Predictive policing: criticità e prospettive dei sistemi di identificazione dei potenziali criminali

di Elisabetta Pietrocarlo

L'articolo analizza l'esperienza americana in materia di predictive policing, con particolare riguardo ai software che, attraverso un risk assessment individuale, identificano i potenziali autori di reati (person-based systems). Ricostruito il dibattito scientifico che si è sviluppato sul tema negli Stati Uniti, anche attraverso l'esame di alcuni tentativi di regolamentazione del fenomeno, sarà possibile tracciare un bilancio critico riguardo all'uso di tali strumenti, anche grazie al raffronto con alcune misure di prevenzione personali di competenza del questore previste nel nostro ordinamento. Ciò consentirà, dopo essersi altresì confrontati con i diversi atti rilevanti in tema di polizia predittiva emanati nello scenario eurounitario, di interrogarsi sulle prospettive e sulle condizioni di impiego di simili strumenti nel sistema penale italiano.

1. Premessa: inquadramento e origini della polizia predittiva.

Il dibattito scientifico sviluppatosi da alcuni anni attorno all'intelligenza artificiale e alle sue possibili applicazioni in campo penale ha portato all'attenzione degli studiosi continentali un fenomeno nuovo e già da tempo diffuso nell'ambito dei *police departments* americani: la c.d. *predictive policing*[1].

[1] V. tra gli studiosi americani FERGUSON, *The Rise of Big Data Policing. Surveillance, Race, and The Future of Law Enforcement*, New York, 2017; ID., *Policing Predictive Policing*, in *Washington Law Review*, 2017, vol. 94, no. 5, 1109; ID., *Illuminating Black Data Policing*, in *Ohio State Journal of Criminal Law*, 2018, 15, 503 ss.; JOH, *Artificial Intelligence and Policing: First Questions*, in *Seattle University Law Review*, 2018, 41, 1139 ss.; ID.,

Editore Associazione "Progetto giustizia penale" | via Festa del Perdono 7, 20122 Milano
c/o Università degli Studi di Milano, Dipartimento di Scienze Giuridiche "Cesare Beccaria"
redazione@sistemapenale.it

Tale termine si riferisce, in linea generale, all'impiego di tecniche analitiche – in particolare, quantitative – che, attraverso l'incrocio di dati, consentono di elaborare previsioni statistiche circa i luoghi di futura commissione di reati (c.d. *crime hot spot*) ovvero i potenziali autori o vittime, orientando le attività di polizia alla prevenzione, più che alla sola repressione del crimine[2]. L'obiettivo ultimo è dunque quello di una riduzione del tasso di criminalità, realizzata attraverso una più razionale allocazione delle risorse e interventi mirati sui soggetti a rischio[3]; il tutto reso possibile grazie all'analisi dei dati.

La cifra che contraddistingue la polizia predittiva è proprio il mutato paradigma alla base delle strategie di *crime management* che passano dall'essere informate da un approccio esclusivamente reattivo – le forze di polizia intervengono a fronte della notizia circa la realizzazione di un reato ai fini dell'individuazione del relativo autore – a uno di tipo proattivo, secondo cui l'intervento della polizia precede – e prescinde da(l) – l'attività criminale, al fine di prevenirla[4].

Come si diceva, la riflessione scientifica sulla *predictive policing* si è sviluppata a seguito dei progressi compiuti negli ultimi anni sul terreno dell'intelligenza artificiale[5]. L'implementazione del *machine learning* insieme all'avvento dei *big data*[6]

Feeding the Machine: Policing, Crime Data, & Algorithms, in *William & Mary Bill of Rights Journal*, 2017, 26, 287 ss.

[2] Nel tempo sono state elaborate diverse definizioni della *predictive policing* che sono riepilogate da MUGARI-OBIOHA, *Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing*, in *Social Sciences*, 2021, 3 s. V. altresì l'efficace definizione formulata da JOH, *Policing by Numbers: Big Data and the Fourth Amendment*, in *Washington Law Review*, 2014, vol. 89, 42, che considera la polizia predittiva come «the application of computer modeling to historical crime data to predict future criminal activity».

[3] PERRY-MCINNIS-PRICE-SMITH-HOLLYWOOD, *Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations*, Washington D.C., 2013, 30; BRANTINGHAM, *The Logic of Data Bias and Its Impact on Place-Based Predictive Policing*, in *Ohio State Journal of Criminal Law*, 2018, vol. 15, no. 2, 473.

[4] MUGARI-OBIOHA, *Predictive Policing and Crime Control*, cit., 1; FERGUSON, *Policing Predictive Policing*, cit., 1137, che evidenzia come la polizia americana abbia puntato l'attenzione sulla *predizione* come parte di un più ampio mutamento di strategia verso la *proactive policing*.

[5] V. BAGARIC-SVILAR-BULL-HUNTER-STOBBS, *The Solution to the Pervasive Bias and Discrimination in the Criminal Justice System: Transparent and Fair Artificial Intelligence*, in *American Criminal Law Review*, 2022, vol. 59, 108 che sottolineano la capacità dell'intelligenza artificiale «to greatly increase the effectiveness of proactive, or predictive, policing». Occorre tuttavia specificare che se è vero che tutti i sistemi di intelligenza artificiale si basano su algoritmi, non tutti gli algoritmi sfruttano l'intelligenza artificiale: esistono infatti sistemi di polizia predittiva che non si avvalgono di algoritmi ad apprendimento automatico ma di meri *rule-based algorithms*, i quali rimangono ancorati (o, potremmo dire, 'costretti') alle istruzioni dell'essere umano.

[6] Secondo PARLAMENTO EUROPEO, *Report on Fundamental Rights Implications of Big Data: Privacy, Data Protection, Non-Discrimination, Security and Law-Enforcement*, 20 febbraio 2017 (https://www.europarl.europa.eu/doceo/document/A-8-2017-0044_EN.html#_section3), «big data refers to the collection, analysis and the recurring accumulation of large amounts of data, including personal data, from a variety of sources, which are subject to automatic processing by computer algorithms and advanced data-processing techniques using both stored and streamed data in order to generate certain correlations, trends and patterns (big data analytics)». Per un inquadramento del fenomeno v., tra i molti autori italiani, DI PORTO, *La rivoluzione* big data. *Un'introduzione*, in *Concorrenza e mercato*, 2016, 5 ss.;

hanno fornito nuova linfa alle potenzialità degli strumenti in questione, i quali possono oggi avvalersi di algoritmi dalle straordinarie capacità di calcolo nonché di un patrimonio informativo di provenienza eterogenea (come banche dati delle forze dell'ordine o acquisite da *databrokers*, i *social networks*, Internet, gli impianti a circuito chiuso)[7] e di dimensioni davvero rilevanti – tale da non poter essere analizzato dalla mente umana[8].

Tuttavia, come è stato osservato, le origini della *predictive policing* risalgono indietro nel tempo e, segnatamente, all'inizio degli anni Novanta allorché fece ingresso nei *police departments* americani la prima *data-driven technologies* per l'analisi statistica dei reati, oggetto poi di ulteriore sviluppo[9]. La ragione della capillare diffusione di simili tecniche analitiche[10] va individuata nella esigenza sempre più avvertita di ricorrere a metodi di valutazione obiettivi, verificabili e, dunque, maggiormente affidabili della sola *human intuition*[11]. L'elemento qualificante di questo nuovo approccio risiederebbe[12] altresì nel rendere le scelte degli agenti di polizia trasparenti e controllabili, contrastando pratiche discriminatorie intenzionali o, comunque, attenuando i pregiudizi inconsci che, almeno in quei sistemi, sovente si annidano nel loro operato[13]. Ciò, peraltro, ha favorito un atteggiamento di –

OTTOLIA, Big Data *e innovazione computazionale*, Torino, 2018; ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *MediaLaws*, 2/2018, 32 ss.

[7] Non a caso le strategie di polizia predittiva sono definite come «the use of data and analytics to predict crime»: v. SELBST, *Disparate Impact in Big Data Policing*, in *Georgia Law Review*, 2017, vol. 52, 114; v. inoltre HUNG-YEN, *On the Person-Based Predictive Policing of AI*, in *Ethics and Information Technology*, 2021, 23, 165 ove si rileva che, mentre l'uso della statistica nelle attività di *law enforcement* non è una novità, sono le nuove tecnologie che sfruttano i *big data* ad aver avviato un cambiamento dei connotati di tali attività.

[8] Mettono in evidenza tali aspetti EGBERT-LEESE, *Criminal Futures. Predictive policing and Everyday Police Work*, Oxon-New York, 2021, 20 s.

[9] Il riferimento è alla creazione, da parte del commissario di polizia William Bratton, di *CompStat* (*computer statistics*): al riguardo, anche per una ricostruzione delle origini della polizia predittiva, JOH, *Policing by Numbers*, cit., 43 s.; EGBERT-LEESE, *Criminal Futures*, cit., 25; FERGUSON, *The Rise of Big Data Policing*, cit., 29.

[10] Lo stesso può dirsi con riferimento all'impiego di *risk assessment tools* nella fase cautelare per calcolare il rischio che l'imputato sia nuovamente arrestato prima del processo ovvero ometta di comparire, nonché in sede di commisurazione della pena per la valutazione del tasso di recidiva. Sul tema, v. per tutti QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Cham, 2020, 131 ss.

[11] Si intende la valutazione rimessa alla discrezionalità del singolo agente.

[12] SELBST, *Disparate Impact in Big Data Policing*, cit., 120. L'uso del condizionale è d'obbligo in quanto, a dispetto delle intenzioni, una delle principali critiche riscontrate nella prassi riguarda proprio la potenzialità discriminatoria degli strumenti in questione (v. *infra* § 3). Lo stesso Autore rileva criticamente come «at the moment, such a promise amounts to little more than a useful sales tactic». In senso analogo, v. ISAAC, *Hope, Hype, and Fear: The Promise and Potential Pitfalls of Artificial Intelligence in Criminal Justice*, in *Ohio State Journal of Criminal Law*, 2018, vol. 15, 543 s.

[13] Invero, di fatto, il crescente ricorso alle prime tecnologie basate sull'analisi dei dati nonché, più di recente, a quelle maggiormente avanzate è originato proprio dalla necessità di far fronte a circostanze ambientali negative di varia natura, quali l'emersione, in alcuni dipartimenti di polizia, di fenomeni corruttivi e situazioni di conflitto con la comunità locale, sfociate spesso in proteste e aspri scontri. È noto, infatti, come nell'intero territorio americano si siano sviluppate, a partire dalla metà dello scorso

quantomeno iniziale – accettazione implicita e di fiducia rispetto all'impiego di simili strumenti[14] che, rispetto allo stato delle cose, erano visti come una valida opportunità di cambiamento.

L'obiettivo del presente lavoro è innanzi tutto quello di illustrare le modalità di funzionamento e le caratteristiche dei *software* in questione, esaminando l'esperienza statunitense, 'terra madre' della *predictive policing* e soffermandosi su quelle registratesi di recente in Italia.

Concentreremo poi la nostra attenzione sulle criticità, segnalate dalla prassi americana, proprie dei sistemi fondati su *risk assessment* individuali. Sono questi ultimi a presentare i più spiccati profili di problematicità sia perché conducono alla identificazione di determinati individui sia, in primo luogo, per i riflessi che la valutazione prognostica sulla pericolosità determina sul piano del trattamento sanzionatorio[15].

Chiuderemo con l'analisi critica dell'intenso dibattito scientifico americano, culminato con isolati tentativi di disciplina del fenomeno, per poi volgere lo sguardo all'oramai frastagliato orizzonte normativo eurounitario[16].

Confidiamo così di disporre delle coordinate per interrogarci sulle future prospettive di regolazione della *predictive policing*, alla ricerca delle relative condizioni di compatibilità con i principi della materia penale e con i diritti fondamentali dell'individuo.

---

decennio, serrate proteste contro la polizia a fronte dell'uccisione di diverse persone di colore, animando così il dibattito sulla necessità di una complessiva riforma del sistema, al fine di sradicare le pratiche discriminatorie perpetrate nei confronti degli afroamericani e, al contempo, di placare il sentimento ostile dei cittadini verso le forze dell'ordine. Per una ricognizione dell'ampio dibattito al riguardo, v. FERGUSON, *The Rise of Big Data Policing*, cit., 21 ss.; v. altresì CASTETS-RENARD, *Human Rights and Algorithmic Impact Assessment for Predictive Policing*, in MICKLITZ-POLLICINO-REICHMAN-SIMONCINI-SARTOR-DE GREGORIO (a cura di), *Constitutional Challenges in the Algorithmic Society*, Cambridge, 2022, 95.

[14] FERGUSON, *Surveillance and the Tyrant Test*, in *The Georgetown Law Journal*, 2021, vol. 110, no. 2, 214 ss.

[15] Da qui si giustifica, a nostro avviso, l'interesse, anche degli studiosi del diritto penale, per la polizia predittiva, sebbene si collochi in un terreno antistante a quello della giustizia penale in senso stretto, ovverosia nelle strategie di prevenzione della criminalità. Invero, la maggior parte degli studi su intelligenza artificiale e sistema penale ricomprende tra i campi di indagine la polizia predittiva: cfr., tra gli altri che saranno citati nel prosieguo, SEVERINO, *Le implicazioni dell'intelligenza artificiale nel campo del diritto con particolare riferimento al diritto penale*, in SEVERINO (a cura di), *Intelligenza artificiale. Politica, economia, diritto, tecnologia*, Roma, 2022, 92 ss.; ID., *Intelligenza artificiale e diritto penale*, in RUFFOLO (a cura di), *Intelligenza artificiale: il diritto, i diritti, l'etica*, cit., 536 ss.; MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in *Discrimen*, 15 febbraio 2020, 6 s.; BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Dir. pen. uomo*, 29 settembre 2019, 8 ss.; CONTISSA-LASAGNI-SARTOR, *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Dir. Internet*, 2019, 4, 620 ss. *Contra* QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings*, cit., 40, secondo cui la polizia predittiva è radicata nella criminologia e nella sociologia, piuttosto che nel diritto penale.

[16] Questa parte dell'indagine sarà alimentata anche dall'analisi di documenti emanati da importanti istituzioni sul versante eurounitario, della normativa in tema di *data protection* nonché della proposta di Regolamento sull'intelligenza artificiale adottata dalla Commissione europea nell'aprile 2021 (ora in fase di approvazione).

Iniziamo dunque a introdurre il lettore nell'universo degli strumenti di polizia predittiva, analizzandone tipologia e modalità di funzionamento.

2. Tassonomia e funzionamento dei *software*: dai *place-based systems*…

Il termine *predictive policing* si presta a ricomprendere diverse tipologie di *software* che, al netto delle rispettive peculiarità, seguono il medesimo processo, articolato in tre fasi: 1) l'inserimento di dati (di una o più tipologie) nel sistema; 2) l'analisi dei dati inseriti attraverso un metodo algoritmico al fine di elaborare la specifica previsione cui il sistema è finalizzato; 3) l'uso di tale previsione da parte degli agenti di polizia per informare le decisioni strategiche e tattiche sul campo.

Molteplici sono però le varianti delle possibili applicazioni concrete a seconda del tipo di dati utilizzati ovvero della tecnica algoritmica che si intende impiegare, nonché – soprattutto – del tipo di 'predizione' che si vuole ottenere.

Sotto quest'ultimo profilo si è soliti distinguere[17] tra sistemi *place-based* e *person-based*: i primi elaborano una predizione basata sulla individuazione delle aree urbane (*crime hot spot*) ove saranno commessi reati, mentre i secondi forniscono una previsione di rischio individuale, identificando coloro che potrebbero commettere reati ovvero diventarne vittime. In quest'ultimo ambito, viene poi da taluni individuato un sottogruppo di *software* denominati *suspect-based*[18], i quali delineano il

---

[17] Segnaliamo che, alla luce della eterogeneità delle applicazioni di *predictive policing* esistenti, nella letteratura sull'argomento sono state proposte diverse e più specifiche tassonomie, che, a ben vedere, non sono poi così distanti tra loro, dal momento che le categorie di *tools* si rivelano tutto sommato corrispondenti nella sostanza. Pertanto, le applicazioni della polizia predittiva possono essere principalmente distinte a seconda che abbiano riguardo al *luogo* ovvero all'*individuo*. Per una panoramica generale, v. MUGARI-OBIOHA, *Predictive Policing and Crime Control*, cit., 5 s. Per una ripartizione basata sul tipo di previsione fornita dall'algoritmo, v. PERRY-MCINNIS-PRICE-SMITH-HOLLYWOOD, *Predictive Policing*, cit., 36: 1) *methods for predicting crimes*, volti cioè a individuare i luoghi e gli orari a maggiore rischio di criminalità; 2) *methods for predicting offenders*, che identificano i potenziali criminali attraverso un *risk assessment* individuale; 3) *methods for predicting perpetrators' identities*, ossia tecniche di profilazione che abbinano i probabili autori di reato con specifici crimini passati; 4) *methods for predicting victims of crimes*, i quali identificano i gruppi o gli individui vittime di reato. V. altresì BACHNER, *Predictive Policing: Preventing Crime with Data and Analytics*, Washington DC, 2013, 86 ss. per una suddivisione basata sull'oggetto dell'analisi: i) *space analysis*; ii) *time and space analysis*; iii) *social network analysis*. Quanto alle prime due classi, si specifica che l'analisi dello spazio è più mirata all'identificazione degli *hot spots*, mentre quella degli orari è incentrata sull'individuazione dei luoghi in cui è probabile che si verifichino reati sulla base dei precedenti episodi di criminalità; può però concludersi che entrambe le categorie abbiano riguardo principalmente al luogo. La categoria sub *iii)* è invece volta all'analisi delle reti relazionali per identificare soggetti a rischio. V. ancora la autorevole classificazione di FERGUSON, *Policing Predictive Policing*, cit., *passim*., che rispecchia il percorso evolutivo dei sistemi in questione e si articola in tre diverse categorie, basandosi sul *target*: a) *Predictive Policing 1.0* (*targeting places of property crime*); b) *Predictive Policing 2.0* (*targeting places of violent crime*); c) *Predictive Policing 3.0* (ta*rgeting persons involved in criminal activity*). I primi due gruppi sono orientati all'individuazione di luoghi sospetti, variando solo per il tipo di reato in rilievo, mentre l'ultimo si focalizza sull'identificazione di soggetti coinvolti in attività criminale, senza distinguere a seconda che si tratti di autori o vittime di reati.

[18] Questa ulteriore specificazione è ripresa da SELBST, *Disparate Impact in Big Data Policing*, cit., 139 s.

profilo del possibile autore di un determinato reato o, più spesso, di una serialità criminale.

Iniziamo con l'esaminare i *place-based systems*, gli strumenti utilizzati per primi e tuttora più diffusi.

Il loro scopo è di identificare le aree geografiche nelle quali, in un determinato arco temporale, è altamente probabile che si verifichino reati, così da impiegare le forze dell'ordine nelle aree suddette a fini preventivi ovvero per arrestare in flagranza l'autore del reato[19] – sul presupposto che una maggiore presenza della polizia nelle aree a rischio dissuada gli autori dal commettere reati[20].

L'idea di fondo alla base dell'implementazione degli strumenti *place-based* è che alcune tipologie di reati tendono ad avere un effetto domino nelle aree limitrofe e, dunque, a essere seguiti da altrettanti reati della stessa specie[21]; ciò in quanto, alternativamente, lo stesso autore torna nel medesimo luogo in cui ha realizzato una condotta criminosa per commettere nuovi reati ovvero sussistono condizioni ambientali che alimentano la criminalità (come l'assenza di forze di polizia nell'area di riferimento). Si tratta del c.d. *near repeat effect* che ad oggi ispira larga parte dei sistemi di *predictive policing* di cui ci stiamo occupando e che, oltre ad avere trovato conferma sul piano empirico con particolare riferimento ai *property crime*, ha un suo fondamento teorico nelle *theories* della *rational choice* e della *routine activity*[22].

La prima si basa sull'assunto che i criminali agiscano in modo intrinsecamente razionale. In sostanza, un ladro professionista, immaginato come un *optimal forager* che esplora attentamente un quartiere per identificare obiettivi di interesse e valutare potenziali pericoli, è probabile si attenga a una formula d'azione, rivelatasi di successo, già collaudata e commetta altri reati nel medesimo contesto ambientale e a una distanza di tempo ravvicinata, così da massimizzare il patrimonio conoscitivo acquisito e minimizzare i rischi[23].

Secondo la teoria della *routine activity*[24], invece, la realizzazione di un reato sarebbe riconducibile, nonché facilitata, da una serie di fattori, tra cui la presenza di un autore motivato, la disponibilità di un 'bersaglio adatto' e l'assenza di adeguate misure di protezione a sua tutela. Ben si comprende allora come l'idea di rafforzare i controlli di polizia in un determinato luogo e in un certo orario possa effettivamente avere un effetto deterrente.

Su queste basi, alcuni ricercatori dell'UCLA hanno iniziato a interrogarsi sulla possibilità di prevedere la realizzazione di alcuni *property crime* – *burglary*, *automobile theft* e *theft from automobiles*[25] – attraverso il ricorso a un algoritmo originariamente

---

[19] FERGUSON, *The Rise of Big Data Policing*, cit., 63; EGBERT-LEESE, *Criminal Futures*, cit., 31.

