per quanto "raffinati", espressivi di intelligenza artificiale.

3.3.1. Strumenti di riconoscimento facciale

Strumenti di riconoscimento facciale o "*facial recognition systems*" sono software che attraverso l'utilizzo di pattern e tecniche di comparazione associano al volto o al video di una persona sconosciuta l'immagine di un soggetto noto rinvenuta in quelle contenute nelle banche dati[295]. Si tratta di un sistema che sfrutta la tecnologia biometrica, ossia quella disciplina che studia le caratteristiche fisiologiche e comportamentali di identificazione dell'individuo.

In particolare, un sistema biometrico può essere definito come «un dispositivo automatico per l'identificazione di una persona sulla base di caratteristiche biologiche, che possono essere fisiologiche (se si riferiscono, ad esempio, ad impronte digitali, il disegno dell'iride, l'immagine del volto) ovvero comportamentali (si pensi al modo di battere sulla tastiera di un individuo)»[296].

I sistemi di riconoscimento facciale rappresentano, quindi, una branca della biometria, che si occupa di sviluppare algoritmi capaci di confrontare due immagini di un volto umano.

[295] E. Sacchetto, *Spunti di riflessione sul rapporto fra biometria e processo penale,* in *Diritto Penale Contemporaneo*, 2019, p.465 ss.

[296] A. Fonsi, *Prevenzione dei reati e riconoscimento facciale: il parere sfavorevole del Garante privacy sul sistema SARI Real Time,* in *Penale Diritto e Procedura*, 2021.

Secondo il Gruppo di lavoro per la tutela dei dati[297], il riconoscimento facciale può essere definito come «un trattamento automatico di immagini digitali che contengono volti di persone ai fini di identificazione, autenticazione, verifica o categorizzazione di tali persone. Il processo di riconoscimento facciale si compone di alcuni distinti sotto processi:

a) Acquisizione dell'immagine: il processo di rilevamento dei tratti del volto di una persona e la conversione in formato digitale. Nell'abito di un servizio online e mobile l'immagine può essere stata acquisita attraverso un sistema diverso, ad esempio con una macchina fotografica digitale e quindi trasferita ad un servizio online;
b) Individuazione di un volto: il processo di individuazione della presenza di un volto all'interno di un'immagine digitale e la marcatura dell'area corrispondente;
c) Normalizzazione: il processo di attenuazione delle variazioni all'interno delle regioni del volto individuate, ad esempio la conversione a una dimensione standard, la rotazione o l'allineamento delle distribuzioni del colore;
d) Estrazione di caratteristiche: il processo finalizzato a isolare ed estrarre le caratteristiche riproducibili e distintive dell'immagine digitale di una persona. L'estrazione delle caratteristiche può essere olistica, basata sui tratti, o una combinazione di due metodi. L'insieme delle caratteristiche essenziali può essere conservato per un successivo confronto in un modello di riferimento.
e) Registrazione: la prima volta che una persona si sottopone ad un sistema di riconoscimento facciale, la sua immagine e/o il modello di riferimento possono essere conservati come elementi per un successivo confronto;
f) Confronto: il processo che misura le somiglianze tra una serie di caratteristiche (del campione) con una serie di caratteristiche già registrate nel sistema. Le principali finalità del confronto sono l'identificazione e l'autenticazione/verifica. Una terza finalità del confronto è la categorizzazione, che consiste nell'estrarre le caratteristiche dell'immagine di una persona al fine di classificare questa persona in una o più grandi categorie (ad esempio età, sesso, colore dell'abbigliamento,

[297] Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati dall'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 200/58/CE.

ecc.). Non è necessario che un sistema di categorizzazione disponga di un processo di registrazione»[298].

Tali sistemi possono sia operare *ex-post*, ossia in differita, mediante la comparazione tra l'immagine da analizzare e la banca dati, sia in *real time*, procedendo in tempo reale al riconoscimento dei volti riscontrati nelle videoriprese delle telecamere.

Questi strumenti di automatizzazione delle procedure di identificazione si sono dimostrati molto utili sia per le forze di polizia nell'attività di prevenzione e repressione di reati, che per la difesa.

Risulta evidente che tale attività costituisce un trattamento di dati personali e, nello specifico, di dati biometrici.

Il 28 gennaio 2020 il Comitato Consultivo sulla protezione delle persone rispetto al trattamento automatizzato di carattere personale 108/1981[299], ha adottato le «*guidelines on Facial Recognition*» [300], individuando specifici orientamenti in materia di riconoscimento facciale e fornendo ad enti quali governi produttori di sistemi di riconoscimento facciale, e pubbliche amministrazioni che utilizzano tali tecnologie, le misure idonee a proteggere i diritti e le libertà degli interessati. In particolare, ai sensi dell'articolo 6 della convenzione 108, il trattamento di speciali categorie di dati, nei quali rientrano quelli biometrici, può essere svolto solo se legittimato da una base giuridica ed inoltre se nel diritto dello stato membro in cui è implementato siano previste garanzie adeguate rispetto ai rischi per gli interessati. Con specifico riferimento al riconoscimento facciale nel settore pubblico, il comitato consultivo della convenzione 108 sancisce espressamente che, dato lo squilibrio di poteri tra i cittadini e le autorità pubbliche, la base giuridica per il trattamento dei dati biometrici deve essere individuata esclusivamente in norme specifiche. Tali norme devono garantire: in primo luogo, che l'utilizzo di tali tecnologie sia strettamente necessario e proporzionato alle finalità per le quali tale uso è implementato; in secondo luogo, le necessarie garanzie da rispettare. L'impostazione delineata dalle line guida trova riscontro nel D.lgs. 51/2018 attuativo della Direttiva UE 680/2016.

---

[298] Gruppo di lavoro per la tutela dei dati Ex art.29, parere 2/2012, in https://www.privacy.it/archivio/grupripareri201202.html.

[299] Anche definita "Convenzione 108".

[300] Adottate il 28 gennaio 2021 dal comitato consultivo della convenzione sulla protezione delle persone rispetto al trattamento automatizzato di carattere personale 108/1981 in https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3.

Tuttavia, oggi questi strumenti vengono utilizzati esclusivamente con finalità repressiva; poiché nel 2019 la Cassazione ha adottato un atteggiamento di chiusura verso l'utilizzo di tale software da parte della difesa, rigettando, «la richiesta difensiva di procedere al riconoscimento facciale dell'imputato tramite la moderna tecnica S.A.R.I. in quanto, la difesa non aveva in alcun modo documentato la valenza scientifica dell'anzidetta tecnologia»[301], fornendo tuttavia una motivazione che sembrerebbe essere non coerente dal momento in cui è stato lo stesso ministero dell'interno ad aver predisposto lo sviluppo del programma S.A.R.I.