[20] FERGUSON, *Predictive Policing Theory*, in *Washington College of Law Research Paper*, 10/2020, 494.

[21] FERGUSON, *Policing Predictive Policing*, cit., 1128.

[22] FERGUSON, *Policing Predictive Policing*, cit., 1128 s.

[23] EGBERT-LEESE, *Criminal Futures*, cit., 31.

[24] FERGUSON, *Policing Predictive Policing*, cit., 1129.

[25] Si tratta, rispettivamente, di furto con scasso, furto d'auto e furto di oggetti dall'automobile.

sviluppato per misurare le scosse sismiche di assestamento dei terremoti. All'esito dello studio, si è pervenuti alla conclusione che i due fenomeni – terremoti, da un lato, e criminalità, dall'altro – seguono schemi simili. Questi i termini del parallelismo: al pari del sisma, la verificazione di un reato in un determinato luogo (epicentro) viene generalmente seguita da ulteriori eventi criminosi nelle zone contigue (potremmo dire, da scosse di assestamento); e la spiegazione di una simile propagazione può essere fatta risalire alle teorie sopra richiamate.

Così, si è dato vita a un progetto con il dipartimento di polizia di Los Angeles che ha condotto alla nascita di *PredPol*[26], un algoritmo predittivo basato sul *near repeat effect* e operante attraverso un processo articolato in due fasi. In primo luogo, si analizzano i dati relativi ai reati realizzati in passato – con riferimento a tre variabili: tipologia, ora e luogo di commissione – per identificare *patterns* (cioè corrispondenze) tra i precedenti comportamenti criminali. In una seconda fase, il sistema individua le probabili zone di attività criminale, ciascuna di una grandezza pari a 500 metri quadrati per 500, sulla base del verificarsi di criteri 'scatenanti'. Il tutto viene poi messo a disposizione degli agenti di polizia sul territorio attraverso mappe in formato digitale, in cui le aree evidenziate corrispondono a quelle verso cui indirizzare le attività di *patrolling*[27].

Come detto, questa primaria versione di *predictive policing* è confinata – non a caso – all'elaborazione di previsioni relative a specifiche tipologie di *property crime*.

La ragione è legata alla loro relativa diffusione, e dunque all'allarme sociale generato, alla propensione alla denuncia e al loro legame con condizioni 'ambientali' che ben possono essere affrontate attraverso una presenza mirata delle forze di polizia[28].

Le statistiche sull'effettivo impatto dei primi esemplari di polizia predittiva sulla riduzione del tasso di criminalità sono discordanti[29] e non pienamente attendibili, in quanto perlopiù provenienti dalle stesse aziende produttrici. Peraltro, uno dei pochi studi indipendenti non ha registrato miglioramenti statisticamente significativi nella riduzione della criminalità rispetto ai distretti che impiegavano le

---

[26] Oggi il *software* ha preso il nome di 'Geolitica'; per ulteriori riferimenti in merito a *PredPol* si rinvia a FERGUSON, *Predictive Policing Theory*, cit., 494 ss.; BRANTINGHAM, *The Logic of Data Bias*, cit., 473 ss.

[27] FERGUSON, *Predictive Policing Theory*, cit., 494, che osserva come *PredPol* si atteggi ad autentico *patrol management system*.

[28] V. su questi aspetti richiamati FERGUSON, *Policing Predictive Policing*, cit., 1126 s.

[29] Secondo le rilevazioni risalenti ai primi sei mesi di utilizzo di *PredPol* nella città di Los Angeles, si è assistito un calo del 25% dei furti con scasso. A Santa Cruz (California), i *property crime* sono diminuiti tra il 4% e l'11%, mentre ad Alhambra (California), dopo un anno di utilizzo della tecnologia, i furti nelle automobili sono diminuiti del 21% e i furti di auto dell'8%. Risultati simili si sono registrati anche in Pennsylvania nelle città di Seattle, Atlanta, e Reading. Tuttavia, è stato osservato che il campione è in realtà imperfetto, poiché all'epoca si era registrata una generale diminuzione del tasso di criminalità nell'intero Paese. Peraltro, secondo studi successivi, alcune città, tra cui Los Angeles, hanno mostrato un'impennata della criminalità dopo le diminuzioni iniziali, v. sul punto FERGUSON, *Policing Predictive Policing*, cit., 1130.

tecniche convenzionali di mappatura degli *hot spots*[30]. Ciononostante, il fenomeno ha avuto inizialmente una vasta diffusione.

Una prima evoluzione dei *place-based systems* ha riguardato l'estensione delle tipologie di reati oggetto della predizione algoritmica, estesi ai *violent crime*[31] (conflitti a fuoco, episodi di violenza connessa alla attività delle *gang*, etc.).

Al contempo, è stata sviluppata una nuova tecnica di analisi alla base del funzionamento dei *software* di *predictive policing*, non più fondata sul *near repeat effect*. Il riferimento è al *Risk Terrain Modeling* (RTM)[32], elaborato dai ricercatori del *Rutgers Center for Public Security* e utilizzato con successo in relazione ad alcuni crimini violenti. Esso si caratterizza per il fatto di ricercare gli *environmental crime drivers*, cioè quei fattori, quelle vulnerabilità ambientali che incentivano la commissione di reati in determinate aree urbane[33]. In altri termini, il modello RTM considera la realtà fisica di una città come un terreno di rischi interconnessi: se pertanto, in una determinata zona, il sistema registra la presenza di più *risk factors*, ciò sarà indicativo di una significativa probabilità di verificazione di reati in tale area. In questa prospettiva, le organizzazioni di polizia dovrebbero essere ripensate come 'agenzie di gestione del rischio'[34] che analizzano, valutano e pongono rimedio alle menzionate vulnerabilità ambientali.

La differenza rispetto alle applicazioni di polizia predittiva prima esaminate risiede nel fatto che il modello non deve essere limitato a *dataset* predefiniti (come, ad esempio, i dati storici sui reati a disposizione della polizia), potendo includere quasi tutte le fonti di dati ipotizzabili, purché logicamente collegate al verificarsi di un reato[35]; naturalmente, a una più ampia varietà di dati considerati corrisponderà una maggiore accuratezza dell'analisi.

In questo caso le statistiche[36] sembrano dare ragione all'impiego di questo modello, atteso che, nei territori delle diverse città che lo hanno adottato, si è registrata una riduzione significativa del tasso di criminalità non solo a breve ma anche a lungo termine.

---

[30] V. lo studio condotto nel 2014 da HUNT-HOLLYWOOD-SAUNDERS, *Evaluation of the Shreveport Predictive Policing Experiment* e finanziato dalla RAND Corporation.

[31] FERGUSON, *Policing Predictive Policing*, cit., 1132.

[32] V. per tutti CAPLAN-KENNEDY, *Risk Terrain Modeling: Crime Prediction and Risk Reduction*, Oakland, 2016. Ulteriori informazioni sono reperibili sul sito ufficiale (www.riskterrainmodeling.com).

[33] In questa logica, ad esempio, le grandi folle che si radunano in determinati luoghi rappresenterebbero un maggior rischio di borseggio, mentre il traffico congestionato nelle ore di punta renderebbe più difficile una rapida fuga, indicando un minore rischio di furto. Al riguardo, v. FERGUSON, *Predictive Policing Theory*, cit., 500.

[34] CAPLAN-KENNEDY, *Risk Management and RTM in ACTION*, 2014 (http://www.riskterrainmodeling.com/uploads/2/6/2/0/26205659/actionplan.pdf).

[35] In questo senso, v. EGBERT-LEESE, *Criminal Futures*, cit., 34: «Data could, for example, refer to the infrastructural characteristics and socio-economic compositions of specific areas, including the likes of income distribution, household size, building stock, highways, metro stations, or nightlife spots».

[36] V. la ricerca condotta da PIZA, *A Multi-jurisdictional Test of Risk Terrain Modeling and a Place-based Evaluation of Environmental Risk-Based Patrol Deployment Strategies*, in www.rutgerscps.org, 2015.

Non resta infine che soffermarsi su quella che potrebbe essere definita l'ultima frontiera[37], ovverosia i sistemi che, in definitiva, combinano i modelli di funzionamento sinora illustrati, considerando, ai fini della predizione, una molteplicità di aspetti quali: «baseline crime rates, near repeat patterns, routine activities theory, socioeconomic factors, seasons, time of month, day of week, time, holidays, sporting events, weather, and other RTM-like factors»[38].

Un esempio è *HunchLab*, sviluppato dalla società Azavea, che utilizza un algoritmo basato su tecniche di *machine learning*, il quale apprende autonomamente sulla base dei dati che elabora, consentendo così al *software* «to 'think' like a crime analyst by imitating years of experience drawn from a police department's own data»[39]. In particolare, il sistema analizza dapprima i dati storici relativi ai reati e successivamente aggiunge le altre tipologie di *non-crime datasets* legati a fattori sociali, economici o addirittura metereologici. All'esito di tale processo, il *tool* fornisce non solo una previsione delle aree urbane più a rischio, ma suggerisce altresì alle forze dell'ordine tattiche mirate per gestire tali rischi[40].

Quanto alla sua incidenza sulla riduzione del tasso di criminalità, sono stati registrati miglioramenti sia nella città di Chicago (Illinois) sia in quella di Philadelphia (Pennsylvania)[41], sebbene non siano mai stati pubblicati risultati ufficiali.

In questo ambito sembra da collocare il *software X-Law*[42], sviluppato da un (al tempo) ispettore della questura di Napoli, sebbene non arrivi a indicare vere e proprie strategie di intervento agli agenti. Basandosi su un algoritmo ad apprendimento automatico, *X-Law* conduce un'analisi non solo dei dati relativi allo storico dei reati predatori urbani (cioè furti, rapine, etc.) ma anche dei fattori socio-economici, demografici, di eventuali eventi o manifestazioni sportive in programma, al fine di

---

[37] MUGARI-OBIOHA, *Predictive Policing and Crime Control*, cit., 6 definiscono *HunchLab* come il *software* di polizia predittiva probabilmente più complicato mentre EGBERT-LEESE, *Criminal Futures*, cit., 34 come un «cutting-edge method for crime prediction».

[38] FERGUSON, *Policing Predictive Policing*, cit., 1136.

[39] AZAVEA, *HunchLab: Under the Hood*, 2015, 16, consultabile su http://blog.pilpul.me/files/2015/09/HunchLab-Under-the-Hood.pdf.

[40] FERGUSON, *Predictive Policing Theory*, cit., 496 specifica che queste tattiche riguardano il modo in cui un agente di polizia dovrebbe interagire con chi lo circonda per combattere un particolare *crime risk*. Ad esempio, prediligere la conversazione piuttosto che arresti, perquisizioni o altre strategie di tipo deterrente.

[41] V. le fonti richiamate da FERGUSON, *Predictive Policing Theory*, cit., 497: FINGAS, *Chicago police see less violent crime after using predictive code. The data suggests technology really does help*, in *Engadget*, 8 agosto 2017; REYES, *Philly Police will be first big city cops to use Azavea's crime predicting software*, in *Technically Media Inc.*, 7 novembre 2013.

[42] Il *software* è stato peraltro brevettato nell'ottobre 2022. Per maggiori dettagli sul suo funzionamento, v. in dottrina ALGERI, *Intelligenza artificiale e polizia predittiva*, in *Dir. pen. proc.*, 2021, 731; BASILE, *Intelligenza artificiale e diritto penale*, cit., 12. Secondo le dichiarazioni dell'ispettore Elia Lombardo (ideatore di *X-Law*) il 29 dicembre 2018 nel corso di un'intervista televisiva, il sistema contribuito ad abbattere il tasso di criminalità, assestandosi su una percentuale del -22% nella città di Napoli e del -39% in quella di Prato.

selezionare – mediante raffigurazione in una mappa digitale a disposizione degli agenti – le aree a più alto rischio di commissione dei reati in determinati orari.

2.1. …ai person-based systems.

I sistemi di maggiore interesse ai nostri fini sono però quelli orientati verso l'identificazione dei *soggetti* coinvolti in attività criminale[43]. Essi si basano sull'idea secondo cui soltanto una piccola quota della popolazione è responsabile di episodi di violenza, sicché l'individuazione di tali soggetti e il conseguente intervento mirato nei loro confronti si rivelano essenziali per ridurre il tasso di criminalità (c.d. *focused deterrence*)[44]. Ciò comporta la compilazione di elenchi di persone ritenute 'a rischio' nonché una *social network analysis* (elementi che nella prassi risultano spesso combinati).

Si procede anzitutto alla predisposizione di liste contenenti le generalità di soggetti che, secondo la polizia, commetteranno crimini in futuro o che sono coinvolti in attività criminali in corso, ma non sono ancora stati arrestati[45]. Sistemi di questo tipo possono, a seconda dei casi, basarsi su questionari, utilizzare modelli di valutazione clinico-psichiatrica o analizzare dati aggregati; non è peraltro infrequente nella prassi l'utilizzo congiunto di più tecniche.

Nell'ambito invece della *social network analysis*, si cerca di desumere la pericolosità in base alla rete sociale del soggetto in questione, sul presupposto che il collegamento con parenti, amicizie, frequentazioni abituali, colleghi, etc. che siano stati in passato autori o anche vittime dei reati di cui si tratta rappresenti un incentivo alla commissione futura di analoghi fatti criminosi[46], sulla falsariga di quanto avviene per le vulnerabilità ambientali di cui si è detto in precedenza[47].

Un discorso separato meritano invece quei sistemi, per la verità meno diffusi negli Stati Uniti, che elaborano il profilo dell'autore di una serialità criminale. I *suspect-based systems* sono stati classificati, come si anticipava, da alcuni studiosi statunitensi come una sottocategoria di quelli *person-based*[48]; tuttavia, essi non utilizzano le tecniche appena menzionate e, quindi, non danno luogo a un *risk assessment* individuale. Si tratta piuttosto di *software* che, sulla base di un'analisi dei

---

[43] V. al riguardo HUNG-YEN, *On the Person-Based Predictive Policing*, cit., 165 che definiscono la tipologia di *software* in questione come la «most controversial, as it singles out individual names and faces».

[44] In argomento, v. FERGUSON, *The Rise of Big Data Policing*, cit., 35 ss.

[45] TUCEK, *Constraining Big Brother: The Legal Deficiencies Surrounding Chicago's Use of the Strategic Subject List*, in *The University of Chicago Legal Forum*, 2018, 430.

[46] EGBERT-LEESE, *Criminal Futures*, cit., 29; FERGUSON, *Policing Predictive Policing*, cit., 1137 s., che rileva come l'esperienza maturata rispetto alle reti terroristiche internazionali insegni che la mappatura di associazioni, connessioni di ogni genere, etc. consenta di identificare importanti *patterns* nella criminalità. Ciò peraltro è assai agevole nella prassi grazie a Internet e ai *social media*.

[47] V. *supra* § 2.

[48] SELBST, *Disparate Impact in Big Data Policing*, cit., 139.

dati relativi a reati passati di carattere seriale (come, ad esempio, le rapine), tentano di individuare *patterns*, cioè corrispondenze sulla cui base individuare un *crime linking* e delineare il profilo – anonimo – del possibile autore. Questa fase 'diagnostica' – che, già di per sé, può essere utile ai fini della risoluzione di crimini già consumati – è altresì funzionale a quella propriamente 'predittiva', nel senso che, in virtù delle risultanze ottenute, è possibile prevedere la realizzazione, da parte dello stesso soggetto, di reati futuri.

Un virtuoso esempio di questo approccio è riscontrabile nell'esperienza italiana. Ci riferiamo al *software KeyCrime*[49], ideato da un esponente della Questura di Milano e poi ulteriormente sviluppato grazie all'impiego dell'intelligenza artificiale e del *machine learning*, che si basa proprio sull'analisi di tutte le informazioni, anche le più dettagliate, ricavabili dai reati seriali già realizzati – circostanze di luogo e di tempo, abbigliamento e gestualità del colpevole, testimonianze dei presenti, etc. – per rilevare elementi in grado di tracciare un 'profilo' del *perpetrator* e di predire le sue successive mosse.

[49] Informazioni sul *modus operandi* di *KeyCrime* – oggi di proprietà di una società privata di cui è presidente l'ex ispettore Mario Venturi, suo ideatore originario – sono disponibili sul relativo sito, v. https://keycrime.com/. In dottrina, v. ALGERI, *Intelligenza artificiale e polizia predittiva*, cit., 731 s.; BASILE, *Intelligenza artificiale e diritto penale*, cit., 12; BONFANTI, Big data *e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in *MediaLaws*, 3/2018, 3; PADUA, *Intelligenza artificiale e giudizio penale: scenari, limiti e prospettive*, in *Processo penale e giustizia*, 2021, 1492; PARODI-SELLAROLI, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Dir. pen. cont. – Fasc.*, 6/2019, 56 s. Peraltro, proprio sulla base di questo *tool*, il Dipartimento di Pubblica Sicurezza del Ministero dell'Interno ha dato vita al progetto *Giove*, un sistema di elaborazione e analisi automatizzata, che segue il medesimo *modus operandi*. Nell'attesa che la polizia predisponga il 'documento di valutazione dell'impatto', da sottoporre al Garante della privacy, è stata presentata una interrogazione parlamentare con la richiesta di chiarire diverse questioni preliminari all'eventuale messa in uso del sistema, anche alla luce del dibattito che si sta sviluppando in sede eurounitaria. V. l'estratto del resoconto della seduta del Senato del 13 giugno 2023 (https://www.senato.it/japp/bgt/showdoc/frame.jsp?tipodoc=Sindisp&leg=19&id=1378767), ove si chiede di chiarire: «a) quali interventi intenda mettere in atto per introdurre il sistema Giove in Italia, se esistano altri *software* di questo tipo già in uso o dei quali si prospetta l'utilizzo; b) quali aziende siano state coinvolte nella definizione di questa tecnologia, della sua implementazione e del suo sviluppo; c) quale sia lo stato dell'arte della interlocuzione con il Garante per la protezione dei dati personali in ordine a una valutazione di impatto che l'introduzione di questo sistema comporterebbe; c) quale tipo di dati e quali *batch* si intenda utilizzare per andare a comporre la memoria operativa del sistema; d) che livello di individuazione sia possibile e ottenibile senza violare la privacy dei soggetti; e) quali siano gli effetti anche sull'urbanistica delle città alla prova di una capacità così penetrante e intrusiva di profilazione delle persone e dei comportamenti, alla luce di un dibattito europeo ed internazionale molto negativo verso l'utilizzo di simili tecnologie così invasive e lesive dei diritti delle persone e nelle more di una decisione europea che regolerà in maniera cogente il suddetto utilizzo, vietando esplicitamente la possibilità di una "polizia predittiva"».

2.1.1. L'esperienza di alcuni *police departments* americani e l'attuale stato dell'arte.

Una interessante applicazione di *person-based predictive policing* volta a individuare i potenziali autori di reati è stata implementata a Kansas City (Missouri)[50] nell'ambito della *Smart Policing Initiative* (SPI), volta a incoraggiare i dipartimenti di polizia locale a utilizzare *data-driven tactics*. In particolare, il procedimento può essere schematizzato in quattro fasi: le prime tre di carattere analitico e l'ultima di stampo 'operativo'.

Si parte da un elenco di *target offenders* che include i sospettati di omicidi, conflitti a fuoco o altre gravi aggressioni; dopodiché – nel secondo segmento – vengono passati in rassegna tutti i contatti formali della polizia con ciascuno di tali soggetti al fine di intercettare i loro *associates* (si pensi, ad esempio, a coloro che sono stati arrestati o fermati con l'*initial offender*). Si procede poi a individuare i soggetti a loro volta collegati a questi ultimi.

Conclusa così la parte analitica del processo, il *team* ottiene un *social network* che comprende tre *layers of offenders*[51]: 1) *initial target offenders*, 2) *target offenders' associates*, 3) *associates of the target offenders' associates*. A questo punto, si passa alla fase, per così dire, 'operativa' in cui si prevede che la polizia contatti tali soggetti, informandoli che sono stati identificati «as a cause of violence in the city»[52].

Ma vi è di più. Gli agenti, da un lato, prospettano loro la possibilità di iniziare un percorso di 'reinserimento sociale' (*those who want help to change will receive it*), attraverso la partecipazione a programmi di *education*, *job training* ovvero di sostegno nel caso di soggetti affetti da dipendenze; dall'altro lato, gli *officers* effettuano una vera e propria diffida nei confronti dei *predicted offenders*, comunicando che, qualora dovessero tenere una condotta non conforme alla legge, saranno puniti. E nella prassi accade che, laddove commettano un reato, siano poi puniti di gran lunga più severamente in ragione dell'ammonimento ricevuto. Basti qui citare il caso, registratosi nel Western District del Missouri, dell'inflizione di una pena detentiva della durata di ben quindici anni a un soggetto sorpreso con un *bullet* nelle proprie tasche[53].

Un sistema analogo è stato adottato sin dal 2013 a Chicago (Illinois): si tratta della *Strategic Subject List* (SSL), meglio nota come *Heat List* e successivamente

---

[50] Ne parla approfonditamente FERGUSON, *Policing Predictive Policing*, cit., 1140 s.

[51] Il progetto iniziale di Kansas City ha condotto all'individuazione di un *social network* di centoventi persone.

[52] FERGUSON, *Policing Predictive Policing*, cit., 1141.

[53] FERGUSON, *Policing Predictive Policing*, cit., 1141, nota n. 198 nonché per un maggiore approfondimento ID., *Predictive Prosecution*, in *Wake Forest Law Review*, 2016, vol. 51, no. 3, 719. Segnaliamo che, secondo la legislazione vigente in Missouri, la fattispecie in parola ricade nel *class D felony* di *unlawful possession of a firearm*, il quale punisce un soggetto già resosi responsabile di un delitto (*felon*) con una pena fino a sette anni di reclusione e $10.000; tuttavia, laddove si tratti di una persona già condannata per un *dangerous felony*, il fatto integrerà un *class C felony*, punibile con la pena detentiva da tre a dieci anni e con la medesima pena pecuniaria prima indicata (v. https://revisor.mo.gov/main/OneSection.aspx?section=571.070).

denominata *Crime and Victimization Risk Model*, la quale rappresenta, secondo alcuni autori[54], il più importante esempio di *social network analysis*.

Il modello SSL[55] esamina gli individui con precedenti penali che sono classificati in base alla probabilità di essere coinvolti in episodi di violenza con armi da fuoco connessi alle *gang* o in un omicidio[56], sia come vittime che come autori di reati, noti come '*Party to Violence*' (PTV). A costoro viene quindi attribuito un *predictive threat score* (che varia da zero a cinquecento).

Il *software* viene generato sulla base di dati relativi al numero di precedenti arresti (in particolare, per *violent crimes* e *unlawful use of a weapon*), di passati coinvolgimenti come vittime in *shootings* o *aggravated battery or assault*[57] nonché riguardanti l'età di un individuo all'epoca dell'ultimo arresto, l'incremento nel tempo della sua attività criminale[58] e l'intensità della sua *criminal history*[59].

Si apre a questo punto una procedura analoga a quella in precedenza descritta, che si conclude con la notifica della *custom notification letter*[60]. Lo *Special Order S10-05* del dipartimento di polizia di Chicago, che delinea la relativa procedura, specifica che quando una persona identificata nella *Heat List* viene arrestata nuovamente, la polizia raccomanderà ai pubblici ministeri di elevare le contestazioni più severe, esorterà la *community advocacy*[61] a opporsi al rilascio su cauzione e si impegnerà in un coordinamento diretto con gli uffici dei pubblici ministeri statali. Merita subito di

---

[54] EGBERT-LEESE, *Criminal Futures*, cit., 29.

[55] Il funzionamento del sistema è descritto analiticamente da TUCEK, *Constraining Big Brother*, cit., 431 ss. Al riguardo, v. anche FERGUSON, *Policing Predictive Policing*, cit., 1138 ss.; EGBERT-LEESE, *Criminal Futures*, cit., 29 s.; MUGARI-OBIOHA, *Predictive Policing and Crime Control*, cit., 6.

[56] L'interesse verso queste forme di criminalità non è casuale. V. il *report* di BRAGA-WEBSTER-WHITE-SAIZOW, *SMART Approaches to Reducing Gun Violence. Smart Policing Initiative Spotlight on Evidence-Based Strategies and Impacts*, marzo 2014, 1 che, nell'illustrare i nuovi mezzi adottati da diversi dipartimenti di polizia, riporta alcuni dati allarmanti sui numeri degli omicidi connessi a episodi di *gun violence* (pari a undicimila) e sottolinea inoltre come simili fenomeni necessitino di essere contrastati anche per la generale sicurezza della collettività.

[57] Si tratterebbe, in sostanza, di reati di minacce e percosse aggravate.

[58] V. CHICAGO POLICE DEPARTMENT, *Special Order S10-05*, 6 ottobre 2015 (https://directives.crimeisdown.com/directives/data/a7a57bf0-1456faf9-bfa14-570a-a2deebf33c56ae59.html?commit=a148929d984a05241f3ed79d55af4f0a185063a3) che si riferisce testualmente a '*the degree to which his criminal activities are on the rise*', senza tuttavia fornire ulteriori informazioni sulle relative modalità di calcolo. Si è ipotizzato che si intenda fare riferimento al numero di arresti recenti, nel senso che lo *score* attribuito sarà più elevato rispetto all'ipotesi di episodi più risalenti (v. POSADAS, *How strategic is Chicago's "Strategic Subjects List"? Upturn investigates*, in *Medium*, 22 giugno 2017).

[59] V. nel dettaglio CHICAGO POLICE DEPARTMENT, *Special Order S10-05*, cit.

[60] Questa lettera descrive nel dettaglio i precedenti contatti dell'individuo con la 'giustizia penale' (quindi, non solo l'indicazione dei suoi precedenti), offre la possibilità di usufruire dei servizi sociali, ma contiene altresì la prospettazione delle conseguenze cui costui andrà incontro laddove non si astenesse dal delinquere.

[61] In sostanza, si prevede che i *court advocacy voluneers*, oltre a essere avvisati dell'udienza per la cauzione e delle successive, partecipino attivamente per difendere l'interesse della comunità al contrasto alla violenza.

essere sottolineato il profilo problematico legato all'espressa previsione del coinvolgimento dei *prosecutors*, che saranno pertanto direttamente influenzati dall'inserimento del sospettato nella lista e dal contenuto della *custom notification letter*, ove saranno elencati i fattori noti relativi al sospettato e alla base del suo inserimento nella *Heat List*[62].

Va infine menzionato *Operation LASER* (acronimo di *Los Angeles Strategic Extraction and Restoration*)[63], il quale si caratterizza per il fatto di prevedere al contempo un modello *person-based* e uno *place-based*.

L'idea alla base di questo *software* – come del resto evoca lo stesso nome – è quella di colpire con la precisione di un *laser* i criminali violenti recidivi e i membri delle bande che commettono reati in aree specifiche[64].

Da un lato, si predispone il *Chronic Offenders Bulletin* che identifica gli individui ad alto rischio mediante un sistema che attribuisce uno *score* sulla base della 'storia criminale' del singolo e di altri fattori di rischio[65], con l'effetto che sarà intensificata la sorveglianza nei loro confronti. Dall'altro lato, il sistema seleziona le *LASER Zones*, che corrispondono a luoghi particolarmente pericolosi e, dunque, meritevoli di un più intenso controllo da parte delle forze di polizia.

In questa strategia si inseriscono anche incontri con i soggetti individuati sia per un approfondimento investigativo sia al fine di ottenere dati da inserire in una piattaforma investigativa digitale[66]. Così facendo si intendeva raccogliere il maggior numero possibile di dati sui gruppi criminali per futuri interventi di controllo e scopi di indagine, senza considerare i rischi di degenerazione in forme di sorveglianza di massa[67].

---

[62] V. FERGUSON, *Predictive Prosecution*, cit., 717 ss. che non esita a esprime tutte le sue perplessità al riguardo.

[63] V. FERGUSON, *Policing Predictive Policing*, cit., 1141 e la ricerca condotta con riguardo all'esperienza del dipartimento di polizia di Los Angeles, da BRAYNE, *Big Data Surveillance: The Case of Policing*, in *American Sociological Review*, 2017, vol. 82, no. 5, 977 ss. Questo sistema è stato finanziato, al pari di quello adottato a Kansas City, nell'ambito della *Smart Policing Initiative* nel 2011.

[64] V. il documento di UCHIDA-SWATT-GAMERO-LOPEZ-SALAZAR-KING-MAXEY-ONG-WAGNER-WHITE, *Los Angeles, California Smart Policing Initiative. Reducing Gun-Related Violence through Operation LASER*, ottobre 2012, 6 (https://vrnclearinghousefiles.blob.core.windows.net/documents/Reducing%20Gun-Related%20Violence%20through%20Operation%20LASER.pdf) laddove afferma: «The program is analogous to laser surgery, where a trained medical doctor uses modern technology to remove tumors or improve eyesight».

[65] I fattori riguardano in particolare: l'appartenenza del soggetto a una *gang*; la sottoposizione a *parole* o *probation*; eventuali precedenti arresti per reati commessi con arma da fuoco; la presenza, sulla fedina penale, di *violent crimes*; l'aver avuto '*quality police contact*' nei due anni precedenti. V., anche per ulteriori riferimenti a LASER, FERGUSON, *Surveillance and the Tyrant Test*, cit., 222 s.

[66] Tale piattaforma era gestita da una società privata, Palantir, ed era volta a permettere alla polizia di Los Angeles di tenere traccia dei vari modelli di criminalità esistenti in città.

[67] V. BRAYNE, *Predict and Surveil: Data, Discretion, and the Future of Policing*, Oxford, 2020, 37 ss.

Il ricorso a siffatti strumenti ha conosciuto due diverse stagioni[68]. In una prima fase si è avuta una diffusione notevole della *predictive policing*[69]; tuttavia, ciò è avvenuto in assenza di una regolamentazione e di controlli sul loro funzionamento. In un secondo momento, il dibattito pubblico e scientifico, che si è sviluppato, ha consentito di far emergere il lato oscuro di questi sistemi (e, in particolare, dei *person-based*).

L'effetto è stato quello di un progressivo abbandono dei *software* in diversi dipartimenti di polizia[70], dovuto, in alcuni casi, all'emanazione, a livello locale, di divieti all'uso di qualsivoglia strumento di polizia predittiva[71]; in altri – è il caso di Chicago[72] e Los Angeles[73] – ai risultati negativi di *audits* eseguiti.

Invero, all'esito delle verifiche compiute dalla RAND Corporation[74] sulla *Stategic Subject List*, è emerso anzitutto che il *software* elaborava predizioni di

---

[68] V. JOH, *Ethical AI in American Policing*, in *Notre Dame Journal on Emerging Technologies*, 2022, vol. 3, no. 2, 10 che parla in proposito di una «second wave of AI-based systems in policing», collocabile idealmente a partire dal 2020 e contrapposta alla prima, risalente al 2010, in cui si registrava un generale entusiasmo rispetto a tali innovative tecnologie. V. anche SILVERMAN, *AI and the Administration of Justice in the United States of America: Predictive Policing and Predictive Justice*, in *Revue Internationale de Droit Pénal*, 2023, 12 s.

[69] Secondo lo studio redatto nell'ambito di Upturn – un'organizzazione che promuove l'equità e la giustizia nella progettazione, nella *governance* e nell'uso della tecnologia – da ROBINSON-LOGAN KOEPKE, *Stuck in A Pattern Early Evidence on "Predictive Policing" and Civil Rights*, agosto 2016 (https://www.upturn.org/static/reports/2016/stuck-in-a-pattern/files/Upturn_-_Stuck_In_a_Pattern_v.1.01.pdf.), è emerso che, nel 2016, da un'indagine condotta sulle cinquanta maggiori forze di polizia degli Stati Uniti, almeno venti di esse hanno utilizzato un sistema di polizia predittiva e almeno altre undici stavano attivamente valutando le opzioni in tal senso. Si dava altresì atto del fatto che, secondo alcune fonti, centocinquanta o più dipartimenti si stavano muovendo verso questi sistemi con progetti pilota, *test* o nuove implementazioni.

[70] Per un quadro costantemente aggiornato sulle tecnologie utilizzate (attualmente o in passato, con indicazione del relativo periodo di interesse) dalle forze dell'ordine negli Stati Uniti, v. il *database* 'Atlas of Surveillance': https://atlasofsurveillance.org/search?utf8=%E2%9C%93&location=&technologies%5B86%5D=on.

[71] È il caso di Santa Cruz (California) che, nel 2020, è stata la prima città degli Stati Uniti a porre un *ban* alla *predictive policing*: v. STURGILL, *Santa Cruz Became the First U.S. City to Ban Predictive Policing*, in *L.A. Times*, 26 giugno 2020 (https://www.latimes.com/california/story/2020-06-26/santa-cruz-becomes-first-u-s-city-to-ban-predictive-policing). Nella dottrina americana, v. in senso critico JOH, *Ethical AI in American Policing*, 14 s. che ritiene preferibile affrontare le problematiche poste dall'intelligenza artificiale.

[72] La *Strategic Subject List* è stata dismessa nel novembre 2019: v. CHARLES, *CPD decommissions 'Strategic Subject List'*, in *Chicago Sun Times*, 27 gennaio 2020 (https://chicago.suntimes.com/city-hall/2020/1/27/21084030/chicago-police-strategic-subject-list-party-to-violence-inspector-general-joe-ferguson). Tuttavia, la polizia di Chicago ha continuato a utilizzare altre tecnologie, come i *place-based systems* e i sistemi di videosorveglianza (per maggiori dettagli sul punto v. FERGUSON, *Surveillance and the Tyrant Test*, cit., 229).

[73] LASER è stato abbandonato nel 2020 e, nello stesso anno, è stato risolto il contratto con *PredPol* in ragione di asseriti tagli di budget; tuttavia, gli studiosi ritengono che le reali motivazioni siano l'intensificarsi delle proteste della comunità locale e l'assenza di statistiche in grado di dimostrare un considerevole impatto del *software* in questione sulla riduzione del tasso di criminalità (v. FERGUSON, *Surveillance and the Tyrant Test*, cit., 226 s.).

[74] Queste hanno riguardato tutte le tecnologie basate sui *big data* impiegate dalla polizia di Chicago: v. il documento redatto da HOLLYWOOD-MCKAY-WOODS-AGNIEL, *Real-Time Crime Centers in Chicago.*

pericolosità individuale carenti sia in punto di efficacia che di accuratezza. Per un verso, il rischio era proiettato su un arco temporale – diciotto mesi – tale per cui risultava compromessa la possibilità di intervenire su situazioni in essere; per altro verso, il *software* prendeva in considerazione un numero così elevato di persone[75] – con significativi punteggi di rischio – che era di fatto impossibile avviare le procedure di monitoraggio e notifica di cui si è detto.

L'*audit* ha poi rilevato la scarsa qualità dei dati di cui il *software* si alimentava – in particolare, quelli relativi ai precedenti contatti con la polizia, quali gli arresti –, che rischiavano di essere agevolmente influenzati da *bias*, trattandosi di elementi ottenuti dai rapporti redatti al tempo dagli agenti di polizia[76].

A risultati non dissimili ha condotto l'*audit* dell'*Inspector General* sull'utilizzo di LASER a Los Angeles[77], che ha evidenziato come il sistema incoraggiasse la polizia a fermare gli individui inseriti nel *Chronic Offenders Bulletin* in assenza però della necessaria copertura costituzionale, in quanto la sola collocazione nella lista non può rappresentare un elemento sufficiente a giustificare il fermo[78]. Inoltre, si criticavano la quasi totale deregolamentazione di LASER, la mancanza di *training protocols* preventivi per testare il suo corretto funzionamento e, non da ultimo, la capacità del sistema di amplificare le già esistenti discriminazioni razziali.

Tuttavia, l'aspetto più preoccupante riguardava il fatto che il meccanismo di attribuzione dello *score* di rischio non teneva spesso conto di una reale corrispondenza tra tasso di pericolosità e precedenti penali del soggetto in questione. Basti considerare che il 44% di coloro che erano inseriti nella lista di cui abbiamo detto aveva subito soltanto un arresto o, addirittura, nessuno[79].

Anche nella giurisprudenza statunitense hanno iniziato a farsi sentire alcune voci critiche: ci riferiamo alle *concurring opinion* espresse nella decisione, risalente al 15 luglio 2020, della Corte d'appello del *Fourth Circuit* relativa al caso *United States of America v. Billy Curry, Jr.*[80]. Sebbene in questa sede si discutesse di un sistema *place-based*, è interessante riportare le parole del giudice Thacker, secondo cui la polizia predittiva «is no longer the shiny new object it may once have appeared to be, but

---

Evaluation of the Chicago Police Department's Strategic Decision Support Centers, Santa Monica, 2019 (https://www.rand.org/pubs/research_reports/RR3242.html). Riferimenti anche in FERGUSON, *Surveillance and the Tyrant Test*, cit., 228 s.

[75] Il calcolo includeva oltre 10.000 persone ad alto rischio e centinaia di migliaia con altri punteggi di rischio.

[76] Enfatizza questo aspetto FERGUSON, *Surveillance and the Tyrant Test*, cit., 228 s. Un ulteriore punto critico riguardava il fatto che il sistema, a differenza di altri (es. *HunchLab*), forniva solo un elenco di *targets*, senza alcuna indicazione strategica utile per la riduzione del *crime rate*, la quale dovrebbe rappresentare il principale obiettivo e, al contempo, la fonte di legittimazione dell'impiego di siffatti strumenti.

[77] V. il resoconto dell'*audit*: https://www.lapdpolicecom.lacity.org/031219/BPC_19-0072.pdf.

[78] V. FERGUSON, *Surveillance and the Tyrant Test*, cit., 227.

[79] Ciò accade perché anche coloro che sono stati vittime di determinati reati sono possibili candidati.

[80] Per il testo della pronuncia v. https://www.ca4.uscourts.gov/opinions/184233A.P.pdf. Nella dottrina italiana v. LONATI, Predictive policing: *dal disincanto all'urgenza di un ripensamento*, in *MediaLaws*, 2/2022, 308 s.

instead has revealed itself to be tarnished with racial bias». Ed è proprio sui profili discriminatori di simili *software* e sull'esigenza di assicurare la qualità dei dati che si è appuntata l'attenzione: il rischio prospettato è quello di una amplificazione dei pregiudizi razziali.

3. Le criticità dei *person-based systems*.

L'ingresso delle nuove tecnologie predittive nei dipartimenti di polizia prometteva una complessiva razionalizzazione e un generale ammodernamento delle strategie di intervento. In particolare, grazie all'analisi algoritmica e, poi, anche al vasto compendio conoscitivo offerto dai *big data*, si prospettava la possibilità di assicurare maggiore imparzialità all'operato degli agenti nonché di ottenere preziose informazioni sulla cui base orientare la loro attività: interventi mirati sui soggetti a rischio, in tempi estremamente più rapidi del normale, con una conseguente e più efficiente allocazione delle risorse umane. Il tutto avrebbe così dovuto determinare una riduzione del tasso di criminalità nonché un risparmio di costi e di tempo. In altre parole, alla polizia predittiva era sottesa l'idea «to do more with less»[81].

Si è trattato tuttavia di promesse non mantenute[82], in quanto la realtà della *predictive policing* e, in particolare, dei sistemi volti a individuare i *potential offenders* si è mossa in una direzione ben diversa fino a condurre, in molti casi, alla dismissione dei *software* in questione.

Un primo ordine di problemi riguarda i *dati* che sono forniti all'algoritmo. È stato anzitutto rilevato che in generale nelle fasi di raccolta, selezione e inserimento dei dati nel sistema può interferire un errore che poi naturalmente si rifletterà sulla validità dell'*outcome*[83].

Ma soprattutto e, prima ancora, si pone un problema di *qualità* dei dati[84]. È noto infatti come, specie rispetto ai *violent crime* più che ai *property crime* (si pensi ai casi di violenza domestica), esista una consistente 'cifra nera', nel senso che le vittime omettono di denunciarli[85], sicché alcune predizioni potrebbero risultare falsate. A ciò si aggiunga che molti dei dati su cui, come abbiamo visto, operano i sistemi *person-based*, sono relativi ai contatti avuti dall'individuo con la polizia: si tratta cioè di dati

---

[81] FERGUSON, *The Rise of Big Data Policing*, cit., 21.

[82] V. PARLAMENTO EUROPEO, *Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale*, Considerando C., ove si afferma che «l'uso sempre più frequente dell'IA nel diritto penale si basa, in particolare, sulla promessa che ridurrà determinati tipi di reati e favorirà l'adozione di decisioni più obiettive; [e] che tale promessa non sempre viene mantenuta». Per maggiori dettagli su tale provvedimento, v. *infra* § 7.

[83] FERGUSON, *Policing Predictive Policing*, cit., 1145.

[84] Tra gli autori italiani, v. in particolare su questo tema PELUSO, *Intelligenza Artificiale e dati di qualità: la tecnologia come valido alleato*, in *MediaLaws*, 2/2022, 326 ss.

[85] V. in questo senso FERGUSON, *Policing Predictive Policing*, cit., 1147 ove si evidenzia che secondo il Department of Justice la metà dei reati in cui è coinvolta una vittima non sono denunciati.

(nello specifico, di rapporti) generati dagli stessi agenti secondo la loro soggettiva percezione. Da qui il rischio che gli *input* forniti al *software* siano viziati a monte da pregiudizi, considerati gli studi volti a evidenziare la presenza, nell'operato della polizia negli Stati Uniti, di un *implicit bias* nei confronti di talune minoranze[86].

La potenzialità discriminatoria si apprezza altresì sotto il diverso profilo delle stesse modalità di funzionamento dei *tools* algoritmici, in quanto nessuno di essi può essere considerato interamente oggettivo «[since their] basic building blocks […] necessarily involve *human discretion*»[87]. Peraltro, le caratteristiche tipiche degli algoritmi predittivi basati sul *machine learning* finiscono per amplificare i pregiudizi, dal momento che gli stessi sono in grado di apprendere autonomamente dalle proprie esperienze di calcolo, così distaccandosi dalle istruzioni iniziali impartite dal programmatore.