S.A.R.I.[302] è un software di riconoscimento facciale, di proprietà dell'azienda Parsec 3.26, utilizzato dalla Polizia di stato a partire dal 2017. Questo sistema consente di comparare le immagini riprese dalle videocamere di sorveglianza con le immagini contenute nella Banca Dati A.F.I.S.[303] e di confrontare poi il risultato con le informazioni contenute nel Casellario Centrale d'Identità della Polizia Criminale. All'interno del Casellario sono archiviati tutti i cartellini foto-segnaletici redatti dalle forze di Polizia italiane e straniere, le impronte digitali, i dati anagrafici e biometrici di tutti i soggetti che vengono sottoposti a rilievi.[304]

Questo software opera in due differenti modalità: in differita, nella sua versione "*Enterprise*", ed in "Real Time".

Il Garante per la Protezione dei Dati Personali definisce il sistema S.A.R.I. *Enterprise* come uno strumento che «non effettuerà elaborazioni aggiuntive rispetto al AFIS-SSA, ma si limiterà ad autorizzare alcune operazioni di ricerca nel *database* dei soggetti foto segnalati attraverso l'inserimento di un'immagine fotografica, che sarà elaborata automaticamente al fine di fornire l'elenco di foto segnaletiche somiglianti, ottenute attraverso un algoritmo decisionale che ne specifica la priorità. Pertanto, l'utilizzo del sistema S.A.R.I. Enterprise costituisce non un nuovo trattamento di dati personali, già previsto e disciplinato dalle predette fonti, bensì una nuova modalità di trattamento di dati biometrici, che dovrà essere effettuata nel rispetto delle regole previste dalla normativa

[301] Sentenza n.39731, della Sez. IV, Cass. Pen, 18.06.2019.
[302] "Sistema automatico di riconoscimento di immagini"
[303] "Automated Fingerprint Identification System" o "Sistema automatizzato di Identificazione delle Impronte".
[304] M.R. Carbone, *SARI, il riconoscimento facciale nella pubblica sicurezza: servono regole e trasparenza,* in *Agenzia Digitale*, 2021.

rilevante in materia di tutela dei dati personali»[305]. Si tratta di un sistema in grado di ricercare, attraverso algoritmi di riconoscimento facciale, un volto presente in un'immagine contenuta all'interno di una banca dati di soggetti foto-segnalati, nello specifico nel *database* AFIS.

Il Garante per la Protezione dei Dati Personali, ha inoltre descritto S.A.R.I. *Real time* come quel sistema che «consente, attraverso una serie di telecamere installate in un'area geografica predeterminata e delineata, di analizzare in tempo reale i volti dei soggetti ivi ripresi, confrontandoli con una banca dati predefinita per lo specifico servizio (denominata "*watch-list*"), la cui grandezza è di massimo 10.000 volti. Ove venga riscontrata, attraverso un algoritmo di riconoscimento facciale, una corrispondenza tra un volto presente nella *watch-list* ed un volto ripreso da una delle telecamere, il sistema è in grado di generare un *alert* che richiama l'attenzione degli operatori»[306]. Quindi il sistema, che si basa su quello *Enterprise*, è pensato per fornire risultati in tempo reale su flussi di video live provenienti da telecamere, posizionate in alcune aree pubbliche della città.

Si riscontrano numerose criticità circa l'utilizzo di tale strumento in quanto, soprattutto per i *software* che operano nella modalità *real time*, è evidente l'incidenza sui diritti fondamentali, quali il diritto alla tutela della dignità umana, il diritto alla riservatezza, il dritto alla protezione dei dati personali, il diritto all'identità, il diritto all'autodeterminazione del titolare dei dati personali, il diritto all'identità, il diritto all'autodeterminazione del titolare dei dati ed il diritto ad un equo processo[307].

In Italia, circa la legittimità dell'utilizzo di tale software si è più volte pronunciata l'Autorità Garante per la Protezione dei Dati Personali. Le maggiori criticità riguardano S.A.R.I. *Real Time*, poiché coinvolge un numero indeterminato di soggetti. Invece, per quanto concerne S.A.R.I. *Enterprise*, il Garante si è espresso in termini favorevoli. Quest'ultimo ha dichiarato la legittimità di tale sistema poiché non costituisce un nuovo trattamento di dati personali, già raccolti da AFIS, ma si tratta di un upgrade rispetto alla ricerca manuale che si eseguiva per il sistema precedente. Il Garante ha inoltre affermato che S.A.R.I. Enterprise costituisce un "mero ausilio" all'agire umano, senza sostituirsi all'operatore di polizia[308].

---

[305] Parere n.440, 26 luglio 2018.
[306] Parere n.127, 25 marzo 2021.
[307] R. Lopez, *La rappresentazione facciale tramite software*, *G. Giappichelli Editore Torino,* 2019, p.239.
[308] E. Currao, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?,* in *Diritto Penale e Uomo,* 2021, p.16 ss.

Di conseguenza sono sorti numerosi dubbi sulla motivazione in base alla quale questo giudizio non si può estendere alla modalità *Real Time*. Riguardo quest'ultima sono state rilevate numerose criticità in materia di trasparenza: non sono state rese note né le modalità di funzionamento, né la percentuale di successo nell'identificazione dei soggetti in modalità *Real Time*, né il tasso di errore statistico del sistema. L'assenza di tali informazioni impedisce di valutare l'affidabilità dell'algoritmo di riconoscimento utilizzato[309].

Proprio per risolvere queste incertezze il Garante della privacy si è pronunciato sul funzionamento di S.A.R.I. *Real Time* con esito negativo. Nel parere del 25 marzo 2021, il garante ha statuito che per tale attività di trattamento dei dati biometrici non esiste oggi una base giuridica idonea. Difatti, secondo il garante, S.A.R.I Real Time effettua un «trattamento automatizzato su larga scala, determinando il passaggio da una sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale»[310].

Una disposizione normativa legittima sarebbe, ad avviso dell'Autorità, l'unico strumento in grado di effettuare una valida protezione di tutti i diritti e delle libertà coinvolte, così da rendere prevedibile l'utilizzo di tali sistemi ed evitare il rischio di usi arbitrari.

3.3.2. Intercettazioni e captatori informatici

Da tempo durante le indagini preliminari, il GIP, utilizza l'ausilio del captatore informatico. Un *malware* che, inserito in maniera occulta all'interno di dispositivi elettronici, è in grado di intercettare le conversazioni della persona sottoposta alle indagini. La sua denominazione tecnica è "*Trojan horse*".

Per definizione un *malware*, o c.d. "programma malvagio", descrive un programma volto a danneggiare il funzionamento e la sicurezza del sistema operativo "attaccato". Tale s*oftware* cerca di invadere, danneggiare o disattivare computer, sistemi, reti, *tablet* e dispositivi mobili, interferendo con il loro normale funzionamento. Tra le categorie più diffuse si ricordano virus, *trojan horse, keylogger, worm* e *backdoor*[311].