Inoltre, mentre i sistemi volti all'individuazione di *crime hot spot* di regola sono alimentati con dati relativi a reati passati, informazioni socio-demografiche, etc., i *software* che elaborano un *risk assessment* individuale 'vivono' di dati personali. Ciò evidentemente può comportare frizioni con il fondamentale diritto alla *privacy* che non possono essere trascurate[88], imponendo, al contrario, l'esigenza di una regolamentazione dei processi di raccolta, analisi, conservazione e cancellazione degli stessi; nondimeno, in ragione della mole di dati processati dall'algoritmo, il rischio che si dia vita a forme di sorveglianza di massa è tutt'altro che remoto[89].

Un secondo ordine di problemi è legato alla nota opacità dell'algoritmo, ovverosia alla non ricostruibilità *ex post* della strada seguita per addivenire a un determinato risultato, sia a causa di ragioni tecniche – si tratta del c.d. *black box problem* dovuto al fatto che gli algoritmi basati sull'intelligenza artificiale, come si diceva poc'anzi, si distaccano dalle istruzioni iniziali per apprendere autonomamente – sia a ragioni prettamente economiche, nel senso che le aziende proprietarie dei *software* oppongono il *trade secret* alle richieste di chiarificazioni sul punto[90]. Non è il caso di sottolineare la rilevanza che, nel settore di nostro interesse, ha per l'individuo il fatto

---

[86] Prende atto di questa realtà FERGUSON, *Policing Predictive Policing*, cit., 1148 nonché 1149 ove constata: «Sadly, racial and class-based bias remain a problem of American policing». Sul punto, v. la ricerca di MAYSON, *Bias In, Bias Out*, in *The Yale Law Journal*, 2019, vol. 128, 2218 ss.

[87] JOH, *Policing by Numbers*, cit., 58 [il corsivo è nostro]; in senso analogo, v. MUGARI-OBIOHA, *Predictive Policing and Crime Control*, cit., 10.

[88] V. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Dir. pen. cont. – Riv. Trim.*, 4/2020, 81 s.

[89] V. JOH, *Ethical AI in American Policing*, cit., 11; BRAYNE, *Predict and Surveil*, cit., 37 ss. Nella letteratura italiana, v. SEVERINO, *Intelligenza artificiale e diritto penale*, cit., 539; PEREGO, *"Predictive policing": trasparenza degli algoritmi, impatto sulla privacy e risvolti discriminatori*, in *BioLaw Journal*, 2020, 453, che richiama la *concurring opinion* del giudice Sotomayor, nella sentenza della Corte Suprema degli Stati Uniti *United States v. Jones* del 2012, con cui ha espresso serie preoccupazioni rispetto alle violazioni della *privacy* derivanti dalla raccolta (in quel caso, attraverso sistemi GPS) di enormi quantitativi di dati personali da parte del Governo.

[90] V. tra i molti JOH, *Ethical AI in American Policing*, cit., 11 s.; HUNG-YEN, *On the Person-Based Predictive Policing*, cit., 166 s.

di conoscere i parametri sulla base dei quali è stato classificato *'at risk'*, anche in considerazione delle conseguenze che ciò comporta.

I rilievi sin qui svolti si riflettono a loro volta sull'affidabilità e sull'accuratezza delle predizioni di pericolosità, che potrebbero rivelarsi errate e, nella peggiore delle ipotesi, qualificare 'a rischio' soggetti che non sono in realtà tali (*false positive*)[91]. Ciò peraltro è effettivamente accaduto nell'esperienza applicativa di LASER a Los Angeles, come è stato rilevato dall'*audit* condotto dall'*Inspector General*[92].

Si rilevano lacune anche sul piano dell'*accountability*, nel senso che i 'bersagli' delle predizioni algoritmiche non sono nelle condizioni di contestare, ai soggetti responsabili, gli effetti lesivi che queste producono a loro danno.

Non deve allora sorprendere che – in virtù delle riscontrate 'debolezze' – i sistemi in questione non abbiano poi, nei fatti, raggiunto l'obiettivo ultimo cui erano diretti, ovverosia la reale riduzione del livello di criminalità.

Accanto a queste critiche, oramai consolidate, ci sembra emergano ulteriori profili meritevoli di segnalazione.

Un primo aspetto attiene alla considerazione, tra i parametri per selezionare i soggetti a rischio, di coloro che sono *in qualche modo collegati* a individui coinvolti in episodi di violenza. Se si tratta di soggetti che non presentano altri indici significativi di pericolosità, non si comprende davvero la ragione per cui debbano essere destinatari delle conseguenze sopra ricordate – diffide, visite a domicilio degli agenti, rischio di inasprimenti di pena per successivi episodi criminosi, monitoraggio da parte della polizia, etc.

Non mancano peraltro, nella casistica in materia, situazioni in cui anche il collegamento con una vittima di conflitti a fuoco sia determinante per ricadere nella 'lista calda'[93]. Ciò dimostra quanto sia elevato il rischio di attribuire la 'patente di pericolosità' a soggetti che, a ben vedere, non sono da considerare tali. Se, da un lato, la *social network analysis* può effettivamente disvelare connessioni che si rivelano fruttuose per l'emersione di gruppi criminali o comunque di soggetti meritevoli di particolare controllo da parte delle forze dell'ordine, dall'altro lato, è necessario che

---

[91] V. le interessanti osservazioni di GLESS, *Predictive policing. In defence of 'true positives'*, in BAYAMLIOĞLU-BARALUIC-JANSSENS- HILDEBRANDT (a cura di), *Being Profiled: Cogitas Ergo Sum. 10 Years of Profiling the European Citizen*, Amsterdam, 2018, 62 ss., secondo cui la polizia predittiva risulta ugualmente problematica anche rispetto ai *true positive*, allorché vengano, ad esempio, arrestati grazie all'ausilio di un *biased software*; in altre parole, si pone l'esigenza di assicurare alla difesa la possibilità di contestare, in sede processuale, l'utilizzo di un simile strumento illegittimo.

[92] V. *supra* § 2.1.1.

[93] V. al riguardo FERGUSON, *Predictive Prosecution*, cit., 720 e TUCEK, *Constraining Big Brother*, cit., 427 s. che riportano la vicenda di un giovane il cui nominativo era apparso sulla c.d. *Heat List*, elaborata dal dipartimento di polizia di Chicago, in ragione del fatto che un suo amico era stato *vittima* di un conflitto a fuoco. A ciò si aggiungevano sì dei precedenti penali a carico del giovane, ma consistenti in una sola condanna per *misdemeanor* e alcuni arresti minori; eppure, ciò ha fatto sì che costui fosse incluso nell'elenco dei soggetti considerati più inclini alla violenza e che, pertanto, fosse destinatario dei relativi avvertimenti circa le possibili conseguenze di un suo eventuale agire illecito, compresa l'inflizione di una pena più severa.

essa sia accompagnata da un riscontro circa l'effettiva pericolosità dell'*associate*; e ciò specie quando – si pensi al sistema in dotazione alla polizia di Kansas City – si ammette l'inclusione nel 'circolo' di soggetti che non presentano neppure un legame diretto con il *target offender* ma soltanto con un suo *associate*. O ancora, quando – come nell'esperienza della *Heat List* di Chicago – è sufficiente essere stato *vittima* di un episodio di violenza per 'finire nel mirino' della polizia.

Un secondo profilo critico è rappresentato dai meccanismi di diffida. Abbiamo visto che essa si sostanzia nell'invito ad astenersi dal commettere ulteriori reati, pena la possibilità di incorrere in conseguenze di rilievo, tra cui l'irrogazione di una sanzione più severa in ragione del precedente avvertimento – e, in effetti, la prassi testimonia come tale eventualità si sia poi concretizzata. Inoltre, il destinatario non dispone di mezzi per contestare il proprio inserimento nelle 'liste calde'.

Un ulteriore *punctum dolens* dei *person-based systems*[94] riguarda la potenziale influenza che la documentazione predisposta dalla polizia all'esito della problematica analisi algoritmica può esercitare sulle determinazioni della pubblica accusa. Ciò deriva dal fatto che, in sistemi come la *Strategic Subject List*, si prevede un coinvolgimento diretto dei pubblici ministeri, non solo perché questi possono partecipare agli incontri con gli individui inseriti nella *Heat List*, ma anche in quanto disporranno della *custom notification letter* contenente, tra l'altro, le risultanze del calcolo algoritmico. E se le criticità degli algoritmi predittivi già destano preoccupazione «when it comes to questions of where to send a patrol car, or even whom to investigate, they matter much more when data directly impacts a prosecutor's decision about individual liberty»[95].

In definitiva, ci sembra che gli specifici *software* in esame associno alle debolezze intrinseche degli algoritmi (qualità dei dati, opacità, scarsa accuratezza, etc.) gli ulteriori, rilevanti profili critici che ci auguriamo di aver messo in risalto. Vediamo allora, in questo scenario, quali sono state le proposte nel dibattito scientifico statunitense per ovviare (almeno in parte) agli aspetti segnalati.

4. Le proposte della dottrina americana.

Il sentimento nei confronti dell'impiego della polizia predittiva è, come è stato osservato, *duplice*: «while technique-centric enterprises […] emphasize potential benefits of AI-based PP [predictive policing], rights-centric NGOs cast doubt on possible violations of civic rights»[96]. Del resto, ciò rispecchia la doppia anima di molte tecnologie – tra cui non possono non rientrare anche i *software* di polizia predittiva – la quale, l'esperienza in materia di *cybercrime* insegna, fa sì che siano suscettibili di un

[94] FERGUSON, *Predictive Prosecution*, cit., 719.

[95] FERGUSON, *Predictive Prosecution*, cit., 706.

[96] Testualmente HUNG-YEN, *On the Person-Based Predictive Policing*, cit., 166.

dual-use[97], potendo esse prestarsi a essere utilizzate «to achieve good or evil»[98]. Il punto centrale allora diviene il *come* determinati strumenti sono concretamente impiegati.

A fronte delle 'debolezze' emerse dall'incontrollato utilizzo dei *software* di polizia predittiva, gli studiosi statunitensi hanno così iniziato a interrogarsi sulle soluzioni in grado di minimizzare i difetti connaturati a simili strumenti.

Abbiamo in precedenza visto come un problema di primario rilievo attenga ai *dati*, sia sotto il profilo dei possibili errori nelle fasi di raccolta, selezione e inserimento nel sistema, sia in relazione alla loro natura discriminatoria e al relativo impatto sulla *privacy*. Al riguardo, è stato anzitutto sostenuto che un primo, fondamentale passo da compiere è quello di rendere gli agenti di polizia edotti di simili rischi, per interrompere questo atteggiamento di totale affidamento alla *predictive policing*. In altre parole, si ritiene che solo la consapevolezza delle suddette criticità «sets the stage for correcting error, auditing error, and training humans to prevent error»[99].

Da qui la proposta di campagne di sensibilizzazione, ad opera dei *police administrators*, degli operatori direttamente coinvolti nell'impiego dei *software*, nonché di appositi corsi di formazione da parte delle stesse società progettatrici dei *software*. Queste ultime, infatti, potrebbero avere interesse a 'educare' il personale delle forze dell'ordine che utilizzerà i loro prodotti, nella misura in cui sarà l'esperienza da loro maturata a sviluppare e migliorare ulteriormente le tecnologie predittive[100].

Naturalmente, occorre poi predisporre concrete misure operative per porre rimedio a simili problematiche, quali meccanismi di *audit* per verificare la qualità degli *input* (ad esempio, si potrebbe prescrivere il controllo, da parte di supervisori o analisti, dei rapporti giornalieri sui reati, ovvero *forensics audit* su larga scala del sistema di *reporting*) nonché specifiche regole in tema di raccolta e conservazione di tali dati per preservare la *privacy* dei soggetti sottoposti alle predizioni del *tool*. Si potrebbe inoltre affidare ai *data services* il compito di 'ripulire' i *database* dai dati duplicati o errati; e, soprattutto, gli stessi *software* potrebbero essere progettati per gestire e, di conseguenza, minimizzare gli errori[101]. Simili misure, peraltro, garantirebbero una maggiore accuratezza delle predizioni elaborate[102] e, in ultima analisi, il raggiungimento dell'obiettivo di riduzione della criminalità.

---

[97] Sul tema in questione nel diverso contesto della criminalità informatica, v. nella dottrina italiana il lavoro di SALVADORI, *Criminalità informatica e tecniche di anticipazione della tutela penale l'incriminazione dei "*dual-use software*"*, in *Riv. it. dir. proc. pen.*, 2017, 747 ss.

[98] V. ancora HUNG-YEN, *On the Person-Based Predictive Policing*, cit., 166 e, in particolare, la nota n. 5.

[99] Così FERGUSON, *Policing Predictive Policing*, cit., 1151.

[100] In tal senso, v. ancora FERGUSON, *Policing Predictive Policing*, cit., 1153.

[101] V. FERGUSON, *Policing Predictive Policing*, cit., 1151 s.

[102] V. BAGARIC-SVILAR-BULL-HUNTER-STOBBS, *The Solution to The Pervasive Bias and Discrimination in the Criminal Justice System*, cit., 111, i quali affermano che, sebbene l'uso dei sistemi di polizia predittiva rimanga controverso, le limitate risultanze a disposizione attesterebbero che gli stessi sono in grado di elaborare predizioni più efficaci rispetto ai metodi tradizionali.

Con riferimento al problema delle discriminazioni, è stato evidenziato come lo stesso non origini direttamente dall'impiego degli strumenti in esame – sebbene sia indubbio che questi, se non correttamente utilizzati, possano amplificarlo – ma fossero già riscontrabili *bias* nel tradizionale operato della polizia statunitense[103]. Allora, *software* costruiti secondo le modalità indicate potrebbero contribuire a rilevare e contrastare le *malpractices* esistenti[104].

Sotto il diverso e centrale profilo della trasparenza, essa assicura, da un lato, il controllo sul *governmental power*[105] e, dunque, il corretto operato della polizia, nonché, dall'altro, il rispetto dei diritti dell'individuo e, in generale, la fiducia dei consociati negli strumenti in considerazione[106].

È pertanto necessario imporre la piena *disclosure* circa le modalità di funzionamento dei *predictive policing systems*, senza che il segreto industriale possa rappresentare un ostacolo. La posta in gioco è tale che bisogna dare preminenza all'interesse del singolo a conoscere «how an automated process came to a particular decision, whether it might contain errors, and thus provide a possible basis for contestation and appeal»[107].

Per altro verso, occorre spiegare ai consociati le ragioni che militano a favore del ricorso ai *software* di cui si tratta, al contempo coinvolgendoli attivamente nei processi di adozione e di convalida degli stessi[108]. Come vedremo, questi aspetti hanno assunto un rilievo centrale nel contesto dei primi tentativi di disciplina della materia registratisi negli Stati Uniti[109].

Un tema diverso, ma connesso a quello della trasparenza, è l'*accountability*[110] di tali strumenti, che consiste nell'assicurare ai cittadini la possibilità di ritenere i *decision-makers* responsabili delle proprie azioni. In questo senso, la dottrina americana ha sottolineato che la polizia predittiva parrebbe rispondere perfettamente a una simile esigenza – «can be a force for accountability»[111] – alla luce della sua natura *data-driven* che consente di rendere pubblici i risultati del relativo utilizzo da parte delle forze dell'ordine, permettendo così alla collettività e al singolo individuo di contestare eventuali comportamenti scorretti.

---

[103] V. la nota n. 86.

[104] V. HUNG-YEN, *On the Person-Based Predictive Policing*, cit., 166. Indicazioni in tal senso sono ricavabili altresì da BAGARIC-SVILAR-BULL-HUNTER-STOBBS, *The Solution to The Pervasive Bias and Discrimination in the Criminal Justice System*, cit., 111; JOH, *Ethical AI in American Policing*, cit., 23.

[105] Evidenzia questo aspetto ZARZKY, *Transparent Predictions*, in *University of Illinois Law Review*, 2013, 1533.

[106] JOH, *Ethical AI in American Policing*, cit., 21 s.

[107] Le suddette affermazioni sono di JOH, *Ethical AI in American Policing*, cit., 21 s.

[108] V. ancora JOH, *Ethical AI in American Policing*, cit., 22.

[109] V. *infra* § 5.

[110] V. FERGUSON, *Policing Predictive Policing*, cit., 1168, che la definisce «the ethical obligation of individuals (in this case, governmental officials) to answer for their actions, possible failings, and wrongdoings».

[111] V. sul punto FERGUSON, *Policing Predictive Policing*, cit., 1170.

Infine, un aspetto a nostro avviso fondamentale emerso nel dibattito americano è la centralità del controllo umano: anche in presenza dei migliori strumenti predittivi, rimane il fatto che l'identificazione di luoghi o soggetti 'a rischio' non può *ex se* ridurre la criminalità. Ciò che davvero conta sono le concrete azioni poste in essere a seguito dell'ottenimento dell'*output* predittivo[112].

In definitiva, dunque, spetta all'uomo (*rectius*, al singolo agente di polizia) governare la *predictive policing*, non solo nella fase di elaborazione, ma anche in quella di valutazione dei relativi risultati al fine di adottare le opportune iniziative. Si afferma allora, (anche) tra gli studiosi d'oltreoceano, l'idea di assegnare a questi strumenti una funzione di supporto delle strategie investigative al fine di migliorarne l'efficienza e l'efficacia, e giammai quella di sostituire la figura dell'uomo.

L'analisi sin qui svolta ci permette di meglio inquadrare i primi tentativi di disciplina del fenomeno negli Stati Uniti.

5. I tentativi di regolamentazione negli USA: la proposta dell'*American Civil Liberties Union* e le *Local Surveillance Technology Oversight Ordinances*.

Il crescente e incontrollato utilizzo dei *software* di polizia predittiva negli Stati Uniti e, in generale, delle c.d. *surveillance technologies* – si pensi, tra le altre, ai sistemi di riconoscimento facciale – ha generato, come si diceva, forti reazioni nelle comunità locali interessate e, in particolare, nelle minoranze, statisticamente interessate in misura rilevante da tali misure[113], che hanno tentato di far sentire la propria voce affinché le istituzioni intervenissero per porre rimedio a siffatta situazione.

A fronte del totale immobilismo dei *policy-makers*, l'*American Civil Liberties Union (ACLU)*, un'organizzazione non governativa fondata nel 1920 e deputata alla difesa dei diritti civili, il 21 settembre 2016 ha lanciato, con il supporto di molti *civil rights groups*[114], la *Community Control Over Police Surveillance (CCOPS) campaign*[115], il cui principale obiettivo è quello di promuovere l'approvazione di una specifica disciplina (c.d. *CCOPS laws*) che garantisca ai residenti locali, attraverso i loro

---

[112] In questo senso, v. per tutti JOH, *Ethical AI in American Policing*, cit., 26 s.; HUNG-YEN, *On the Person-Based Predictive Policing*, cit., 169 s.

[113] È esemplificativa l'esperienza di Chicago con la *Heat List* e di Los Angeles con LASER, in cui, rispettivamente, la maggior parte degli individui inseriti nella 'lista calda' erano uomini di colore e quelli selezionati nel sistema californiano erano perlopiù individui di sesso maschile latinoamericani e di colore. V. al riguardo FERGUSON, *Surveillance and The Tyrant Test*, cit., 233.

[114] V. MAASS, *Join the Movement for Community Control Over Police Surveillance*, in *Electronic Frontier Foundation*, 21 settembre 2016 ().

[115] Informazioni di dettaglio su tale campagna sono disponibili sul sito dell'ACLU: https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance?redirect=feature/community-control-over-police-surveillance. Nella dottrina americana, v. FERGUSON, *Surveillance and the Tyrant Test*, cit., 250 ss.; JOH, *Ethical AI in American Policing*, cit., 13 s.

rappresentanti comunali, il potere di decidere se e come le tecnologie di sorveglianza debbano essere utilizzate dalle forze di polizia nella propria area.

A tal fine, è stato elaborato il *CCOPS bill*[116], ovverosia il modello di ordinanza che i governi locali sono invitati ad adottare per regolare il processo di approvazione di ogni decisione (finanziamento, acquisizione o utilizzo) concernente una *surveillance technology*, al fine di promuovere «transparency, the public's welfare, civil rights, and civil liberties»[117].

In termini generali, secondo il modello CCOPS le ordinanze dovrebbero prevedere che un determinato *municipal entity* ottenga la *preapproval* del proprio *city council* (cioè del consiglio comunale o di un altro organo di controllo eletto) prima di richiedere fondi, acquisire, prendere in prestito o utilizzare tali tecnologie.

È interessante notare che, secondo le indicazioni dell'ACLU, tale autorizzazione deve essere successiva a un'audizione pubblica obbligatoria del consiglio comunale, durante la quale ai cittadini, previa apposita notifica, viene offerta «a fair and adequate opportunity to provide online, written and oral testimony»[118]. È proprio con questa previsione che il *bill* intende assicurare il più ampio coinvolgimento della società civile nelle decisioni concernenti le tecnologie di sorveglianza.

Inoltre, il modello impone di presentare: rapporti sull'impatto della tecnologia di sorveglianza in questione, relative politiche di utilizzo, *audits* annuali, *public hearings and reports*, tutele per i *whistleblowers* e rimedi legali in caso di mancato rispetto delle prescrizioni. Così facendo, si vuole assicurare che i *municipal entity* (nel nostro caso, i *police departments*) valutino nel dettaglio i rischi della tecnologia in esame per la *privacy* e le libertà civili e, al contempo, adottino politiche volte a minimizzarli nonché prevedano processi di controllo[119].