Ci troviamo di fronte ad una grande novità rispetto alla microspia, dispositivo utilizzato in precedenza per le intercettazioni telefoniche, a differenza di quest'ultima, il captatore,

[309] J. Della Torre, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della hign court of justice (ma raccoglie le critiche del garante della privacy d'oltremanica),* in *Sistema Penale*, 2020, p.17 ss.
[310] Comitato Consultivo della Convenzione 108.
[311] "Malware" in *Enciclopedia Treccani online.*

viene inserito da remoto all'interno di *smarthphone, tablet* o *computer*, andando ad "intercettare" non solo le comunicazioni telefoniche, ma tutte le attività svolte con il proprio dispositivo. Una volta istallato, il captatore assume la gestione dell'intero sistema, insieme alla correlata possibilità di registrare ogni attività della tastiera, dello schermo, ed inoltre alla possibilità di effettuare *screen-shot* di quest'ultimo[312].

Una volta introdotto nel sistema informatico, il captatore è in grado di: «leggere quello che è archiviato nel dispositivo, dal contenuto dei documenti di testo alla rubrica dei contatti, fino alle comunicazioni scambiate via *Whatsapp*, *Telegram*, *Messanger*, gestire da remoto i software che vengono istallati; scaricare immagini e filmati e controllare quelli presenti nelle gallerie; memorizzare i pulsanti sulla tastiera e fare lo *screenshot* di quello che compare sullo schermo; collegarsi ad internet; inserire dati o alterare quelli esistenti; rintracciare gli spostamenti se l'apparecchio infettato è dotato di sistema *gps*; accendere il microfono o la telecamera consentendo di svolgere un'intercettazione ambientale o una videoripresa; tutte le funzioni che possono essere calibrate sulla base delle esigenze del caso specifico adottando opportuni accorgimenti tecnici»[313].

Il materiale che viene estrapolato è immediatamente traferito, attraverso procedure che ne assicurano l'integrità, all'interno di un archivio digitale[314].

L'utilizzo di questi software per lo svolgimento delle indagini è reso indispensabile dal fatto che le nuove forme di manifestazione del crimine si avvalgono della tecnologia informatica per la commissione dei reati. Se quindi da un lato, sembra indispensabile riconoscere l'importanza dell'accesso a tali nuovi strumenti tecnologici per perseguire un'efficacie azione di contrasto del crimine, dall'altro lato, risulta molto delicato individuare quale siano i confini del loro impiego per fini investigativi. Perciò si ricerca un equilibro con la confliggente esigenza di tutela dei diritti fondamentali degli individui coinvolti nella vicenda processuale[315].

Tuttavia, affinché sia possibile l'utilizzo dei *malware* in esame, è necessario che siano conformi a requisiti tecnici stabiliti dal Ministero della giustizia. È evidente che tali

---

[312] T. Di Giulio, *L'utilizzo del captatore informatico: il "trojan di Stato",* in *Diritto Consenso*, 2021.

[313] G. Caneschi, *Le nuove indagini tecnologiche e la tutela dei diritti fondamentali. L'esperienza del captatore informatico*, in *Diritto Penale Contemporaneo*, 2019, p.418 ss.

[314] R. Giorli, *Le intercettazioni: il loro impiego quale mezzo di ricerca della prova,* in *Diritto Consenso*, 2021.

[315] R. De Vita, A. Ludisia, *Vita digitale a rischio: i captatori informatici tra pericoli per i diritti umani e rduzionismo giuridico,* in *Osservatorio Cybersecurity Eurispes, 2019, p.9 ss.*

strumenti, essendo altamente invasivi, rappresentano una minaccia alla riservatezza non solo degli indagati, ma anche dei soggetti terzi coinvolti. Pertanto, è necessaria una specifica tutela che limiti l'impatto di questi sulla *privacy*, poiché si tratta di un mezzo per effettuare intercettazioni, ed in quanto tale, limitativo della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione. La Costituzione italiana, all'articolo 15, prevede che le intercettazioni devono essere disposte solo con un «atto motivato dall'autorità giudiziaria» e nel rispetto delle «garanzie stabilite dalla legge», garantendo così sia una riserva di legge che di giurisdizione. È dunque importante trovare un equilibrio tra l'efficacia delle investigazioni e il rispetto dei diritti fondamentali dei soggetti coinvolti, in particolare il diritto alla riservatezza e alla tutela dei dati personali[316].
Di fatto, le varie riforme legislative in materia di intercettazioni, culminate con l'entrata in vigore della legge n.103 del 2017, meglio nota come "riforma Orlando", hanno avuto come obbiettivo principale quello di trovare un giusto equilibrio tra la tutela delle privacy e le esigenze investigative delle forze dell'ordine.
In particolare, l'articolo 266 del codice di procedura penale stabilisce una distinzione tra le intercettazioni effettuate in un luogo di privata dimora e quelle svolte in luoghi pubblici o comunque aperti al pubblico. Nel primo caso, l'utilizzo del captatore è ammesso solo se sussiste un fondato motivo per ritenere che l'attività criminosa si stia svolgendo in quel luogo.
Tuttavia, vi sono alcune eccezioni a questa regola, ad esempio, è prevista una deroga per i reati elencati dal comma 3 *bis* e comma 3 *quarter* dell'articolo 51 c.p.p., che si riferisce alla criminalità organizzata, al terrorismo, all'induzione alla prostituzione ed alla violenza sessuale. In questi casi, l'utilizzo del captatore è permesso anche in assenza di un fondato motivo per ritenere che l'attività criminosa sia in atto.
Un ulteriore eccezione all'obbligo di fondato motivo per utilizzare un captatore è stabilita al comma 2 *bis* dell'articolo 266 c.p.p. Secondo questa norma l'uso del captatore nei luoghi di privata dimora è consentito solo «per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'articolo 4»[317]. Invece, per quanto riguarda i luoghi aperti al pubblico, l'uso del

[316] [316] G. Caneschi, *Le nuove indagini tecnologiche e la tutela dei diritti fondamentali. L'esperienza del captatore informatico*, cit, p.419 ss.
[317] Ai sensi del codice di procedura penale, articolo 266 bis, comma 2bis.

captatore è sempre consentito per i reati elencati dal comma 1 del medesimo articolo del codice di procedura penale.

Inoltre, l'articolo 267 c.p.p. prevede che, per garantire la riserva di giurisdizione sancita dall'articolo 15 della Costituzione, le intercettazioni mediante captatore devono essere autorizzate da un decreto motivato dal giudice delle indagini preliminari, solo quando vi sono gravi indizi di reato e quando sia assolutamente necessario per portare avanti le indagini.

Per il p.m. che utilizza il captatore informatico, data la conseguente restrizione del diritto di riservatezza del singolo, il legislatore ha previsto un ulteriore obbligo di motivazione. Quest'ultimo, all'interno del decreto, deve specificare «le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini», in aggiunta «se si procede per delitti diversi da quelli dell'articolo 51, commi 3-bis e 3-quarter, e dai delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione», deve indicare, per dimostrare che vi sia un'attività criminosa in atto «i luoghi e il tempo, anche indirettamente determinati, in relazioni ai quali è consentita l'attivazione del microfono»[318].

La legge che regolamenta l'utilizzo del captatore informatico come strumento di intercettazione ambientale, sebbene sia stata criticata per aver omesso la regolamentazione di altri possibili utilizzi di questo strumento, sembra essere un esempio positivo di come sia possibile favorire e disciplinare l'uso di strumenti tecnologici nel sistema giudiziario nel rispetto dei principi costituzionali[319].

Tuttavia, si ritiene necessario un ulteriore intervento legislativo per regolamentare gli utilizzi del captatore che al momento non sono ammessi a causa della mancanza di una specifica disciplina, mancanza che genera una un vuoto legislativo sprovvisto di protezione. Questo intervento dovrebbe essere in linea con il principio di riserva di legge e giurisdizione sancito dall'articolo 15 della Costituzione.

[318] Ai sensi del codice di procedura penale, articolo 266 comma 1.

[319] C. Morelli, *Trojan di stato, le novità della legge di conversione sul DL intercettazioni,* in *Altalex,* 2020.

3.4. Responsabilità penale dei sistemi intelligenti

In una società ove l'intelligenza artificiale riveste un ruolo sempre più incisivo nella nostra vita quotidiana e si assistite sempre più frequentemente a droni autori di omicidi, auto pilotate senza conducente protagoniste di incidenti stradali, *bot* del reato di bagarinaggio online o social *bot* autori di reati di molestie, sembra opportuno chiedersi come poter regolamentare la responsabilità penale dei c.d. "sistemi intelligenti"[320], ovvero "*machina delinquere potest*"?

Occorre determinare a chi sia attribuibile il reato commesso (alla macchina, al suo programmatore o utilizzatore?) e in che modo debba essere delineata tale responsabilità.

In particolare, alcuni autorevoli autori denunciano l'esigenza di modificare e adattare le attuali fattispecie di reato contenute nel codice penale, al fine di ricomprendere anche altre forme di responsabilità differenti da quelle in essere e ad esse non riconducibili[321].

La questione, poi, si complica ulteriormente quando si tenta di individuare la responsabilità degli "agenti intelligenti" di *machine learning* e *deep learning* dove – a differenza dei "sistemi intelligenti" in cui l'algoritmo è impostato interamente dal programmatore – insiste una conoscenza empirica, basata, dunque, sulla esperienza immediata e pratica[322].

Nei "sistemi intelligenti", infatti, la macchina costituisce semplicemente una *longa manus* del programmatore – utilizzatore, mediante la quale viene commesso il reato, riducendosi pertanto a un mero strumento. L'azione criminosa sarà imputabile sia sul piano oggettivo (condotta omissiva) che soggettivo (dolo, colpa o preterintenzione) all'uomo[323].

Diversamente, nelle macchine addestrate con algoritmi di *machine learning* o *deep learning* attribuire la responsabilità all'uomo risulta ben più complicato[324].

---

[320] D. Curtotti, W. Nocerino, *Le intercettazioni tra presenti con captatore informatico*, in Baccari G.M., Bonzano G., La Regina K., Mancuso E.M. (a cura di), Le recenti riforme in materia penale, Milano, 2017, 557 ss.

[321] F. Basile, Intelligenza artificiale e diritto penale: quale aggiornamento e quale nuova riflessione, in https://www.researchgate.net/publication/355049151, 2021, 9 e ss.

[322] P. Bronzo, *Intercettazioni ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, in Giostra G., Orlandi R. (a cura di), *Nuove norme in tema di intercettazioni*, cit., 236 ss.

[323] Cfr. Marinucci G., Dolcini E., Gatta G.L., Manuale di diritto penale: parte generale, Milano, 2018.

[324] A. Cappellini, *Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale*, in *Discrimen*, 2019.

Tali difficoltà emergono chiaramente dalla stessa interpretazione dell'art. 27 della Costituzione che, sancendo il principio della personalità della responsabilità penale, prevede una responsabilità penale per un fatto proprio e colpevole, richiedendosi a tal fine che il fatto possa essere addebitato all'autore quantomeno al titolo di colpa.

Inoltre, sempre l'art. 27 della Costituzione statuisce il principio della finalità rieducativa della pena, secondo cui «la pena deve tendere alla rieducazione del condannato».

Ecco allora che sorgono nuovi interrogativi: «Possono essi essere considerati persone? O, quanto meno, possono essere assimilati alle persone, al fine di un'attribuzione di responsabilità non solo civile, ma anche penale? [...].

Possiamo davvero parlare di un coinvolgimento soggettivo dell'autore – macchina al fatto commesso? Possiamo concepire una rimproverabilità, per l'appunto personale, della macchina? Possiamo parlare di capacità di intendere e di volere, in relazione a una rete neurale? Possiamo configurare una "colpa" o addirittura un "dolo" dell'algoritmo?»[325].

Sul punto c'è chi risponde positivamente[326], ritenendo che ai sistemi IA possa essergli attribuita, *rectius* estesa, la responsabilità personale prevista per gli enti ai sensi del D.lgs. 231/2001.

Tuttavia, a questa affermazione si può agilmente obiettare che tale *fictio giuridica* non può valere anche per i sistemi IA, ciò in quanto la responsabilità *ex* D.lgs. 231/2001 riproduce lo schema della responsabilità individuale che presuppone sempre una finalità rieducativa delle sanzioni amministrative comminate agli enti, non possibile – invece – per i sistemi di intelligenza artificiale[327].

Ciò nonostante, non può che auspicarsi un intervento legislativo volto a regolamentare e chiarire il regime della responsabilità penale degli attuali e futuri agenti intelligenti a tutela degli individui[328].

Al contrario, il rischio è quello di assistere a pericolosi vuoti normativi che si tradurrebbero in zone franche, «sacche di illiceità all'interno delle quali non è possibile

---

[325] così testualmente, Basile F., *Intelligenza artificiale e diritto penale: quale aggiornamento e quale nuova riflessione*, cit., 9 e ss; D. Falcinelli, *Il dolo in cerca di una direzione penale. Il contributo della scienza robotica ad una teoria delle decisioni umane*, in *Arch. pen.*, fasc. 1, 2018, 9.

[326] M. Bassini, L. Liguori, O. Pollicino, *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, in F. Pizzetti (a cura), *Intelligenza artificiale*, cit., pp. 363 ss., ai quali, pertanto, è in questa sede possibile rinviare.