Come riportato dall'ACLU, al momento il *CCOPS bill* ha avuto attuazione in ventidue giurisdizioni statunitensi, le quali si sono dotate di una *Local Surveillance Technology Oversights Ordinance*[120]. È interessante notare come, all'esito di un'analisi comparativa[121], siano stati rintracciati alcuni elementi comuni alla gran parte delle

---

[116] Il *CCOPS bill* è consultabile al seguente link: https://www.aclu.org/legal-document/community-control-over-police-surveillance-ccops-model-bill. Inoltre, per semplificare alcuni requisiti del *CCOPS bill* e dunque promuovere il ricorso a queste ordinanze, sono stati elaborati due modelli simili nell'ambito dell'iniziativa *NYU Policing Project*: l'*Authorized Policing Technology (APT) Act* – sostanzialmente sovrapponibile al modello *CCOPS* – e l'*Authorized Databases and Policing Technology (ADAPT) Act*, che si indirizza ai *databases*, centrali nel contesto delle tecnologie di sorveglianza, al fine di estendere anche a questi le procedure di *transparency* e *oversight* (v. https://www.policingproject.org).

[117] Così recita la stessa intestazione del *CCOPS bill*.

[118] V. *CCOPS bill*, 1.

[119] V. FERGUSON, *Surveillance and the Tyrant Test*, cit., 251, secondo cui, sebbene il modello non lo specifichi, affinché le ordinanze siano operative, sarà essenziale il contributo di esperti in materia di *surveillance tecnhologies* e di *privacy law* per condurre l'analisi dei rischi e redigere rapporti per conto della comunità.

[120] Per un'analisi di tali ordinanze v. FIDLER, *Local Police Surveillance and the Administrative Fourth Amendment*, in *Santa Clara High Technology Law Journal*, 2020, 545 ss.

[121] V. il *white paper* di CHIVUKULA-TAKEMOTO, *Local Surveillance Oversight Ordinances*, Samuelson Law,

ordinanze adottate, pur non mancando tratti di differenziazione, atteso che i *local governments* non hanno riprodotto esattamente le indicazioni contenute nel *CCOPS bill*[122].

Cerchiamo allora di fare un bilancio, mettendo in risalto la tipologia di ordinanze che ci sembrano meritevoli di candidarsi a modello di riferimento.

Innanzi tutto, si riscontra una generale uniformità rispetto alla definizione di *'surveillance technology'*[123] accolta nei diversi provvedimenti esaminati, tra cui rientrano naturalmente, per ciò che rileva ai nostri fini, i *software* di *predictive policing*. Si tratta evidentemente di un profilo centrale nella misura in cui esso condiziona la sottoposizione alla disciplina prescritta delle decisioni riguardanti il relativo impiego (o finanziamento, acquisizione, etc.).

Si registrano invece alcune differenze in relazione all'ambito di operatività: alcune ordinanze si applicano a tutti i dipartimenti della giurisdizione, altre ne esentano alcuni dal proprio perimetro applicativo o prevedono regole speciali per le forze dell'ordine[124], altre ancora coprono solo un dipartimento[125]. Il fatto di escludere o prevedere 'clausole di salvezza' per i *law enforcement departments*, benché si registri nella minoranza dei casi, di fatto vanifica il tentativo di regolare la *predictive policing*, in nome dell'asserita esigenza di preservare le attività investigative. A ciò si associa il fatto che la maggioranza delle *ordinances* contempla una esenzione dal processo di approvazione, in presenza di *'exigent circumstances'*[126].

Sono poi abbastanza omogenee le previsioni relative ai documenti da presentare a corredo della istanza di approvazione della tecnologia da impiegare, richiedendosi tendenzialmente in tutti i casi l'elaborazione di *policies*, *impact report* e

---

Technology & Public Policy Clinic – Berkeley School of Law, University of California, febbraio 2021 (https://www.law.berkeley.edu/case-project/local-surveillance-oversight-ordinances-white-paper/).

[122] Pone l'accento su questo aspetto FIDLER, *Local Police Surveillance*, cit., 546.

[123] Quasi tutte le definizioni includono sia un *tipo* di dispositivo che si qualifica come tecnologia di sorveglianza, sia uno *scopo* per il quale tale dispositivo deve essere utilizzato. Ad esempio, l'ordinanza adottata ad Oakland (California) definisce la tecnologia di sorveglianza come «any software, electronic device, system utilizing an electronic device, or similar, [that is] used, designed, or primarily intended to collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information associated with, or capable of being associated with, any individual or group». Inoltre, in molti casi, si prevede un elenco di tecnologie specifiche. V. CHIVUKULA-TAKEMOTO, *Local Surveillance Oversight Ordinances*, cit., 5.

[124] È il caso, tra gli altri, dell'ordinanza emanata a Nashville (Tennessee) che esclude dal suo perimetro applicativo le attività di «acquisition or use of surveillance technology by or on behalf of law enforcement that is used on a temporary basis for the purpose of a criminal investigation supported by reasonable suspicion, or pursuant to a lawfully issued search warrant, or under exigent circumstances as defined in case law». V. sul punto CHIVUKULA-TAKEMOTO, *Local Surveillance Oversight Ordinances*, cit., 7.

[125] Così l'ordinanza adottata nella città di New York che si applica soltanto al *police department*, v. CHIVUKULA-TAKEMOTO, *Local Surveillance Oversight Ordinances*, cit., 8.

[126] Sulle diverse definizioni di '*exigent circumstances*' nelle varie ordinanze e per un approfondimento generale sui casi di esenzione, v. CHIVUKULA-TAKEMOTO, *Local Surveillance Oversight Ordinances*, cit., 16 ss.

una relazione annuale sulle pratiche e le politiche di sorveglianza[127]. Così come si stabilisce in prevalenza che la disciplina si applichi retroattivamente, cioè anche rispetto a tecnologie di sorveglianza già in uso[128].

Ad ogni modo, riteniamo che il requisito più importante – e che peraltro è previsto in tutte le ordinanze, eccetto una[129] – riguardi la costituzione di un *elected oversight body*, composto dai rappresentanti della comunità locale e incaricato di revisionare e approvare i *reports* nonché le *policies* presentate ai sensi dell'ordinanza. Si tratta invero della risposta concreta all'obiettivo che ha dato luogo alla nascita dell'iniziativa *CCOPS* dell'ACLU, ovverosia quello di incentivare la partecipazione dei cittadini alle decisioni sulle tecnologie di sorveglianza che, come abbiamo avuto modo di rilevare, possono avere pesanti riflessi sui diritti dei singoli individui.

Per altro verso, ci pare da valorizzare il coinvolgimento – seppur previsto dalla netta minoranza dei provvedimenti in esame – di un organismo indipendente cui è attribuito un ruolo di primario rilievo nell'ambito del processo di approvazione, essendo deputato a esaminare le *surveillance technologies* e a fornire raccomandazioni sul punto.

In questo senso, è significativa l'esperienza di Oakland (California) – qualificata dagli studiosi americani come un *gold standard*[130] – ove si è assistito alla istituzione della *Privacy Advisory Commission*[131], dotata di penetranti funzioni di consulenza preventiva rispetto alla approvazione delle tecnologie di sorveglianza. In particolare, si tratta di un organismo composto dai rappresentanti della comunità che offre al *city council* una consulenza tecnica sui rischi per la *privacy* della nuova tecnologia di sorveglianza, prepara relazioni pubbliche annuali sulle *surveillance technologies* esistenti e supervisiona le audizioni pubbliche sull'uso delle stesse da parte del governo[132].

Infine, è sicuramente apprezzabile il fatto che quasi tutte le ordinanze prevedano meccanismi di *enforcement* – la cui tipologia, a ben vedere, varia in alcuni gruppi di provvedimenti[133] – nel caso in cui la procedura di approvazione non sia rispettata, così assicurando l'effettività del complesso sistema.

---

[127] Per maggiori dettagli v. CHIVUKULA-TAKEMOTO, *Local Surveillance Oversight Ordinances*, cit., 8 ss.

[128] CHIVUKULA-TAKEMOTO, *Local Surveillance Oversight Ordinances*, cit., 11.

[129] Il riferimento è alla città di New York, ove si prevede una mera considerazione dell'opinione del pubblico: «the [police] commissioner shall *consider* public comments and provide the final surveillance technology impact and use policy to the speaker and the mayor»; V. CHIVUKULA-TAKEMOTO, *Local Surveillance Oversight Ordinances*, cit., 10.

[130] FIDLER, *Local Police Surveillance*, cit., 548.

[131] V. FERGUSON, *Surveillance and the Tyrant Test*, cit., 253, che la definisce come «one of the more prominent independent community oversight bodies».

[132] V. FERGUSON, *Surveillance and the Tyrant Test*, cit., 254, il quale evidenzia che, con riguardo alle attività di *law enforcement*, la commissione ha, tra l'altro, elaborato le politiche di utilizzo per i lettori automatici di targhe, i droni senza pilota e altre tecnologie, oltre ad avere contribuito a vietare i *software* di riconoscimento facciale.

[133] Ad esempio, il meccanismo più comune è un *privacy right of action*, mentre è più rara l'introduzione di apposite *misdemeanors*. V. CHIVUKULA-TAKEMOTO, *Local Surveillance Oversight Ordinances*, cit., 13 ss.

Ebbene, all'esito di questa panoramica sulle *Local Surveillance Technology Oversight Ordinances*, rimangono perplessità su diversi fronti.

Anzitutto si tratta di una iniziativa che, come è stato evidenziato, non ha avuto un seguito assai diffuso, se solo si considera che neppure la metà degli Stati americani ha effettivamente adottato un'ordinanza, sebbene vi siano stati casi in cui erano state avanzate proposte poi respinte o bloccate[134]. Le ragioni sono molteplici[135], ma sicuramente vi sono resistenze da parte delle stesse forze di polizia a questo tipo di controllo capillare sulle loro scelte strategiche, che sono difficilmente superabili in assenza di una legge statale.

Sotto il diverso profilo dell'efficacia e dell'effettività delle disposizioni concretamente inserite nelle ordinanze, abbiamo rilevato come vi siano 'esenzioni' di carattere soggettivo (la definizione dei *government bodies* coperti dal provvedimento) e oggettivo (le *exigent circumstances* che esonerano dalla procedura di *preapproval*), che potrebbero nei fatti comprometterne l'operatività rispetto alla polizia predittiva.

Siamo ancora lontani, insomma, da quella risposta politica di ampio respiro alle istanze di regolamentazione della *predictive policing*[136] e, in generale, dell'intelligenza artificiale che, sola, potrebbe rappresentare una valida soluzione alle problematiche che tali strumenti sollevano. Tuttavia, crediamo che, in rapporto alla precedente situazione di completa *deregulation*, la soluzione offerta dall'ACLU e seguita da alcune amministrazioni locali rappresenti un primo, importante passo in avanti. Il processo di autorizzazione descritto, la provenienza delle ordinanze da un ente vicino alle esigenze della comunità interessata, l'effettivo coinvolgimento dei relativi rappresentanti nell'approvazione di ogni strumento e la previsione di meccanismi di *enforcement* per garantire l'efficacia complessiva del sistema sono senza dubbio elementi apprezzabili che possono, inoltre, servire da guida per il futuro sviluppo di una legislazione più estesa.

Al contrario, in assenza di questi primi tentativi di regolazione, due sono gli scenari possibili: il perdurante e incontrollato utilizzo della polizia predittiva, con tutte le problematiche prima evidenziate ovvero l'emanazione, a fronte di rischi legati a contestazioni pubbliche su larga scala, di divieti assoluti rispetto all'impiego di specifiche tecnologie, basati sull'illusione di poter così arginare le pratiche discriminatorie della polizia registratesi negli USA[137]. In realtà, crediamo che un simile approccio di chiusura sottovaluti che le nuove tecnologie in questione – se

---

[134] JOH, *Ethical AI in American Policing*, cit., 14.

[135] V. ad esempio le riflessioni di FIDLER-LIU, *Four Obstacles to Local Surveillance Ordinances*, in *Lawfare*, 4 settembre 2020 (https://www.lawfareblog.com/four-obstacles-local-surveillance-ordinances).

[136] V. SILVERMAN, *AI and the Administration of Justice in the United States of America*, cit., 17 s. che rileva l'assenza di iniziative legislative pendenti; tuttavia, sul diverso piano della *soft law*, riporta un progetto dell'American Law Institute (ALI), dal titolo *Principles of the Law, Policing*, che offre alcune linee guida anche agli agenti di polizia nell'uso dei sistemi algoritmici, indicando il necessario rispetto dei consueti *standard* (in punto di trasparenza, accuratezza, *fairness*, etc.) atti a minimizzare i rischi connessi al loro impiego.

[137] È critica rispetto all'adozione di *bans* JOH, *Ethical AI in American Policing*, cit., 14 s.

debitamente regolate – possono offrire l'opportunità di porre un freno a queste pratiche ripensando alle strategie operative dei dipartimenti di polizia[138].

Questo è il quadro oggi dello stato della specifica regolamentazione in tema di *predictive policing* negli Stati Uniti. Per comprendere tuttavia quale sia nel suo insieme l'orizzonte regolatorio, è necessario indirizzare l'attenzione verso iniziative a più ampio raggio, quale il progetto elaborato di recente dalla Casa Bianca sui principi che devono governare l'intelligenza artificiale, a cui dedicheremo adesso la nostra attenzione.

5.1. Il Blueprint for an AI Bill of Rights.

Nell'ottobre 2022, l'*Office of Science and Technology Policy* (OSTP) presso la Casa Bianca[139] ha pubblicato il *'Blueprint for an AI Bill of Rights. Making Automated Systems Work for the American People'*, un libro bianco che, in maniera non vincolante, fissa alcuni principi per il corretto utilizzo dei sistemi automatizzati di intelligenza artificiale, che dovrebbero servire da guida per il futuro sviluppo di politiche in materia a salvaguardia dei diritti civili.

In particolare, il suo ambito di applicazione riguarda: «(1) automated systems that (2) have the potential to meaningfully impact the American public's rights, opportunities, or access to critical resources or services»[140].

Non si tratta evidentemente di un documento che si presta a disciplinare in modo puntuale la polizia predittiva né avrà un effetto diretto sull'utilizzo di simili *software*, non comportando limitazioni o divieti. Tuttavia, i principi di *soft law* ivi

---

[138] Per alcuni significativi dati, v. FERGUSON, *The Rise of Big Data Policing*, cit., 22 ss., che riporta i risultati di una indagine condotta nell'ambito del Dipartimento di Polizia di Ferguson (Missouri), secondo cui tra il 2012 e il 2014 gli afroamericani sono stati coinvolti nell'85% dei fermi di veicoli, nel 90% delle citazioni e nel 93% degli arresti, nonostante rappresentassero solo il 67% della popolazione della città.

[139] Si tratta di un ufficio, istituito nel 1976, con il compito di fornire al Presidente degli Stati Uniti e al suo *Executive Office* consulenze in diverse materie, tra cui la tecnologia e lo sviluppo nazionale. Per maggiori informazioni, v. il sito ufficiale https://www.whitehouse.gov/ostp/.

[140] THE WHITE HOUSE, *Blueprint for an AI Bill of Rights. Making Automated Systems Work for the American People*, ottobre 2022, 8 (il testo completo è reperibile al seguente link: https://www.whitehouse.gov/ostp/ai-bill-of-rights/#notice). Il documento specifica altresì che per 'automated system' si intende «any system, software, or process that uses computation as whole or part of a system to determine outcomes, make or aid decisions, inform policy implementation, collect data or observations, or otherwise interact with individuals and/or communities. Automated systems include, but are not limited to, systems derived from machine learning, statistics, or other data processing or artificial intelligence techniques, and exclude passive computing infrastructure. 'Passive computing infrastructure' is any intermediary technology that does not influence or determine the outcome of decision, make or aid in decisions, inform policy implementation, or collect data or observations, including web hosting, domain registration, networking, caching, data storage, or cybersecurity. Throughout this framework, automated systems that are considered in scope are only those that have the potential to meaningfully impact individuals' or communities' rights, opportunities, or access».

contenuti si riferiscono proprio a tali sistemi, i quali presentano i due presupposti applicativi prima richiamati.

L'idea di fondo che anima il *Blueprint* è quella secondo cui i sistemi automatizzati hanno consentito di raggiungere progressi straordinari nei diversi settori in cui hanno fatto ingresso, però – si legge – «this important progress must not come at the price of civil rights or democratic values»[141]. Pertanto, il libro bianco individua in primo luogo cinque principi e le *associated practices*, che dovrebbero guidare la progettazione, l'uso e l'impiego di sistemi automatizzati per proteggere i cittadini americani dalle potenzialità lesive dell'intelligenza artificiale; a ciascuno di essi seguono poi *three supplemental sections*, in cui si specificano, rispettivamente, le ragioni per le quali ogni singolo principio è rilevante (*'why this principle is important'*), le aspettative circa l'uso dei sistemi automatizzati (*'what should be expected of automated systems'*) e, infine, i risvolti pratici derivanti dall'applicazione di ogni principio (*'how these principles can move into practice'*).

Cerchiamo quindi di ricostruire il contenuto essenziale del documento in esame.

Il primo principio implica che i sistemi automatizzati siano *safe and effective*, a partire dalla loro progettazione nonché durante il loro utilizzo. Simili considerazioni derivano dalla asserita consapevolezza dell'esistenza, nella prassi, di sistemi affetti da anomalie di funzionamento, le quali hanno avuto ripercussioni negative sulla società civile. A titolo esemplificativo, per ciò che rileva ai nostri fini, il libro bianco richiama espressamente quei *software* di polizia predittiva volti all'individuazione di *crime hot spot* che determinano il ripetuto invio di pattuglie in certi quartieri, sebbene questi non denotino il più alto tasso di criminalità. Siffatte predizioni errate si ritiene rappresentino il risultato di un *feedback loop*, derivante dal fatto che la concentrazione dei controlli in una determinata area urbana originariamente qualificata 'a rischio' dal *tool* consentirà ragionevolmente alla polizia di rilevare un certo numero di reati; reinserendo poi nel sistema i dati relativi a tali ultime attività criminali, si finirà per incrementare il tasso di rischio di quella zona, con il risultato di convogliare lì tutte le risorse – trascurando, di conseguenza, altri quartieri – e di sottoporre a una sorveglianza eccessiva i relativi residenti[142].

Di conseguenza, al fine di garantire la sicurezza e l'efficacia di un sistema automatizzato, il documento suggerisce di prevedere misure atte a proteggere gli individui dai possibili effetti lesivi, quali: evitare l'uso di dati inappropriati o irrilevanti per l'attività da svolgere, compreso il riutilizzo di dati o di *outcome* che potrebbe causare danni ancor più gravi; compiere verifiche per rilevare, gestire e monitorare eventuali rischi, sia in chiave preventiva sia in fase di utilizzo del sistema; consultare le *impacted communities* prima di autorizzare il ricorso al sistema

---

[141] THE WHITE HOUSE, *Blueprint for an AI Bill of Rights*, cit., 3.

[142] Nella dottrina italiana, evidenziano, tra gli altri, una simile criticità SEVERINO, *Intelligenza artificiale e diritto penale*, cit., 541 s.; BASILE, *Intelligenza artificiale e diritto penale*, cit., 30.

automatizzato ovvero modifiche significative; istituire organismi indipendenti deputati al monitoraggio della efficacia e della sicurezza dei sistemi medesimi.

Il secondo principio riguarda invece la protezione dalla discriminazione algoritmica. Si tratta, come abbiamo visto, di una problematica particolarmente avvertita nel panorama americano, emersa con forza anche nelle diverse applicazioni di *predictive policing*. Il progetto raccomanda quindi di prestare molta attenzione nelle diverse fasi di selezione e raccolta dei dati, nonché di valutare gli specifici rischi discriminatori per assicurare che i sistemi automatizzati siano non solo utilizzati ma anche progettati in maniera tale da garantire l'uguaglianza.

Il terzo principio attiene alla *data privacy*, implicando che ogni individuo disponga di una tutela adeguata a fronte di pratiche abusive di trattamento dei dati e abbia altresì la possibilità di decidere come i dati che lo riguardano debbano essere utilizzati.

Sebbene non esista ancora negli Stati Uniti «a comprehensive statutory or regulatory framework governing the rights of the public when it comes to personal data»[143], è necessario predisporre misure che assicurino, rispetto ai sistemi automatizzati, gli *standard* di *privacy-by-design* e *privacy-by-default* nonché prevedere, oltre ad apposite procedure di *risk identification and mitigation*, altrettanti accorgimenti in grado di limitare la raccolta dei dati in relazione agli obiettivi strettamente necessari[144].

In questo contesto, ciò che sembra destare le maggiori preoccupazioni della Casa Bianca riguarda le pratiche di sorveglianza, cui è riservata un'apposita sezione. Qui si sottolinea, tra l'altro, l'esigenza di sottoporre simili *practices* a più penetrante controllo pubblico – attraverso *preventive assessment* che scongiurino, soprattutto, i rischi di discriminazione – nonché di circoscriverle, anche qui, ai casi in cui risultino strettamente necessarie e proporzionate alla finalità che si intende perseguire.

Passando al quarto punto, ci si imbatte nel *notice and explanation principle*, che richiama senz'altro alla mente il fondamentale tema della trasparenza algoritmica, il quale viene qui in rilievo in una duplice accezione: da un lato, il *Blueprint* intende garantire al pubblico il diritto di essere edotto dell'utilizzo di un sistema automatizzato e, dall'altro, quello di comprendere, mediante un documento redatto in una lingua agevolmente accessibile dal destinatario, «how and why it contributes to outcomes that impact you»[145].

---

[143] THE WHITE HOUSE, *Blueprint for an AI Bill of Rights*, cit., 31.

[144] Si tratta, a ben vedere, di principi che ricalcano quelli contenuti nel GDPR e che rimarcano l'importanza di assicurare gli *standard* in tema di *privacy* nel corso dell'intero 'ciclo di vita' del sistema automatizzato nonché il governo dei rischi. Si rinvia a PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in ID. (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 106 ss.

[145] THE WHITE HOUSE, *Blueprint for an AI Bill of Rights*, cit., 40. Sul tema della trasparenza, v. in particolare, nella dottrina italiana, CONSULICH, "Flash offenders". *Le prospettive di* "accountability" *penale nel contrasto alle intelligenze artificiali devianti*, in *Riv. it. dir. proc. pen.*, 2022, 3, 1027, che rileva come essa presenti (quantomeno) 'due volti': «il *diritto del cittadino* di sapere *ex ante* se stia interagendo con una qualche forma di intelligenza artificiale e il *potere dell'Autorità pubblica* di ricostruirne, almeno *ex post*, i

Il progetto, tra l'altro, al fine di rimarcare la centralità di simili garanzie, riporta l'esperienza dei *software* di *predictive policing* finalizzati a identificare i potenziali autori di reati e a collocarli all'interno di una *watch list*. Ebbene, si sottolinea come il relativo utilizzo non sia stato accompagnato da alcuna spiegazione «regarding how the system came to its conclusions»[146], sebbene «both police and the public deserve to understand why and how such a system is making these determinations». Occorre dunque assicurare che gli *impacted individual* conoscano il *modus operandi* del *software*; pertanto, si raccomanda altresì l'utilizzo di sistemi che siano tali da poter essere *explainable*.

L'ultimo principio – *human alternatives, consideration and fallback* – si riferisce in sostanza alla necessità di contemplare la possibilità, per l'individuo, di non essere sottoposto al sistema automatizzato, laddove si riscontrino problemi, e di rivolgersi a una persona fisica che sia in condizione di valutarli e risolverli rapidamente. Inoltre, si specifica che i sistemi destinati a essere impiegati in ambiti sensibili (tra cui è espressamente menzionata la giustizia penale) dovrebbero, in aggiunta, essere '*tailored to the purpose*', prevedere uno spazio significativo per la supervisione, includere la formazione di tutte le persone che interagiscono con il sistema e contemplare di *default* l'intervento umano in relazione alle decisioni 'ad alto rischio' o che abbiano comunque effetti negativi sul destinatario.

Si tratta, a ben vedere, di un principio fondamentale che completa e rafforza il quadro di garanzie in precedenza tratteggiate, nella misura in cui assicura che una persona in carne e ossa possa rilevare e porre rimedio a eventuali errori del sistema che si ripercuotano sull'individuo.

In definitiva, ci sembra che l'iniziativa della Casa Bianca lasci presagire l'inizio di una nuova stagione. È infatti significativa l'adozione di un documento che, seppur non vincolante, si mostra ben consapevole delle criticità che i sistemi automatizzati pongono per i diritti fondamentali dell'individuo e prevede misure concrete in grado di ovviare a siffatte problematiche, assurgendo così a solida base di partenza per l'elaborazione di un quadro normativo.

6. Un bilancio sui *person-based systems* e un raffronto con le misure di prevenzione dell'avviso orale e dell'ammonimento del questore.

L'esame delle proposte avanzate dalla dottrina americana e dei provvedimenti che hanno tentato, a vario titolo, di disciplinare la *predictive policing* ci ha restituito un quadro nel quale emergono diverse soluzioni di interesse al fine di dare risposta alle numerose problematiche legate all'impiego di *person-based systems*.

Ci riferiamo anzitutto alla previsione di specifiche procedure per selezionare e raccogliere i dati che assicurino anche il rispetto della *privacy* nonché all'idea di

---

meccanismi di funzionamento e i processi decisionali» [il corsivo è dell'Autore].

[146] THE WHITE HOUSE, *Blueprint for an AI Bill of Rights*, cit., 42.

utilizzare gli stessi algoritmi per rilevare e contrastare le discriminazioni; alla specifica elaborazione, su suggerimento del modello COPPS, di *policies* di utilizzo, *impact report*, etc. e all'istituzione di organismi di controllo pubblico; ancora, all'esplicito riconoscimento, da parte del *Blueprint* della Casa Bianca, dell'esigenza di assicurare sempre la trasparenza circa il *modus operandi* dei sistemi in questione; e, soprattutto, alla valorizzazione della centralità del controllo umano.

Si tratta di correttivi in grado di contrastare le 'debolezze intrinseche' degli algoritmi di cui si tratta; è tuttavia l'impiego dei risultati prodotti da tali sistemi a rimanere fortemente problematico. L'esperienza, che abbiamo ripercorso, dei dipartimenti di Kansas City e Chicago ci pare emblematica. Il principale punto critico è rappresentato dai meccanismi di diffida e dalle relative conseguenze sul piano sanzionatorio; meccanismi che, per la verità, evocano istituti ben noti e da tempo presenti nel nostro sistema.

A venire in rilievo è anzitutto l'*avviso orale* di cui all'art. 3 del d.lgs. 6 settembre 2011, n. 159 (c.d. Codice Antimafia), come noto, una misura di prevenzione personale – per vero, la più blanda[147] – il cui *nomen* originario era per l'appunto quello di 'diffida'. La stessa consiste in un avviso, da parte del questore nella cui provincia la persona destinataria ha dimora, relativo alla sussistenza di indizi a suo carico, con indicazione dei motivi alla loro base, al quale si accompagna l'invito a tenere una condotta conforme alla legge.

I soggetti possibili destinatari dell'avviso[148] sono individuati mediante richiamo all'art. 1 del Codice, ovverosia coloro che per la condotta e il tenore di vita debba ritenersi, sulla base di elementi di fatto, che vivono abitualmente, anche in parte, con i proventi di attività delittuose (lett. b)) nonché coloro che per il loro comportamento debba ritenersi, sulla base di elementi di fatto (tra i quali rileva, per

---

[147] Così BASILE, *Manuale delle misure di prevenzione. Profili sostanziali*, Torino, 2020, 82, il quale ricorda che l'avviso orale è divenuto una misura di prevenzione autonoma solo nell'ambito del Codice Antimafia, mentre in passato la 'diffida' costituiva un presupposto per la successiva applicazione della sorveglianza speciale di pubblica sicurezza nei confronti dei proposti rientranti in una fattispecie di pericolosità generica, i quali, nonostante l'avvertimento, non avessero serbato una condotta conforme alla legge.

[148] Segnaliamo che, per far fronte all'esigenza di contrastare la violenza giovanile, resa impellente in considerazione di drammatici fatti di cronaca, il Governo ha adottato il d.l. 15 settembre 2023, n. 123 recante 'Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la sicurezza dei minori in ambito digitale', attraverso il quale, come si legge nel Comunicato stampa del Consiglio dei Ministri n. 49 del 7 Settembre 2023, si è inteso, *inter alia*, estendere l'applicabilità dell'avviso orale anche ai minorenni che abbiano compiuto 14 anni, mediante l'aggiunta del comma 3-*bis* all'art. 3 del Codice Antimafia, il quale stabilisce che «il questore convoca il minore, unitamente ad almeno un genitore o ad altra persona esercente la responsabilità genitoriale»; gli effetti dell'avviso cesseranno comunque al compimento della maggiore età. Inoltre, i soggetti in questione potranno incorrere, a particolari condizioni, nel divieto di possedere cellulari e altri dispositivi per le comunicazioni dati e voce. In caso di violazione delle prescrizioni connesse alla misura, anche il minorenne potrà incorrere nella sanzione penale prevista per i maggiorenni *ex* art. 76, comma 2, Codice Antimafia (reclusione da uno a tre anni e multa da euro 1.549 a euro 5.164). Il testo integrale del comunicato è accessibile al seguente link: https://www.governo.it/it/articolo/comunicato-stampa-del-consiglio-dei-ministri-n-49/23491.

espressa previsione normativa, anche la violazione di talune misure)[149], che sono dediti alla commissione di reati contro l'integrità fisica o morale dei minorenni, la sanità, la sicurezza o la tranquillità pubblica (lett. c)). Si tratta in sostanza delle ipotesi di c.d. pericolosità generica, da cui come noto è stata espunta, per effetto della sentenza n. 24/2019 della Consulta, quella di cui alla lett. a) riguardante le persone abitualmente dedite ai traffici delittuosi, in ragione della sua riscontrata carenza in punto di precisione[150].

Sebbene l'art. 3 taccia sul punto, si ritiene che la misura in esame presupponga anche una valutazione prognostica sulla pericolosità del soggetto per la sicurezza pubblica[151], intesa dalla giurisprudenza, nello specifico contesto dell'avviso orale, non necessariamente come la probabilità che questi commetta reati in futuro ma come *sospetto* «della presenza di elementi tali da ritenere la configurabilità, nel soggetto destinatario dell'avviso, di una *personalità propensa a seguire particolari comportamenti antigiuridici*»[152]. Occorre inoltre specificare che la misura si giustifica in quanto detta 'pericolosità' sia attuale[153].

Di regola, l'avviso orale (c.d. semplice)[154] non determina alcun effetto limitativo dei diritti del relativo destinatario. L'unica eccezione è rappresentata dai casi di cui all'art. 3, comma 4, a mente del quale il questore può imporre a coloro che siano stati condannati in via definitiva per un delitto non colposo alcuni specifici divieti di possedere o utilizzare, anche in parte, una serie di oggetti e apparati che

---

[149] L'art. 1, lett. c) si riferisce espressamente alle reiterate violazioni del foglio di via obbligatorio e dei divieti di frequentazione di determinati luoghi.

[150] V. Corte cost. 24 gennaio 2019, n. 24, in *Dir. pen. cont.*, 4 marzo 2019, con nota di FINOCCHIARO, *Due pronunce della Corte costituzionale in tema di principio di legalità e misure di prevenzione a seguito della Sentenza De Tommaso della Corte Edu*. Per la verità la Consulta non aveva preso una posizione circa la possibile, residua operatività dell'art. 1, lett. a) rispetto alle misure del foglio di via e dell'avviso orale, ritenendo che ciò esulasse dal suo esame, che era incentrato sulla rilevanza di tale disposto in quanto richiamato dall'art. 4 quale presupposto della sorveglianza speciale e delle misure patrimoniali. Tuttavia, in dottrina si esclude che la fattispecie di pericolosità in questione possa sopravvivere limitatamente alle misure personali più blande, v. in questo senso BASILE, *Manuale delle misure di prevenzione*, cit., 47 s.

[151] Sulla necessità di accertare tale requisito anche in materia di avviso orale v. MENDITTO, *Le misure di prevenzione personali e patrimoniali*, Milano, 2012, 47. In giurisprudenza, v. da ultimo T.a.r. Lombardia Milano, Sez. I, 2 gennaio 2023, n. 7 ove si afferma che il questore può applicare la misura in questione «in presenza di indizi tali da far ragionevolmente ritenere che, ove gli stessi non modifichino i propri comportamenti, potranno incorrere nella commissione di condotte pericolose per la sicurezza e per la tranquillità pubblica». Su questo aspetto e sulla possibilità di ricondurre la pericolosità per la pubblica sicurezza al concetto di pericolosità sociale *ex* art. 203 c.p. v. BASILE, *Manuale delle misure di prevenzione*, cit., rispettivamente, 83 e 69 ss.

[152] Così, da ultimo, T.a.r. Veneto Venezia, Sez. III, 27 marzo 2019, n. 468 [il corsivo è nostro].

[153] CHELO, Sub *Art. 3, d.lgs. n. 159/2011*, in SPANGHER-MARANDOLA (a cura di), *Commentario breve al Codice Antimafia e alle altre procedure di prevenzione*, Milano, 2019, 24 che sul punto richiama T.a.r. Campania Salerno, Sez. I, 4 dicembre 2012, n. 2191.

[154] Così CHELO, Sub *Art. 3, d.lgs. n. 159/2011*, cit., 24.

possano agevolare la sua condotta pericolosa[155] e, laddove questi siano violati, si configurerà il delitto previsto dall'art. 76, comma 2, del Codice Antimafia[156].

Quanto a possibili riflessi negativi sul trattamento sanzionatorio – nel caso in cui l'avvisato commetta reati (e lo stesso vale per ogni destinatario di una misura di prevenzione personale) – occorre guardare agli artt. 71, 72 e 73 del Codice Antimafia.

La prima delle disposizioni richiamate contempla, da un lato, una circostanza aggravante – di duplice natura, a seconda della fattispecie integrata[157] – laddove il soggetto in questione si renda responsabile di uno dei reati ivi elencati, nonché la procedibilità d'ufficio e la possibilità di procedere all'arresto fuori dei casi di flagranza (in relazione ai delitti, tra quelli richiamati, per cui è ammesso l'arresto in flagranza)[158]. Infine, si prescrive l'applicazione di una misura di sicurezza detentiva in aggiunta alla pena prevista per il reato.

L'art. 72 impone, del pari, un aggravamento di pena in relazione alle ipotesi nelle quali il sottoposto a una misura di prevenzione personale commetta reati concernenti le armi e gli esplosivi di cui agli artt. 1 e 2, commi 1 e 2, della l. 18 aprile

---

[155] Si tratta in particolare del «divieto di possedere o utilizzare, in tutto o in parte, qualsiasi apparato di comunicazione radiotrasmittente, radar e visori notturni, indumenti e accessori per la protezione balistica individuale, mezzi di trasporto blindati o modificati al fine di aumentarne la potenza o la capacità offensiva, ovvero comunque predisposti al fine di sottrarsi ai controlli di polizia, armi a modesta capacità offensiva, riproduzioni di armi di qualsiasi tipo, compresi i giocattoli riproducenti armi, altre armi o strumenti, in libera vendita, in grado di nebulizzare liquidi o miscele irritanti non idonei ad arrecare offesa alle persone, prodotti pirotecnici di qualsiasi tipo, nonché sostanze infiammabili e altri mezzi comunque idonei a provocare lo sprigionarsi delle fiamme, nonché programmi informatici ed altri strumenti di cifratura o crittazione di conversazioni e messaggi» (così art. 3, comma 4, Codice Antimafia).

[156] Cfr. Art. 76, comma 2, Codice Antimafia: «Chiunque violi il divieto di cui all'articolo 3, commi 4, 5 e 6-*bis*, è punito con la reclusione da uno a tre anni e con la multa da euro 1.549 a euro 5.164. Gli strumenti, gli apparati, i mezzi e i programmi posseduti o utilizzati sono confiscati ed assegnati alle Forze di polizia, se ne fanno richiesta, per essere impiegati nei compiti di istituto».

[157] Cfr. Art. 71, comma 1, Codice Antimafia: «Le pene stabilite per i delitti previsti dagli articoli 270 *bis*, 270 *ter*, 270 *quater*, 270 *quater*.1, 270 *quinquies*, 314, 316, 316 *bis*, 316 *ter*, 317, 318, 319, 319 *ter*, 319 *quater*, 320, 321, 322, 322 *bis*, 336, 338, 353, 377, terzo comma, 378, 379, 416, 416 *bis*, 416 *ter*, 418, 424, 435, 513 *bis*, 575, 600, 601, 602, 605, 610, 611, 612, 628, 629, 630, 632, 633, 634, 635, 636, 637, 638, 640 *bis*, 648 *bis*, 648 *ter*, del codice penale, nonché per i delitti commessi con le finalità di terrorismo di cui all'articolo 270 *sexies* del codice penale, sono aumentate da un terzo alla metà e quelle stabilite per le contravvenzioni di cui agli articoli 695, primo comma, 696, 697, 698, 699 del codice penale sono aumentate nella misura di cui al secondo comma dell'articolo 99 del codice penale se il fatto è commesso da persona sottoposta con provvedimento definitivo ad una misura di prevenzione personale durante il periodo previsto di applicazione e sino a tre anni dal momento in cui ne è cessata l'esecuzione».

[158] Cfr. Art. 71, comma 2, Codice Antimafia: «In ogni caso si procede d'ufficio e quando i delitti di cui al comma 1, per i quali è consentito l'arresto in flagranza, sono commessi da persone sottoposte alla misura di prevenzione, la polizia giudiziaria può procedere all'arresto anche fuori dei casi di flagranza».

1975, n. 110[159], mentre l'art. 73 riserva al medesimo soggetto una risposta sanzionatoria più grave nel caso di specifiche violazioni del Codice della strada[160].

Con riguardo alla revoca della misura, l'art. 3 stabilisce che essa può essere domandata dall'avvisato in qualsiasi momento e, in caso di silenzio del questore nei sessanta giorni successivi, la richiesta si intenderà accolta, secondo il meccanismo del silenzio-assenso; qualora, invece, a fronte di siffatta istanza, l'autorità pubblica emetta un provvedimento di rigetto, questo sarà impugnabile mediante ricorso gerarchico al prefetto entro sessanta giorni dalla notifica. Il destinatario dell'avviso potrà altresì avvalersi dei seguenti mezzi di impugnazione: il ricorso straordinario al Presidente della Repubblica, per soli motivi di legittimità; il ricorso al giudice amministrativo; nonché il ricorso, in via giurisdizionale, al T.a.r., poiché trattasi di atto amministrativo[161].

Circa invece i divieti annessi all'avviso orale, la medesima disposizione prescrive che questi siano opponibili davanti al tribunale in composizione monocratica[162].

Ebbene, i punti di contatto tra la misura preventiva *de qua* e la diffida prevista nell'ambito dei descritti sistemi di *predictive policing* sono innegabili: siamo, in entrambi i casi, al cospetto di un avviso eseguito dalla polizia che si articola, dapprima, in una *disclosure* di – potremmo dire genericamente – 'sospetti' a carico di un soggetto pericoloso e, successivamente, in una intimazione a non violare la legge; inoltre, alla base di ambedue le ipotesi vi è una valutazione di stampo probabilistico da cui emerga la pericolosità dell'individuo.

Tuttavia, a ben vedere, ci sembra che tra le due ipotesi ricorrano differenze tali da far emergere la problematicità dei sistemi americani.

Ricordiamo invero come nell'esperienza di Kansas City e Chicago si sia prevista la minaccia, al momento del *warning*, dell'irrogazione di pene più severe allorché l'avvisato non si astenga dal commettere (genericamente) reati.

Di contro, abbiamo visto come, benché l'avviso orale possa determinare un inasprimento sanzionatorio laddove il relativo destinatario ometta di tenere un comportamento conforme alla legge, una simile ipotesi sia circoscritta ai casi di

---

[159] Cfr. Art. 72 Codice Antimafia: «Le pene stabilite per i reati concernenti le armi alterate nonché le armi e le munizioni di cui all'articolo 1 della legge 18 aprile 1975, n. 110, sono triplicate e quelle stabilite per i reati concernenti le armi e le munizioni di cui all'articolo 2, commi primo e secondo, della stessa legge sono aumentate nella misura in cui al terzo comma dell'articolo 99 del codice penale, se i fatti sono commessi da persona sottoposta con provvedimento definitivo ad una misura di prevenzione personale durante il periodo previsto di applicazione e sino a tre anni dal momento in cui ne è cessata l'esecuzione».

[160] Cfr. Art. 73 Codice Antimafia: «Nel caso di guida di un autoveicolo o motoveicolo, senza patente, o dopo che la patente sia stata negata, sospesa o revocata, la pena è dell'arresto da sei mesi a tre anni, qualora si tratti di persona già sottoposta, con provvedimento definitivo, a una misura di prevenzione personale».

[161] V. MENDITTO, *Le misure di prevenzione*, cit., 49.

[162] Per maggiori dettagli sul punto v. CHELO, Sub *Art. 3, d.lgs. n. 159/2011*, cit., 25 s.; nonché MENDITTO, *Le misure di prevenzione*, cit., 55 s.

commissione di ben precise fattispecie di reato. In altre parole, a non convincere è il fatto che l'inflizione di una pena più grave derivi dalla commissione di *qualsiasi reato* da parte del soggetto diffidato; senza considerare poi che la sanzione può in concreto raggiungere, come dimostrato dal caso registratosi nel *Western District* del Missouri, livelli davvero sproporzionati (come quindici anni per il possesso di un *bullet*). Inoltre, il destinatario dell'avviso orale dispone di puntuali mezzi di impugnazione per contestare e, eventualmente, ottenere la revoca della misura – circostanza, questa, assente nell'esperienza oltreoceano.

Una diversa figura che merita di essere presa in esame e che, parimenti, testimonia i profili critici legati al ricorso ai sistemi di *predictive policing* americani è l'*ammonimento del questore*[163] in materia di atti persecutori, disciplinato dall'art. 8 del d.l. 23 febbraio 2009, n. 11 (convertito con modificazioni dalla l. 23 aprile 2009, n. 38, provvedimento con il quale è stato per l'appunto introdotto, nel nostro ordinamento, il delitto di cui all'art. 612-*bis* c.p.).