[327] P. Severino, *Op. cit.*, 532 ss.

[328] C. Piergallini, *Intelligenza artificiale: da "mezzo" ad "autore del reato",* in Rivista Italiana di Diritto e Procedura Penale, 2020, 4, 1743 s.s.

imputare alcuna responsabilità alla persona fisica»[329], con l'effetto di continuare ad ignorare un fenomeno ormai divenuto parte integrante della società moderna.

[329] Così Basile F., *Intelligenza artificiale e diritto penale: quale aggiornamento e quale nuova riflessione*, cit., 9 ss.

CONCLUSIONI

L'intelligenza artificiale, grazie all'ingente volume dei dati a disposizione e alla loro velocità e varietà, è un fenomeno in rapidissimo sviluppo; fenomeno, che attraverso l'automatizzazione di numerosi processi, ha portato a una vera e propria rivoluzione.

Il lavoro svolto ha evidenziato come l'utilizzo degli algoritmi, nello svolgimento delle attività di polizia predittiva, necessiti di una precisa regolamentazione normativa in grado di assicurare, da un lato, un bilanciamento tra tutela dei principi e dei diritti fondamentali, dall'alto, la pubblica sicurezza e l'ottimizzazione delle forze di polizia.

Ben si comprende come l'uso degli algoritmi nell'ambito della sicurezza e della giustizia non vada demonizzato a prescindere, ma necessiti di una regolamentazione puntale da parte dell'ordinamento. La sinergia tra uomo e macchina affascina da secoli l'essere umano e può costituire un valido supporto alle attività decisionali, ma occorre fissare dei limiti e delle linee guida uniformi a livello internazionale, per evitare che i grandi benefici lascino spazio alle gravi violazioni dei diritti fondamentali.

Tutti gli scenari analizzati sembrano accomunati dall'attuale assenza di una regolamentazione normativa, e in particolare di una regolamentazione che prevenga o reprima offese penalmente rilevanti. Le previsioni in esame, tuttavia, potrebbero presto divenire realtà, confermando che l'assenza normativa comporterebbe conseguenze drammatiche.

Difatti, attraverso l'utilizzo dei *software* di *pedictive policing* quale strumento di prevenzione della criminalità, è possibile l'elaborazione di ingenti quantità di informazioni e la conseguente massimizzazione dell'operato della polizia volto a garantire la tutela della sicurezza urbana. La combinazione di Big Data, macchine intelligenti e tecniche analitico statistiche abbinate con tecniche criminologiche, fa si che tali *software* possano essere utili soprattutto per prevenire la commissione di reati di tipo predatorio. Tali reati si contrappongono ai reati violenti dove non risulta possibile, a causa dell'elemento "impulsività", applicare le competenze criminologiche su cui si fondano le tecniche di polizia predittiva. Risulta quindi impossibile ignorare i benefici che l'utilizzo di tali algoritmi prospetta all'interno del nostro ordinamento.

Tuttavia, è necessario evidenziare l'incidenza di tali strumenti di IA sui principi e sui diritti fondamentali dell'individuo. Dall'analisi di questo lavoro sono emersi evidenti profili di incompatibilità tra l'utilizzo di *software* di *predictive policing* e la tutela dei dati

personali. L'attuale normativa, contenuta nel GDPR, non risulta in grado di tutelare in maniera sufficientemente esaustiva e chiara i diritti in esame. Tali diritti si fondano sull'entità dei dati, sensibili e non, che alimentano gli algoritmi. Ciò comporta vuoti interpretatavi che facilitano l'elusione della normativa e, di conseguenza, non garantiscono la tutela dei diritti degli individui.

Inoltre, elementi di incompatibilità sorgono in tema di trasparenza e non discriminazione. Ad oggi, non risulta possibile garantire con assoluta certezza che i software di polizia predittiva producano informazioni corrette, complete ed eque. Problema che concerne la modalità di funzionamento dell'algoritmo, in quanto il risultato finale è posto in un rapporto di dipendenza con il data set iniziale. In altre parole: dipende dalla qualità dei dati forniti.
Infine, non risulta sempre possibile la conoscibilità del codice sorgente dell'algoritmo e delle modalità di funzionamento, in quanto, poiché ideati da imprese commerciali, questi ultimi sono coperti dalle norme sul diritto d'autore, sulla tutela brevettuale ed in particolare sul segreto industriale a tutela dei software.
Le attività di polizia di prevenzione sono ritenute efficaci fin tanto che riescono ad anticipare la commissione di un delitto o favoriscono l'arresto in flagranza dell'autore. Ribadita la necessità di analizzare dati provenienti da fonti affidabili e sicure per avere un'elaborazione informatica di qualità "non sembra sussistere, in tali casi, alcuna problematica sostanziale – quantomeno sul piano processuale – poiché, tanto il principio di materialità, quanto il principio di offensività sembrano rappresentare idonei ed adeguati argini rispetto alla circostanza che l'impiego degli algoritmi in discorso possa alimentare una deriva del giudizio penale verso la punibilità delle mere volontà criminali, piuttosto che delle condotte concretamente poste in essere da un determinato individuo"[330]. Invece, quando i risultati dell'elaborazione algoritmica hanno rilevanza nella attività della polizia giudiziaria, si impongono esigenze di tutela dell'accertamento probatorio.
Difatti, per quanto concerne l'ammissibilità nel processo dei calcoli matematici di un programma informatico e della validità delle prove per mezzo di algoritmi, è auspicabile un intervento legislativo volto a disciplinare i presupposti e le modalità operative di

[330] D. Polidoro, tecnologie informatiche e procedimento penale, Op. cit., p.10.

questa particolare specie di indagini digitali. La necessità è quella di stabile un equilibrio tra i diritti lesi e l'interesse al perseguimento della giustizia. Al netto di tali considerazioni, è solo tramite un approccio normativo che si potrà scongiurare il rischio di trasformare un enorme potenziale di crescita in un'arma lesiva delle garanzie e della dialettica processuale.

L'essere umano deve rimanere il modello in funzione del quale vengono costruiti gli algoritmi di IA e il soggetto beneficiario delle loro elaborazioni. Non si ritiene opportuno che per i dispositivi informatici siano pervisti margini di autonomia tali da determinare effetti giuridici diretti nella sfera degli interessati, se non nella misura in cui si tratti di attività vincolate da chiari parametri a monte e sia sempre il responsabile umano del procedimento a far propria la decisione algoritmica. Questo non significa, soprattutto per quanto riguarda gli strumenti di indagine, che l'uomo non possa essere oggetto, inteso come destinatario della loro attività, ma che ciò debba avvenire solo nel momento in cui a tale oggetto siano riconosciuti e resi concretamente esercitabili i diritti tradizionalmente previsti.

La tutela dei diritti fondamentali compromessi dai software di polizia predittiva viene quindi garantita dalla tipologia, quantità e qualità dei dati imput forniti al sistema. Di ciò deve tenere conto il legislatore nell'attuare un piano di regolamentazione, tendenza che già emerge dagli utili interventi normativi dell'Unione Europea. Bisogna, quindi, evidenziare e avere ben chiare le problematiche in materia e nel contempo considerare che non sia possibile oggi pensare che strumenti di IA, quali quelli in esame, non facciano parte della quotidianità.

In conclusione, le applicazioni dell'IA possono agevolmente contribuire a realizzare alcuni degli obbiettivi propri del diritto penale, ma è necessario considerare sempre l'IA quale scienza fallibile, non sempre idonea a fornire risultati correttamente rappresentativi della realtà. Si auspica una regolamentazione chiara e dettagliata concernente l'utilizzo dei software di polizia predittiva in tutte le loro possibili applicazioni, non vietandone il totale utilizzo bensì prevedendo interventi legislativi volti a valorizzare la potenzialità nella tutela dei diritti riconosciuti dall'ordinamento.

BIBLIOGRAFIA

Ainora I., *Polizia predittiva: la nuova frontiera dell'investigazione,* in *Informare, magazine di libera informazione,* 2022.

Alecci S., Bertacchini E., Bove M., et al., *Prevedibilità, predittività e umanità del giudicare (XIII Assemblea Nazionale degli Osservatori sulla Giustizia Civile),* in "Rivista scientifica di Diritto Processuale Civile", 2018.

Barbujani E., *La giustizia predittiva e l'incalcolabile*, in *Cassa forense*, 2020.

Basile F., *Esiste una nozione ontologicamente unitaria di pericolosità sociale? Spunti di riflessione, con particolare riguardo alle misure di sicurezza e alle misure di prevenzione,* in "Rivista italiana diritto processuale penale", 2018.

Basile F., *Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione,* in *Il sistema penale ai confini delle* hard sciences. *Percorsi epistemologici tra neuroscienze e intelligenza artificiale*, a cura di F. Basile, M. Caterini, S, Romano, Pisa 2021.

Basile F., *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine,* in *Diritto Penale e Uomo - DPU*, fasc. 10/2019 (online).

Bassini M., Liguori L., Pollicino O., *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi?,* in *Intelligenza artificiale protezione dei dati personali e regolazione,* a cura di F. Pizzetti Torino, 2018.

Bennett Moses L., Chan J., *Algorithmic prediction in policing: assumptions, evaluation, and accountability,* in *Taylor & Francis Online,* 2016.

Bonafe M., Trevisi C., *Intelligenza artificiale, l'algoritmo "trasparente": un rebus ancora da sciogliere,* in "Agenda Digitale", 2019 (online).

Bonetti P., *Funzioni e corpi di polizia: problemi giuridici e prospettive per un riordino costituzionalmente orientato*, in "ASTRID", 2009.

Brayne S., *Predict and Surveil: Data, Discretion, and the Future of Policing*, in "Oxford University Press", 2020.

Bronzo P., *Intercettazioni ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, in *Nuove norme in tema di intercettazioni,* a cura di Giostra G., Orlandi R., Torino 2018.

Burgess M., *UK police are using AI to inform custodial decisions – but it could be discriminating against the poor,* in "Wired", 2018.

Calderini B., *Sorveglianza di massa, la Cina è un sistema a "diritti affievoliti": perché lo tolleriamo e cosa rischiamo*, in "Agenzia Digitale", 2022.

Caneschi G., *Le nuove indagini tecnologiche e la tutela dei diritti fondamentali. L'esperienza del captatore informatico,* in *Diritto Penale Contemporaneo – DPC,* fasc. 2/2019.

Canzio G., *Il dubbio e la legge,* in *Diritto Penale Contemporaneo – DPC,* fasc. 1/2018.

Caplan J.M., Kennedy L.W., Barnum J.D., Piza E.L., *Crime in Context: Utilizing Risk Terrain Modeling and Conjunctive Analysis of Case Configurations to Explore the Dynamics of Criminogenic Behavior Settings.,* in "City University of New York", 2017.

Cappellini A., *Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale*, in "Discrimen", 2019.

Carbone M.R., *SARI, il riconoscimento facciale nella pubblica sicurezza: servono regole e trasparenza,* in "Agenzia Digitale", 2021.

Carratta A., *Decisione robotica e valori del processo,* in “Rivista di diritto processuale”, 2020.

Carrer S., *Se l’amicus curiae è un algoritmo: il chicchierato caso Loomis alla Corte Suprema del Wisconsin*, in “Giurisprudenza Penale Web”, 2019.

Castelletti L., Rivellini G., Straticò E., *Efficacia degli strumenti di Violence Risk Assessment e possibili ambiti applicativi nella psichiatria forense e generale italiana,* in “Journal of Psychopathology”, 2014.

Cath C., Wachter S., Mittelstadt B., Taddeo M., *Artificial Intelligence and the Good Society: the US, EU and UK approach*, 2018.

Chiusi F., Fischer S., Kayser-Brill N., et l., *Automating Society Report 2020*, Berlino 2020.

Cinque G., *La sicurezza delle comunità connesse dev’essere* «*integrata*»*: ecco come realizzarla,* in “Agenzia Digitale”, 2022.

Comitato di esperti sugli intermediari di Internet (MSI-NET), *Algorithms and Human Rights*, Consiglio d’Europa, in *rm.coe.int*, 2017.

Commissione Europea, Piano coordinato sull’intelligenza artificiale, 2018, Bruxelles.

Commissione Europea, *una definizione di IA: principali capacità e discipline scientifiche, 2019.*

Consiglio di Stato, sezione VI, 4 febbraio 2020, n.881.

Contissa G., Lasagni G., Sartor G., *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in “Diritto di internet”, 2019.

Corte Costituzionale, 27 marzo 1987, n. 77.

Corte di Cassazione, Sezione I Civile, Ordinanza n.14382/2021, punto VII.

Corte Europea dei Diritti dell'Uomo, *Guida all'articolo 8 della Convenzione europea sui diritti dell'uomo.*

Currao E., *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?,* in *Diritto Penale e Uomo,* 2021.

Curtotti D., Nocerino W., *Le intercettazioni tra presenti con captatore informatico*, in *Le recenti riforme in materia penale*, a cura di Baccari G.M., Bonzano G., La Regina K., et al., Milano 2017.

De Hert P., Papakonstantinu V., *The New Police and Criminal Justice Data Protection Directive: A First Analysis,* in "New Journal of European Criminal Law", 2016.

De Vita R., Ludisia A., *Vita digitale a rischio: i captatori informatici tra pericoli per i diritti umani e rduzionismo giuridico,* in "Osservatorio Cybersecurity Eurispes"*, 2019.*

Della Torre J., *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della hign court of justice (ma raccoglie le critiche del garante della privacy d'oltremanica),* 2020.