In particolare, la disposizione richiamata attribuisce alla persona offesa, fino a quando non è proposta querela, la facoltà di «esporre i fatti all'autorità di pubblica sicurezza avanzando richiesta al questore di ammonimento nei confronti dell'autore della condotta»[164]. Siffatta richiesta sarà poi trasmessa senza ritardo al soggetto competente, il quale, «assunte se necessario informazioni dagli organi investigativi e sentite le persone informate dei fatti, ove ritenga fondata l'istanza, ammonisce oralmente il soggetto nei cui confronti è stato richiesto il provvedimento, invitandolo a tenere una condotta conforme alla legge e redigendo processo verbale»[165]. Una copia di quest'ultimo sarà poi rilasciata alla vittima e all'ammonito.

Si tratta di una misura di prevenzione personale *sui generis*[166] poiché, pur non essendo disciplinata nell'ambito del Codice Antimafia, rappresenta una ipotesi 'speciale' di avviso orale, la cui finalità è quella di intervenire, in chiave preventiva, sul fenomeno dello *stalking*[167], attribuendo al questore un potere di diffida anticipato

---

[163] GASPARRE, *L'istituto giuridico dell'ammonimento del questore per l'appartenente alla Polizia di Stato: peculiarità e conseguenze*, in *Riv. pen.*, 2021, 4, 309 e nota 2, evidenzia si tratti di un istituto di derivazione anglosassone, riconducibile al c.d. *restraining order*, e accostabile alla misura di prevenzione dell'avviso orale.

[164] V. art. 8, comma 1, d.l. 23 febbraio 2009, n. 11 (convertito con modificazioni dalla l. 23 aprile 2009, n. 38).

[165] V. ancora art. 8, comma 2, d.l. 23 febbraio 2009, n. 11, cit.

[166] BRICCHETTI-PISTORELLI, *Istanza di ammonimento: una prima forma di tutela*, in *Guida dir.*, 2009, 10, 69 ss.; GASPARRE, *L'istituto giuridico dell'ammonimento*, cit., 315. Sostengono del pari la natura di misura di prevenzione dell'ammonimento MARANDOLA, *I profili processuali delle nuove norme in materia di sicurezza pubblica, di contrasto alla violenza sessuale e* stalking, in *Dir. pen. proc.*, 2009, 8, 964 s.; MENDITTO, *Le misure di prevenzione*, cit., 18. In giurisprudenza, v. per tutti T.a.r. Piemonte Torino, Sez. I, 2 marzo 2012, n. 290.

[167] V. sul punto MARANDOLA, *I profili processuali delle nuove norme in materia di sicurezza pubblica*, cit., 962, la quale evidenzia come l'ammonimento possa essere eseguito anche prima che le condotte persecutorie assumano rilevanza penale *ex* art. 612-*bis* c.p., proprio per fare in modo che le stesse si arrestino allo stadio iniziale.

(e alternativo) rispetto alla instaurazione del procedimento penale[168] – come del resto dimostra la previsione di un limite temporale ('fino a quando non è proposta querela') ai fini della presentazione della richiesta[169] – che, tuttavia, come vedremo a breve, può avere importanti riflessi in campo penale, sia sul piano sostanziale sia su quello processuale.

Al pari di quanto riscontrato in relazione all'avviso orale e ai due sistemi *person-based* analizzati, l'autorità pubblica (*id est*, il questore), ai fini dell'adozione della misura qui in esame, dovrà dunque effettuare una previa valutazione della pericolosità del soggetto; tuttavia – e si tratta di un aspetto che merita di essere sin da subito valorizzato – tale accertamento non rivestirà un carattere 'generale', bensì incontrerà un duplice limite, di carattere oggettivo e soggettivo. Difatti, da un lato, lo stesso non riguarderà la generica propensione del soggetto di cui si richiede l'ammonimento ad assumere comportamenti antigiuridici, bensì avrà ad oggetto la sua specifica attitudine a compiere atti persecutori; dall'altro lato, suddetto scrutinio sarà focalizzato sulla persona offesa, e non sulla generalità dei consociati, al fine di appurare se costui possa rappresentare un pericolo per chi ha presentato richiesta di ammonimento[170].

L'aspetto che tuttavia rileva maggiormente ai nostri fini riguarda la previsione, all'art. 8, comma 3, di una circostanza aggravante speciale e a effetto comune, che è integrata allorché il delitto di atti persecutori sia commesso da parte

---

[168] L'ammonimento è stato altresì esteso, ad opera del dell'art. 3 del d.l. 14 agosto 2013, n. 93 (convertito con modificazioni dalla l. 15 ottobre 2013, n. 119), ai delitti di percosse e lesioni personali commesse nell'ambito di violenza domestica. In queste ipotesi, tuttavia, il procedimento preventivo di carattere amministrativo non è alternativo bensì eventualmente cumulativo a quello giudiziario, dal momento che si prevede che il questore possa procedere 'anche in assenza di querela'. Esistono poi ulteriori differenze di disciplina, tra cui il fatto che non è richiesta l'istanza della persona offesa ai fini dell'attivazione del procedimento, ma la norma si riferisce alla segnalazione di chiunque, purché in forma non anonima. Per maggiori approfondimenti, si rinvia a GASPARRE, *L'istituto giuridico dell'ammonimento*, cit., 311 s. Ancora, l'art. 7 della l. 29 maggio 2017, n. 71 ha previsto l'ammonimento anche in materia di cyberbullismo. Da ultimo, il d.l. n. 123/2023 (v. *supra* nota n. 148), all'art. 5, commi 2-4, ha esteso l'ammonimento in materia di *stalking* «fino a quando non è proposta querela o non è presentata denuncia per taluno dei reati di cui agli articoli 581, 582, 610, 612 e 635 del codice penale, commessi da minorenni di età superiore agli anni quattordici nei confronti di altro minorenne». Inoltre, il provvedimento (art. 5, commi 5-7) ha previsto la medesima estensione nei confronti dei minori di età compresa tra i 12 e i 14 anni che commettano delitti puniti con la reclusione non inferiore nel massimo a cinque anni. In entrambi i casi, si prescrive che il questore convochi il minore, unitamente ad almeno un genitore (o chi esercita la responsabilità genitoriale), e gli effetti dell'ammonimento cessano comunque al compimento della maggiore età. Infine, ai sensi del comma 8, si commina la sanzione amministrativa pecuniaria da 200 euro a 1.000 euro «nei confronti del soggetto che era tenuto alla sorveglianza del minore o all'assolvimento degli obblighi educativi nei suoi confronti», salvo che non provi di non aver potuto impedire il fatto.

[169] V. MARANDOLA, *I profili processuali delle nuove norme in materia di sicurezza pubblica*, cit., 962 che osserva come ciò sia indicativo del fatto che il procedimento di ammonimento precede l'attività processuale in senso stretto disciplinata dal codice di procedura penale (artt. 330 e ss.); v. anche GASPARRE, *L'istituto giuridico dell'ammonimento*, cit., 310 che parla al riguardo di un 'doppio binario' di tutela, penale e amministrativa.

[170] Con riferimento a tale specifico aspetto, v. GASPARRE, *L'istituto giuridico dell'ammonimento*, cit., 314.

del soggetto già ammonito; inoltre, in tale ipotesi, muta, ai sensi del comma 4, il regime di procedibilità (non più a querela della persona offesa, bensì d'ufficio)[171].

Peraltro, in dottrina è stato opportunamente evidenziato che, sebbene la disciplina dell'ammonimento nulla dica al riguardo, è necessario circoscrivere l'operatività dell'aggravante in questione ai casi in cui il reato di *stalking* sia poi realizzato dal soggetto diffidato *a danno della stessa persona* che ha presentato la richiesta di ammonimento; diversamente, si configurerebbe una «forma di recidiva 'impropria', in spregio di quella che sembrerebbe essere la volontà legislativa»[172]. Allo stesso modo, la procedibilità d'ufficio deve essere vincolata alla «identità dei fatti per i quali si procede a quelli per cui è stato eseguito l'ammonimento»[173].

Come si vede, sussiste dunque una *stretta correlazione* tra ammonimento e successiva commissione del delitto di cui all'art. 612-*bis* c.p., nella misura in cui si prevede che l'aggravamento di pena e il mutamento del regime di procedibilità conseguano alla realizzazione delle condotte persecutorie da parte del *soggetto già ammonito* (e nei confronti della *persona offesa che ha chiesto l'ammonimento*). Una simile circostanza, unitamente alle illustrate peculiarità dello scrutinio di pericolosità, ci induce a ritenere che la previsione di un trattamento sanzionatorio più gravoso – nonché della procedibilità d'ufficio – non sollevi i delicati problemi posti dai meccanismi di diffida alla base dei sistemi di *predictive policing* impiegati a Kansas City e Chicago.

Occorre inoltre precisare che proprio in considerazione delle possibili ricadute dell'ammonimento nei confronti del destinatario, che consentono di qualificarlo come un provvedimento amministrativo immediatamente lesivo, la giurisprudenza maggioritaria riconosce la possibilità a tale soggetto di impugnarlo davanti agli organi di giustizia amministrativa, in quanto titolare di un interesse concreto e attuale[174]. Ebbene, ci pare che questa rappresenti un'altra condizione imprescindibile per legittimare l'applicazione di un trattamento sanzionatorio più severo a fronte dell'inosservanza dell'intimazione dell'autorità pubblica.

In definitiva, ci sembra che questo raffronto con l'avviso orale e l'ammonimento in materia di atti persecutori faccia chiaramente emergere le criticità

---

[171] V. art. 8, commi 3 e 4, d.l. 23 febbraio 2009, n. 11, cit.: «3. La pena per il delitto di cui all'articolo 612 *bis* del codice penale è aumentata se il fatto è commesso da soggetto già ammonito ai sensi del presente articolo. 4. Si procede d'ufficio per il delitto di cui all'articolo 612 *bis* del codice penale quando il fatto è commesso da soggetto già ammonito ai sensi del presente articolo».

[172] Così MARANDOLA, *I profili processuali delle nuove norme in materia di sicurezza pubblica*, cit., 965 s.; v. altresì BRICCHETTI-PISTORELLI, *Istanza di ammonimento*, cit., 70.

[173] V. ancora MARANDOLA, *I profili processuali delle nuove norme in materia di sicurezza pubblica*, cit., 966 nonché BRICCHETTI-PISTORELLI, *Istanza di ammonimento*, cit., 70.

[174] In questo senso, v., *ex multis*, T.a.r. Calabria Reggio Calabria, Sez. I, 4 novembre 2010, n. 1171; T.a.r. Liguria, 12 gennaio 2010, n. 31. In dottrina, v. in particolare GASPARRE, *L'istituto giuridico dell'ammonimento*, cit., 314; D'ARIENZO, *La prevenzione del reato di* stalking. *Limiti all'esercizio del potere di ammonimento orale: il sindacato giurisdizionale ed i poteri istruttori del giudice amministrativo*, in *Giur. it.*, 2012, 11, 2423. *Contra*, v. T.a.r. Sicilia Palermo, Sez. I, 31 marzo 2011, n. 605; T.a.r. Sicilia Palermo, Sez. I, 13 aprile 2010, n. 4957.

dei meccanismi di diffida previsti nel contesto dei *person-based systems* americani. Al contempo, però, all'esito di tale analisi, è possibile intravedere alcuni ambiti – quelli cioè delle suddette misure di prevenzione questorili – nei quali si potrebbe ipotizzare l'uso di *risk assessment tools*.

È venuto dunque il momento di interrogarci sulle condizioni che potrebbero legittimare l'ingresso di questi strumenti nel nostro ordinamento.

Per disporre tuttavia di un quadro completo, dobbiamo prima confrontarci con lo scenario eurounitario, ove già da tempo le istituzioni e diversi organismi sono impegnati sul delicato fronte dell'elaborazione di una disciplina che governi l'uso dell'intelligenza artificiale.

7. Le prospettive di regolamentazione a livello eurounitario: tra *hard law* e *soft law*.

La *predictive policing*, seppur nata negli Stati Uniti, ha registrato nel tempo un'evoluzione anche nel continente europeo[175], attirando pertanto l'attenzione e le preoccupazioni delle istituzioni circa i suoi possibili effetti distorsivi. Negli ultimi anni invero si è assistito al proliferare di strumenti di *soft law*[176] e studi volti a sensibilizzare i diversi operatori coinvolti a un uso consapevole di siffatti sistemi e, in generale, degli algoritmi predittivi in campo penale. Si è trattato di strumenti che, seppur privi dell'efficacia propria degli atti normativi in senso stretto, hanno offerto un importante contributo all'identificazione dei limiti e dei rischi, specie per i diritti fondamentali dell'individuo, che queste nuove tecnologie presentano e che meritano di essere presi in seria considerazione.

Il riferimento è anzitutto alla *Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e nei relativi ambienti*, emanata dalla Commissione europea per l'efficacia della giustizia (CEPEJ) il 4 dicembre 2018[177] e definita come un

---

[175] V. MUGARI-OBIOHA, *Predictive Policing and Crime Control*, cit., 7 s. che riporta l'esempio tedesco di PRECOBS e altri *software*, nonché le applicazioni pratiche utilizzate in Olanda e nel Regno Unito. V. inoltre il fascicolo della *Revue Internationale de Droit Pénal*, 2023 (https://www.penal.org/en/2023-0), contenente una rassegna dell'esperienza di diversi Paesi circa la diffusione dell'AI nell'amministrazione della giustizia penale (e, dunque, della *predictive policing*): tra gli altri, per quanto riguarda, l'Italia, v. GIALUZ-QUATTROCOLO, *AI and the Administration of Criminal Justice in Italy*, in *Revue Internationale de Droit Pénal*, 2023, 1 ss.

[176] Sulla sempre più marcata diffusione della *soft law* e sul suo ruolo nel diritto penale nonché per ulteriori riferimenti di carattere generale, v. BERNARDI, *Sui rapporti tra* soft law *e diritto penale*, in *Riv. it. dir. proc. pen.*, 2011, 536 ss.

[177] COMMISSIONE EUROPEA PER L'EFFICIENZA DELLA GIUSTIZIA (CEPEJ), *Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi*, 3 dicembre 2018. Essa si rivolge «agli attori pubblici e privati incaricati di creare e lanciare strumenti e servizi di intelligenza artificiale relativi al trattamento di decisioni e dati giudiziari (apprendimento automatico o qualsiasi altro metodo derivante dalla scienza dei dati)», nonché ai *policy-makers* chiamati a disciplinare lo sviluppo e l'uso di siffatti strumenti.

«emblematico esempio di *soft law*»[178], la quale fissa una griglia di (cinque) principi fondamentali che assumo rilievo anche nel contesto qui in esame.

Al di là della centralità del primo di essi – che attiene al *rispetto dei diritti fondamentali* nella elaborazione e attuazione dei sistemi di intelligenza artificiale[179] – assume una portata particolarmente incisiva rispetto alla polizia predittiva il (secondo) principio di *non discriminazione*, volto a «prevenire specificamente lo sviluppo o l'intensificazione di qualsiasi discriminazione tra persone o gruppi di persone»[180]. Invero, sappiamo bene come i sistemi in analisi presentino una potenzialità discriminatoria che, quindi, deve essere contrastata anzitutto attraverso il controllo sia nella fase dell'elaborazione che in quella dell'utilizzo, specialmente quando il trattamento si basa direttamente o indirettamente su dati sensibili, quali quelli relativi all'origine razziale o etnica, alle condizioni socio-economiche, etc. Inoltre, qualora si rilevino *bias*, la Carta sottolinea la necessità di prevedere apposite «misure correttive al fine di limitare o, se possibile, neutralizzare tali rischi e sensibilizzare gli attori»[181], suggerendo altresì di utilizzare l'apprendimento automatico proprio per individuare ed eliminare le possibili discriminazioni.

Anche il terzo principio, di *qualità e sicurezza*, funge da guida nel contesto di nostro interesse, imponendo di utilizzare, in relazione «al trattamento di decisioni e dati giudiziari, fonti certificate e dati intangibili con modelli elaborati multidisciplinarmente, in un ambiente tecnologico sicuro»[182]. Abbiamo invero cercato di rimarcare, nel corso della nostra analisi, l'importanza della qualità dei dati nonché i rilevanti rischi per gli individui rappresentati dall'impiego dei *dirty data*; ed è proprio sulla necessità di una accorta selezione degli *input* che la CEPEJ appunta l'attenzione[183].

Il quarto principio è alquanto articolato e si riferisce a *trasparenza*, *imparzialità* ed *equità*, alludendo espressamente alla necessità di «rendere le metodologie di trattamento dei dati accessibili e comprensibili [nonché di] autorizzare verifiche esterne»[184]. La stessa nota esplicativa si mostra ben consapevole della contrapposizione tra gli interessi economici delle aziende produttrici dei *software*, che reclamano la tutela del segreto industriale, e le esigenze di «trasparenza (accesso al

---

[178] Così QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *Leg. pen.*, 18 dicembre 2018, 2.

[179] COMMISSIONE EUROPEA PER L'EFFICIENZA DELLA GIUSTIZIA (CEPEJ), *Carta etica europea*, cit., 7.

[180] COMMISSIONE EUROPEA PER L'EFFICIENZA DELLA GIUSTIZIA (CEPEJ), *Carta etica europea*, cit., 8.

[181] COMMISSIONE EUROPEA PER L'EFFICIENZA DELLA GIUSTIZIA (CEPEJ), *Carta etica europea*, cit., 8.

[182] COMMISSIONE EUROPEA PER L'EFFICIENZA DELLA GIUSTIZIA (CEPEJ), *Carta etica europea*, cit., 10.

[183] Dalla nota esplicativa si ricava altresì che tale principio impone l'esigenza di ricostruire e controllare *ex post* il percorso seguito dall'algoritmo, al fine di appurare l'assenza di alterazioni. A questo si ricollega, in particolare, il canone della sicurezza, nel senso che i modelli e gli algoritmi elaborati devono poter essere memorizzati ed eseguiti in ambienti sicuri, in modo da garantire l'integrità e l'intangibilità del sistema. Inoltre, la Carta raccomanda la costituzione di 'squadre di progetto miste' (che riuniscano competenze tecnologiche, giuridiche e sociali) per la produzione dei sistemi, in modo da sfruttare al meglio il sapere multidisciplinare.

[184] COMMISSIONE EUROPEA PER L'EFFICIENZA DELLA GIUSTIZIA (CEPEJ), *Carta etica europea*, cit., 11.

processo creativo), imparzialità (assenza di pregiudizi), equità e integrità intellettuale (privilegiare gli interessi della giustizia)»[185], invitando alla ricerca di un equilibrio e prospettando la soluzione ritenuta preferibile, ovverosia la totale trasparenza tecnica, accompagnata dalla spiegazione, con un linguaggio chiaro e familiare, del processo seguito dall'algoritmo. Quest'ultima precisazione è molto importante poiché, come è stato sottolineato in letteratura, anche allorché il *reverse engeneering* sia possibile, soltanto gli esperti saranno in grado di comprendere le informazioni a disposizione[186], che rimangono oscure per gli effettivi destinatari dell'*outcome* algoritmico. A tal fine, la stessa Carta prospetta la possibilità di istituire autorità o esperti indipendenti incaricati di verificare le metodologie di trattamento, di fornire una consulenza preventiva ovvero di rilasciare vere e proprie certificazioni, che tuttavia dovrebbero poi essere riesaminate secondo una cadenza prestabilita.

Veniamo così all'ultimo e fondamentale principio, ovverosia quello del *controllo da parte dell'utilizzatore*[187], orientato al dichiarato fine di «precludere un approccio prescrittivo e assicurare che gli utilizzatori siano attori informati e abbiano il controllo delle loro scelte»[188]. In altre parole, come si specifica nella nota esplicativa, l'impiego dell'intelligenza artificiale deve accrescere, rafforzare l'autonomia dell'uomo, e mai limitarla.

Sebbene la Carta declini questo principio in relazione alle decisioni giudiziarie, riteniamo che esso valga rispetto a ogni impiego degli algoritmi predittivi e, dunque, anche nel campo della *predictive policing*. Gli agenti di polizia insomma non devono appiattirsi sulle risultanze algoritmiche – con tutti i rischi che ne derivano in caso di predizioni errate o discriminatorie – ma devono sfruttarle, nell'esercizio delle proprie funzioni investigative, come fonti di ampliamento del proprio panorama informativo.

In definitiva, riteniamo che una legislazione in materia di polizia predittiva non possa prescindere da nessuno dei principi consacrati nella Carta che, unitamente ad ulteriori accorgimenti, ben potrebbero, come meglio diremo[189], autorizzare un uso di questi sistemi conforme ai diritti fondamentali dell'individuo.

Di interesse ai nostri fini è altresì, nel panorama europeo, lo studio *'Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights'*[190]. Come evoca lo stesso titolo, esso è volto ad analizzare l'impatto dell'intelligenza artificiale sui diritti

---

[185] COMMISSIONE EUROPEA PER L'EFFICIENZA DELLA GIUSTIZIA (CEPEJ), *Carta etica europea*, cit., 11.

[186] QUATTROCOLO, *Intelligenza artificiale e giustizia*, cit., 8.

[187] Valorizza questo principio SEVERINO, *Le implicazioni dell'intelligenza artificiale*, cit., 101.