Di Giulio T., *L'utilizzo del captatore informatico: il "trojan di Stato",* 2021.

European ethical Charter on the use of Artificial Intelligence in judicial system and their environment, 2018.

Falcinelli D., *Il dolo in cerca di una direzione penale. Il contributo della scienza robotica ad una teoria delle decisioni umane*, in "Arch. pen.", fasc. 1/2018.

Famiglietti F., *La polizia di sicurezza, Manuale di diritto di pubblica sicurezza,* Roma 2014.

Ferguson A., *Predictive Policing and Reasonable Suspicion,* 2012.

Ferrero E., *Le Smart City nell'ordinamento giuridico,* in "Il Piemonte delle Autonome rivista quadrimestrale di scienze dell'Amministrazione", fasc. 4/2014.

Figini S., Porta V., *Algoritmi anticrimine: tutte le tecnologie in campo,* in "Agenda Digitale", 2019.

Fonderi A., *La pericolosa passione della Cina per i dati biometrici,* in "Wired", 2020.

Fonsi A., *Prevenzione dei reati e riconoscimento facciale: il parere sfavorevole del Garante privacy sul sistema SARI Real Time,* in "Penale Diritto e Procedura", 2021.

Friedman B., *Unwarred: Policing without permission,* in "Ferrar Straus and Giroux", 2017.

Gerstner D., *Using Predictive Policing to Prevent Residential Burglary – Findings from the Pilot Project P4 in Baden-Wurttember, Germany,* Department of Criminology, Max Planck Institute for Foreign and International Criminal Law, Germany 2015.

Gialuz M., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio, Giuffrè Fracis Lefebvre,* 2016.

Gialuz M., *Quando la giustizia penale incontra l'intelligenza artificilale: luci e ombre dei risk assessment tools tra stati uniti ed europa*, in "Diritto Penale Contemporaneo-DPC", fasc. 3/2019.

Gilsinan J.F., *The Numbers Dilemma: The Chimera of Modern Police Accountability System,* in St. Luis University Public Law Review, 2012.

Giorli R., *Le intercettazioni: il loro impiego quale mezzo di ricerca della prova,* 2021.

Giraldi A., *Algorithms and Big Data Towards a crime-preventing groupware,* in *Roma Tre Law Review*, volume three/number two/twenty twenty one, 2021.

Giraldi A., Grossi L., Massaro A., Notaro L., Sorbello P., *Intelligenza artificiale e giustizia penale,* 2020.

Hannemyr G., Seres S., Sunde I.M., *Predictive policing, can data analysis help the police to be in the right place at the right time?,* 2015.

Hardyns W., Rummens A., *Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges,* in "European Journal on Criminal Policy and Research", 2018.

Iaselli M., *Sistemi automatizzati per il consenso serve la trasparenza dell'algoritmo,* in *Altalex,* 2021.

Sorrentino U., Zanobini G., voce *Polizia predittiva,* in *Vocabolario della lingua italiana*, 1935.

Joh E. E., *The Undue Influence of survelliance Tecnology companies on Policing,* in *New York University Law Review Online,* 2017.

Kamensky J.M., *Fighting Crime in a New Era of Predictive Policing,* in *Governing the future of states and localities*, 2013.

Kaplan J., *Intelligenza artificiale, Guida al futuro prossimo,* Luiss *University Press,* 2018.

Kent police Corporate Services Analysis Department, *PredPol operetional review – initial findings, in Kent-police-pp-report.pdf, 2013.*

Kerber V., *A short history of predictive policing in the United States,* in *Medium*, 2022.

Lamanuzzi M., *Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento 2017/679/UE e nuove responsabilità per gli enti,* in *vita e pensiero Jus,* 2017.

Lavogna A., Suffia G., *La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale,* in *Giustizia penale e nuove tecnologie, Diritto penale contemporaneo*, 2021.

Lippert-Rasmussen K., *Born free and equal? A philosophical inquiry into the nature of discrimination,* in *Oxford University Press*, 2014.

Lopez R., *La rappresentazione facciale tramite software, G. Giappichelli Editore Torino,* 2019.

Losano M.G., *Corso di Informatica Giuridica*, in Unicopli, Milano, 1983, Vol 1.

Lum K., Isaac W., *To predict and serve?,* in *Royal Statistical Society,* 2016.

Lynskey O., *Criminal justice profiling and EU data protection law: precarious protection from predictive policing,* Cambridge University Press, 2019.

Mac A., *Dati biometrici, la mappa della sorveglianza paese per paese,* in *Sole 24 ore,* 2019.

Manes V., *Intelligenza artificiale e giustizia penale,* Giappichelli Editore, 2021.

Mantovani R., *Innovazione Precobs, il computer made in Germany che prevede i crimini,* in *Focus*, 2014.

Marinucci G., Dolcini E., Gatta G.L., Manuale di diritto penale: parte generale, Milano, 2018.

Martorana M., *Intelligenza Artificiale e diritto penale, la risoluzione del Parlamento europeo,* in *Altalex,* 2021.

Martorana M., Pinelli L., *Polizia e giustizia predittive: cosa sono e come vengono applicate in Italia,* in *Agenda Digitale,* 2021.

Massimini M., *Automatizzazione dei dati personali: significato, benefici e dubbi in ottica GDPR,* in *Privacy.it,* 2021.

Mastrobuoni G., *Impact: Imagine being able to predict a crime in the future*, in *Research case study dell'Università di Essex*, 2018.

McCarty J., Minsky M.L., Rochester N., Shannon C.E., "*A proposal for the Dartmouth summer research project on artificial intelligence"*, in Dartmouth College, 1955.

Meijer A., Wessels M., *Predictive Policing: Review of Benefits and Drawbacks,* in *International Journal of Public Administration*, 2019.

Morabito C., *La chiave del crimine,* in *Polizia Moderna,* 2015.

Morelli C., *Algoritmi e diritti umani: si rischia la collisione? (immaginate a danno di chi?),* in *Altalex,* 2018.

Morelli C., *Trojan di stato, le novità della legge di conversione sul DL intercettazioni,* in *Altalex,* 2020.

Morelli C., *XLAW, il brevetto italiano di polizia predittiva*, in Altalex, 2022.

Natale A., *Una giustizia (im)prevedibile?*, in *questione di giustizia,* fascicolo 4/2018,

Nobels M., Ward J.T., Tillyer R., *The Impact of Neighborhood on Spatiotemporal Patterns of Burglary,* in *Journal of Research in Crime and Delinquency*, 2016.

Norga A., *4 vantaggi e 4 svataggi della polizia predittiva,* in *Liberties*, 2021

Oosterloo S., Van Schie G., *The Politics Biases of the "Crime Anticipation System" of the Dutch Police,* Utrecht Data School, in Utrecht University, 2018.

Osterloo S., Schafer M.T., *Predicting crime trough data: analysis of the data assemblage of the Dutch Crime Anticipation System,* in *New Media and Digital Culture*, Utrecht University, 2020.

Oswald M., Grace J., Urwin S., Barnes G.C., *Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality,* in *Information & Communications Technology Law*, 2018.

Padua G., *Intelligenza artificiale e giudizio penale: scenari limiti e prospettive,* in *Giappichelli,* 2018.

Pagallo U., *Etica e diritto dell'Intelligenza Artificiale nella governace del digitale: il Middle-out Approach,* in *Intelligenza artificiale: il diritto, i diritti e l'etica,* a cura di Ruffolo U., *Giuffrè Francis Lefebvre,* Milano, 2020, p. 29-41.

Paolozzi F., *Focus sulla Giurisprudenza Costituzionale in materia di Sicurezza Pubblica*, in *Servizio Affari legislativi e qualità dei processi normativi della giunta regionale,* Regione Emilia-Romagna, 2011.

Parlamento Europeo e del Consiglio dell'Unione Europea, Direttiva (UE) 2016/680, in *Gazzetta ufficiale dell'Unione europea.*

Parlamento Europeo, *Report on foundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement,* 2017.

Parlangeli D., *Google ti mostra come funziona il Machine Learning, dal tuo browser,* in *Wired*.it, *2017.*

Parodi C., Sellaroli V., *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco,* in *Diritto Penale Contemporaneo,* 2019.

Pelliccia R., *Polizia Predittiva: il futuro della prevenzione criminale?,* in Cyberlaws.

Pellissero M., Riverditi M., *Reati contro la personalità dello stato e l'ordine pubblico,* Torino, 2014.

Perego B., *Predictive policing: trasparenza degli algoritmi, impatto sulla privacy e risvolti discriminatori,* in *BioLaw Journal Rivista di Biodiritto,* 2020.
Perry W.L., McInnis B., Price C.C., Smith S., Hollywood J.S., *Predictive policing: The Role of Crime Forecasting in Law Enforcement Operations,* in *RAND Corporation*, 2013.

Piergallini C., *Intelligenza artificiale: da "mezzo" ad "autore del reato",* in Rivista Italiana di Diritto e Procedura Penale, 2020.

Punzi A., *Diritto certezza e sicurezza,* G. Giappichelli editore – Torino, 2017.

Quattroloco S., *Intelligenza artificiale e giustizia: nella cornice della carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche,* in *La legislazione penale,* 2018.

Regione Campagna, *XLAW: L'algoritmo-poliziotto che prevede furti e rapine*, in *Smau Napoli,* 2018.

Sacchetto E., *Spunti di riflessione sul rapporto fra biometria e processo penale,* in *Diritto Penale Contemporaneo*, 2019.

Saetta B., *Profilazione e processi decisionali automatizzati,* in *Protezione dati personali*, 2018.

San Francisco Police Commission, *CompStat Policing in San Francisco,* in *SF.GOV.*

Seagate, *L'intelligenza artificiale migliora le attività operative della pubblica sicurezza nelle città smart,* in *SEAGATE*, 2020.

Severino P., *Intelligenza artificiale e diritto penale,* in *Intelligenza artificiale: il diritto, i diritti e l'etica,* a cura di Ruffolo U., *Giuffrè Francis Lefebvre*, Milano, 2020, p. 521-545.

Severino P., *Intelligenza artificiale. Politica, economia, diritto, tecnologia*, a cura di Severino P., *Luiss University Press*, Roma, 2022.

Signorelli A.D., *Il software italiano che ha cambiato il mondo della polizia predittiva*, in *wired*, 2019.

Signorelli A.D., *Quando l'algoritmo diventa sbirro: pro e contro della polizia predittiva,* in *vice*, 2016.

Silkie C., *Big Brother Watch defending civil liberties, protecting protecting privacy,* 2019.

SIMSI, *What is Risk Terrain Modeling?,* in *Simsi.com*, 2017.

Sindacato Autonomo di Polizia, *UNO SGUARDO AL FUTURO (SPERIAMO PROSSIMO) KEYCRIME,* in *sap-nazionale.org*, 2019.

Smith C., *The controversial crime-fighting program that changed big-city policing forever. Is Compstat's main legacy safe street – or stop and frisk?*, in *Intelligencer*, 2018.

Smolvico M., Amigoni F., Schiaffonati V., *Intelligenza artificiale,* in amigoni.faculty.polimi.it.

Tavella G., *Polizia predittiva e smart city: vecchie e nuove sfide per il diritto penale*, in *Fondazione Leonardo Civiltà delle Macchine Umanesimo Digitale*, 2021.

Thomas R., *La criminalistica e l'algoritmo XLAW che prevede i reati,* in *Polizia Penitenziaria.it*

Tonini P., *Manuale di procedura penale, G*iuffrè Francis Lefebvre, Milano, 2019.

Tulumello E., *Se prevedere il crimine discrimina, polizia predittiva, algoritmi che discriminano. La matematiche rimane neutrale?,* in *Monnalisa bytes*, 2020.

U.S. Department of Justice; Office of Justice Programs, *Transcript: Perspectives in Law Enforcement -The Concept of Predictive Policing: An Interview With Chief William Bratton,* in *U.S. Department of Justice,* 2009.

United States Department of Homeland Security, «*Fusion Center Locations and Contact Information*», 2022.

Vecchio A., *Xinjianf, Cina: sorveglianza e analisi predittiva si fanno con lo smartphone,* in *Difesa online*, 2019

Venturi M., *KeyCrime La chiave del crimine, I profili dell'abuso*, in *Giornale scientifico a cura dell'O.N.A.P. – Osservatorio Nazionale Abusi Psicologici*, 2014.

Viganò F., *Il principio di prevedibilità della decisione giudiziale in materia penale,* in Diritto *Penale Contemporaneo,* 2016.

Wacher S., Mittelstradt B., Floridi L., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation,* in *International Data Privacy Law, Oxford academic,* 2017.

Willis J.J.,Mastrofski S.D.,Weisburd D., *Compstat in Practice: An In-Depth Analysis of Three Cities,* in *National Policing Institute,* 2003.

Zara G., *Tra il probabile e il certo. La valutazione del rischio di violenza e di recidiva criminale,* in Diritto *Penale Contemporaneo,* 2016.

Zelikow P., Kojm C.A., Marcus D., *The 9/11 Commission Report*, in National Commission on Terrorist Attacks upon the United States, 2002.

Ziccardi G., Perri P., *Dizionario Legal tech*, Giuffrè Francis Lefebvre, 2020.

Zilordi A., *Intelligenza artificiale e processo penale tra norme, prassi e prospettive*, in *Questione di Giustizia*, 2019.