[188] COMMISSIONE EUROPEA PER L'EFFICIENZA DELLA GIUSTIZIA (CEPEJ), *Carta etica europea*, cit., 12.

[189] V. *infra* § 8.

[190] Il documento è stato elaborato, nel luglio 2020, dalla Prof.ssa Gloria González Fuster della Vrije Universiteit Brussel su commissione del *Policy Deparment for Citizens' Rights and Constitutional Affairs* del Parlamento europeo: v. GONZÁLEZ FUSTER, *Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights*, Policy Deparment for Citizens' Rights and Constitutional Affairs – European Parliament, 2020 (https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2020)656295).

fondamentali, così come consacrati nel diritto dell'Unione europea, nel campo delle attività di *law enforcement* e della giustizia penale[191].

In questa sede, ciò che preme evidenziare sono, in particolare, le conclusioni cui si perviene circa l'incidenza dei *software* di polizia predittiva sui diritti dell'individuo nonché i suggerimenti rivolti ai *policy-makers*.

Quanto al primo profilo, il documento mette anzitutto in evidenza come l'uso dell'intelligenza artificiale nelle attività di *law enforcement* possa seriamente compromettere il diritto alla *privacy* e alla *data protection*, poiché – come ha più volte ricordato la Corte europea dei diritti dell'uomo (Corte Edu) – la possibilità per i governi di acquisire un profilo dettagliato degli aspetti più intimi della quotidianità delle persone, raccogliendo diversi tipi di dati, può comportare interferenze particolarmente invasive nella sfera personale dell'individuo[192].

Il documento sottolinea altresì come simili interferenze potrebbero avere contemporaneamente un impatto negativo diretto sulla libertà di espressione e di informazione (*ex* art. 11 della Carta di Nizza), nonché sulla libertà di riunione e di associazione (art. 12 della Carta di Nizza), allorché i sistemi di intelligenza artificiale siano utilizzati per il monitoraggio degli spazi pubblici (il riferimento è al riconoscimento facciale in tempo reale) e delle comunicazioni, ad esempio nei *social*

---

[191] La prima parte delinea sinteticamente il quadro giuridico applicabile nel contesto in questione, derivante dalla normativa, primaria e secondaria, dell'Unione europea e da quella del Consiglio d'Europa (Convenzione europea sui diritti dell'uomo – CEDU – e Convenzione sul trattamento automatizzato – c.d. Convenzione 108+). La seconda parte offre invece una panoramica dello stato dell'arte delle applicazioni dell'intelligenza artificiale con particolare riguardo alla *predictive policing*, al riconoscimento facciale, all'uso di algoritmi nell'amministrazione della giustizia penale nonché alle frontiere. A tale ampia disamina di carattere ricognitivo, segue una minuziosa indagine sull'incidenza di queste tendenze sui *fundamental rights* e, in particolare, sul diritto alla *privacy* e alla protezione dei dati personali, sulle libertà di espressione, informazione, riunione e associazione, sulla non discriminazione, sul *right to an effective remedy and to a fair trial*, nonché, infine, sui diritti del minore. Lo studio si conclude con il resoconto dei risultati della ricerca e con alcune raccomandazioni alle istituzioni.

[192] Con specifico riferimento al tema di nostro interesse, lo studio si sofferma sui sistemi di *risk scoring* impiegati dalle autorità pubbliche, richiamando una pronuncia della Corte distrettuale dell'Aia (The Hague District Court, 5 February 2020, case number C/09/550982) concernente uno strumento di questo genere, impiegato dal governo olandese per combattere le frodi attraverso la preventiva identificazione di soggetti 'a rischio'. Qui emergono preoccupazioni relative al rispetto del diritto alla *data protection*, nel caso di specie compromesso poiché la disciplina non forniva informazioni chiare sui dati che giustificavano il punteggio di alta rischiosità, né indicazioni dettagliate sul metodo di analisi e sul funzionamento del sistema, così violando il principio secondo cui l'interessato deve ragionevolmente essere in grado di tracciare i propri dati personali. È interessante notare che uno dei parametri per valutare la compatibilità dei *software* è l'art. 8 CEDU, che sancisce il diritto al rispetto della vita privata e ammette interferenze soltanto laddove esse siano necessarie e proporzionate rispetto allo scopo previsto. In tal senso, la Corte ha osservato che, all'esito di un esame alla luce dei principi fondamentali del trattamento dei dati stabiliti dalla Carta dei diritti fondamentali dell'Unione europea (c.d. Carta di Nizza) e dal GDPR – in particolare, i principi di trasparenza, limitazione delle finalità e minimizzazione dei dati – il sistema in questione non era sufficientemente trasparente e verificabile. Questi ultimi rilevi ci sembrano porre questioni di spessore anche sul terreno dei *person-based* e meritano, dunque, di essere attentamente considerati allorché si tratti di verificare la legittimità di un determinato strumento.

media[193]. Tuttavia, simili preoccupazioni potrebbero riguardare anche la polizia predittiva, se consideriamo ad esempio l'esperienza del sistema LASER a Los Angeles ove i dati sui soggetti a rischio raccolti venivano poi inseriti in una piattaforma investigativa digitale per monitorare la criminalità[194].

Ad ogni modo, l'ambito in cui, secondo lo studio, vengono maggiormente in considerazione i potenziali impatti negativi della polizia predittiva è quello dei rischi di discriminazione, definiti in generale come una delle *most pressing challenges of the use of new technologies*[195]. Nello specifico, si rivela cruciale il fatto che il *software* predittivo possa prendere in esame variabili come la storia criminale e il *background* familiare, le quali possono far sì che il comportamento passato di un certo gruppo decida il destino di un individuo[196].

Per altro verso, i redattori dello studio, proprio sulla base della prassi applicativa statunitense in materia di *predictive policing*, rimarcano l'importanza della qualità o, meglio, della *neutralità* dei dati di cui si alimenta l'algoritmo, ribadendo la necessità di procedere a una selezione accurata[197].

L'ultimo profilo di nostro interesse è quello dedicato all'incidenza delle nuove tecnologie sui diritti dei minori, soprattutto nei casi in cui i sistemi di *predictive policing* raccolgano dati relativi a tali soggetti[198]. Al riguardo, si sottolineano i rischi per il loro processo di libera crescita in una società democratica che merita, invero, di essere preservato.

Il lavoro si conclude con alcune raccomandazioni che riprendono temi, come visto, presenti nel dibattito in materia e che trovano eco altresì nei contenuti della proposta di *AI Act*[199].

La prima raccomandazione invita i legislatori a esaminare le possibili lacune e inefficienze della normativa europea sulla protezione dei dati, così come le leggi nazionali di attuazione, nella prospettiva della loro operatività nelle attività di *law enforcement* (e non solo) a tutela degli individui, atteso che, a giudizio dello studio,

---

[193] GONZÁLEZ FUSTER, *Artificial Intelligence and Law Enforcement*, cit., 40.

[194] V. *supra* § 2.1.1.

[195] GONZÁLEZ FUSTER, *Artificial Intelligence and Law Enforcement*, cit., 40.

[196] Secondo lo studio, così si trascura il fatto che ogni essere umano è unico, con il pericolo di creare '*echo chambers*' al cui interno i pregiudizi preesistenti potrebbero essere ulteriormente rafforzati.

[197] GONZÁLEZ FUSTER, *Artificial Intelligence and Law Enforcement*, cit., 41, ove si segnala che i *software* basati sui dati relativi a reati passati rischiano di generare predizioni errate, poiché questi costituiscono un *report* soltanto parziale degli interventi della polizia. Anche i sistemi che non sembrano utilizzare alcun dato personale possono avere un impatto negativo, ad esempio, allorché le previsioni sugli *hot spot* determino controlli eccessivi in certi quartieri e, di conseguenza, la definizione di profili etnici o sociali dei gruppi che vi abitano.

[198] GONZÁLEZ FUSTER, *Artificial Intelligence and Law Enforcement*, cit., 43 s. Ciò è avvenuto in relazione al *software Gang Violence Matrix*, utilizzato dalla *Metropolitan Police* di Londra per identificare e valutare il livello di pericolosità dei membri delle bande coinvolti in episodi di violenza (v. p. 23 s.).

[199] V. *infra* § 7.2.

l'attuale quadro giuridico dell'Unione europea in materia di *data protection* non offre sufficienti garanzie per gli individui rispetto all'uso dei *software* in questione[200].

Le altre raccomandazioni attengono alla realizzazione di interventi *ad hoc* rispetto ai versanti più sensibili della materia: è il caso della trasparenza, che per essere efficacemente assicurata, richiede, ad esempio, *impact assessments* ad ampio spettro, con il coinvolgimento attivo dei gruppi e degli individui che potrebbero subire gli effetti negativi derivanti dall'impiego dei *software*[201]. Analogamente, si raccomanda fortemente l'introduzione di una normativa dedicata all'*algorithmic decision-making for law enforcement purposes*.

Raccomandazioni ancora più puntuali sono contenute nel *report*[202] del 2020 dell'*European Union Agency for Fundamental Rights* (FRA)[203], che si concentra dapprima su un'analisi dei rischi in punto di rispetto dei diritti fondamentali nell'ambito della polizia predittiva e di altri settori (servizi sociali, diagnosi medica e pubblicità mirata)[204], per poi rivolgersi ai *policy-makers*.

La premessa – comune agli atti sin qui esaminati – è che i moderni strumenti rispettino tutti i diritti fondamentali, così come sanciti nella Carta di Nizza e nei Trattati dell'Unione europea, che vengono in rilievo a seconda del contesto in cui l'intelligenza artificiale è impiegata.

In secondo luogo, si suggerisce di valutare preventivamente l'impatto dei *tools* in questione sui *fundamental rights* per ridurre gli effetti negativi (ad esempio attraverso *checklists*) nonché di prevedere un sistema di controllo efficace e affidabile per monitorare e, se necessario, gestire simili 'incidenti', anche avvalendosi delle strutture già esistenti (si pensi, a titolo esemplificativo, alle *Data Protection Authorities*) e assicurando che i suddetti organismi siano dotati di risorse e poteri adeguati, oltre che, soprattutto, del necessario *expertise* per prevenire eventuali violazioni e fornire un supporto effettivo alle vittime.

Non poteva poi mancare nel documento un invito a contrastare il rischio di discriminazioni, mediante la previsione di controlli preventivi dei *software* e lo

---

[200] Ciò in quanto accade alternativamente che: le garanzie generali previste dal GDPR non si applicano necessariamente quando il trattamento avviene per tali finalità in virtù di restrizioni e deroghe; la *Law Enforcement Directive*, che potrebbe essere lo strumento pertinente applicabile, prevede garanzie simili a quelle del GDPR, ma non pienamente equivalenti, oltre al fatto che possono esservi limitazioni alla sua operatività (v. GONZÁLEZ FUSTER, *Artificial Intelligence and Law Enforcement*, cit., 67 s.)

[201] GONZÁLEZ FUSTER, *Artificial Intelligence and Law Enforcement*, cit., 68. Un simile requisito richiama alla mente il *public oversight* previsto nelle *Local Surveillance Technology Oversight Ordinances*, v. *supra* § 5.

[202] Per un primo commento al *report* sia consentito rinviare a PIETROCARLO, *Intelligenza artificiale e diritti fondamentali*, in www.criminaljusticenetwork.eu, 15 febbraio 2021. Riferimenti a quest'ultimo emergono anche in SEVERINO, *Le implicazioni dell'intelligenza artificiale*, cit., 98.

[203] Si tratta di un organismo indipendente deputato a diffondere la cultura *fundamental rights-oriented* nei diversi Paesi membri.

[204] Tale analisi è stata effettuata grazie a oltre cento interviste di esponenti di organizzazioni pubbliche e private nonché di esperti – tra cui appartenenti ad autorità di vigilanza, organizzazioni non governative e avvocati – che, nelle rispettive attività lavorative, si confrontano a vario titolo con l'utilizzo di strumenti governati da AI.

sfruttamento della stessa intelligenza artificiale per rilevare e minimizzare il suo potenziale discriminatorio.

Quanto al tema della *data protection*, l'Agenzia europea riscontra problematicamente un diffuso *deficit* di conoscenza della normativa in materia da parte di coloro che impiegano tali strumenti e invita, pertanto, le istituzioni a colmare questa lacuna, mentre ritiene soddisfacenti le misure di tutela di cui alla *Law Enforcement Directive*[205].

Un aspetto centrale – peraltro oggetto di attenzione tanto nella Carta etica della CEPEJ, quanto nello studio commissionato dal Parlamento europeo – attiene all'esigenza di prevedere rimedi alle possibili ripercussioni negative dell'intelligenza artificiale sull'individuo, facendo sì che questi possa rivolgersi alle autorità giudiziarie nazionali per contestare le decisioni algoritmiche e che tale possibilità sia *'effective in practice as well as in law'*, senza che il segreto industriale possa rappresentare un ostacolo. Si suggerisce quindi l'elaborazione, da parte delle istituzioni eurounitarie e degli Stati membri, di linee guida volte a garantire la trasparenza in questo settore nonché l'introduzione di un obbligo, a carico delle organizzazioni pubbliche e private che impiegano *AI systems*, di fornire, alle vittime di violazioni, informazioni circa il funzionamento degli strumenti utilizzati.

Va infine menzionata la Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale[206], che, nel richiedere un divieto permanente rispetto all'utilizzo dei sistemi di analisi e/o riconoscimento automatici negli spazi pubblici nonché una moratoria sulla diffusione dei sistemi di riconoscimento facciale con funzione di identificazione[207], ha rivolto la propria attenzione anche al tema di nostro interesse.

Al di là di importanti affermazioni contenute nei Considerando[208], analizzando il cuore del disposto della Risoluzione, è possibile intravedere un certo

---

[205] Per la relativa analisi, si rinvia a *infra* § 7.1.

[206] Per un commento, v. VALSECCHI, *L'intelligenza artificiale nel diritto penale: la Risoluzione del Parlamento europeo del 6 ottobre 2021*, in *MediaLaws*, 1° febbraio 2022; v. altresì BARONE, *Intelligenza artificiale e processo penale: la linea dura del Parlamento europeo. Considerazioni a margine della risoluzione del Parlamento europeo del 6 ottobre*, in *Cass. pen.*, 2022, 1180 ss.

[207] V., rispettivamente, PARLAMENTO EUROPEO, *Risoluzione del Parlamento europeo del 6 ottobre 2021*, cit., §§ 26 e 27.

[208] Già all'*incipit* della Risoluzione (Considerando A), ci si imbatte subito in una precisazione fondamentale, che dovrebbe sempre fungere da premessa allorché si discuta di AI (e, in generale, di algoritmi): quest'ultima «non dovrebbe essere vista come fine a [sé] stessa, ma come uno *strumento* al servizio delle persone»[208]. Ciò significa che, laddove sia impiegata per la prevenzione della criminalità, l'AI deve essere funzionale al miglior esercizio dei compiti affidati al singolo agente di polizia e non sostituirsi ad esso. Occorre pertanto adottare un approccio critico e antropocentrico, alla ricerca di un continuo bilanciamento tra le opportunità che la tecnologia offre e il rispetto dei diritti fondamentali dell'individuo. Un ulteriore, importante monito, lo ritroviamo al Considerando Q, ove il Parlamento paventa il rischio che, con il ricorso a questi sistemi, si stravolga l'essenza del moderno diritto penale, basato «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».

parallelismo[209] con la proposta di *Artificial Intelligence Act* della Commissione nella misura in cui, seguendo l'approccio *risk-based* dei sistemi di intelligenza artificiale, classifica gli strumenti destinati a essere utilizzati dalle autorità di contrasto per effettuare valutazioni individuali di pericolosità delle persone fisiche al fine di determinare il rischio di reato o recidiva in relazione a una persona fisica o il rischio per vittime potenziali di reati tra quelli 'ad alto rischio'.

La Risoluzione specifica poi che, in campo penale, qualsiasi *tool* deve essere 'come minimo' sicuro e adatto allo scopo previsto; deve inoltre rispettare i principi di equità, minimizzazione dei dati, responsabilità, trasparenza, non discriminazione e spiegabilità; ancora, il suo sviluppo, la sua diffusione e il suo utilizzo devono essere soggetti a una valutazione dei rischi e una verifica di necessità e proporzionalità, con l'ulteriore previsione di salvaguardie proporzionate ai rischi individuati[210]. Questi aspetti sono poi dettagliatamente affrontati nel prosieguo della Risoluzione[211].

Delineato il quadro dei principali rischi legati all'uso dell'intelligenza artificiale nel settore penale e identificate le misure che devono essere implementate per minimizzarli, il Parlamento dedica un paragrafo *ad hoc* alla polizia predittiva[212], mostrando tutte le sue perplessità. In particolare, in virtù della non completa affidabilità delle predizioni che simili *software* possono elaborare, ritiene che questa non possa «costituire l'unica base per un intervento». Inoltre, in considerazione dell'esperienza applicativa statunitense che ha messo a nudo gli impatti lesivi dei *tools* sui diritti fondamentali, conducendo – come si è visto[213] – a una loro dismissione, la Risoluzione si oppone all'utilizzo, da parte delle forze dell'ordine, di quei sistemi che elaborano «previsioni sui comportamenti degli individui o di gruppi sulla base di dati

---

[209] V. VALSECCHI, *L'intelligenza artificiale nel diritto penale*, cit., che sottolinea come vi siano dei 'punti di contatto' tra i due atti.

[210] V. PARLAMENTO EUROPEO, *Risoluzione del Parlamento europeo del 6 ottobre 2021*, cit., § 4.

[211] Quanto al tema della sicurezza, il Parlamento sottolinea la necessità di predisporre misure protettive adeguate e idonee a prevenire attacchi dolosi, a partire dalla fase di progettazione del *tool* (c.d. *security-by-design*), oltre alla previsione di un *controllo umano preventivo* per testare la solidità delle applicazioni. Circa le potenzialità discriminatorie dell'AI, si punta l'attenzione sull'importanza di alimentare il sistema con dati neutri, evitando così che l'uso degli strumenti di AI in campo penale determini disuguaglianze. In considerazione dei possibili effetti distorsivi dei sistemi in esame, la Risoluzione mette l'accento sull'*accountability*, ossia sull'esigenza che la relativa responsabilità ricada sempre su una persona fisica o giuridica individuabile e che esista uno 'specifico quadro giuridico chiaro e preciso', affinché possa essere assicurato l'esercizio del diritto di difesa e il diritto di accesso a un giudice. A ciò si riconnettono la trasparenza e la *explainability* degli algoritmi – logici presupposti della possibilità di contestare la decisione automatizzata –, da assicurare attraverso l'acquisto, mediante una procedura di appalto appropriata, dei soli sistemi suscettibili di revisione e, possibilmente, l'impiego di *software open source*. Ulteriori cautele, per così dire, procedimentali sono individuate in una previa valutazione di impatto obbligatoria sui diritti fondamentali affidata, ad esempio, alle autorità preposte alla *data protection* e nell'introduzione di *audit* periodici, per testare la capacità di individuare e correggere anomalie. Infine, si sancisce l'imprescindibilità del controllo umano nell'assunzione di decisioni che producono 'effetti giuridici o analoghi'.

[212] V. PARLAMENTO EUROPEO, *Risoluzione del Parlamento europeo del 6 ottobre 2021*, cit., § 24.

[213] V. *supra* § 2.1.1.

storici e condotte precedenti, dell'appartenenza a un gruppo, l'ubicazione e qualsiasi altra caratteristica al fine di identificare le persone che potrebbero commettere un reato».

Rispetto a questi sistemi, sembrerebbe che l'organo europeo ravvisi criticità in punto di rispetto dei diritti fondamentali dell'individuo insuperabili, che non sono controbilanciate dal conseguimento di effettivi vantaggi per l'efficacia delle attività di *law enforcement*, poiché dalla prassi è emerso chiaramente che il pericolo di previsioni inaffidabili è tutt'altro che remoto. Si tratta di rilievi che hanno progressivamente acquisito sempre maggior peso, se si considera che il dibattito in corso sulla proposta di Regolamento sull'intelligenza artificiale sembra militare proprio verso questa direzione.

7.1. La c.d. Law Enforcement Directive.

Il quadro normativo sin qui ricostruito è relativo agli strumenti di *soft law*, vi sono tuttavia anche strumenti di *hard law* che, pur non occupandosi *ex professo* dei sistemi di *predictive policing*, si ritiene possano trovare applicazione nel campo in esame.

Il primo di essi è la Direttiva UE/2016/680 (c.d. *Law Enforcement Directive*)[214], che si colloca nell'ambito della normativa dell'Unione europea in tema di *data protection*. Vediamo anzitutto se la stessa è applicabile nel settore qui in esame e, in caso affermativo, quali sono le tutele da essa offerte.

Il testo di riferimento costituisce legge speciale rispetto al *General Data Protection Regulation* (Regolamento UE/2016/679)[215], trovando applicazione, ai sensi dell'art. 2, comma 1, al *trattamento* dei *dati personali* da parte delle *autorità competenti* per *finalità* di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica.

Ciò posto, il primo nodo da sciogliere riguarda la nozione di 'dati personali', i quali sono individuati, agli effetti della Direttiva, in «qualsiasi informazione riguardante una persona fisica identificata o identificabile, (l'«interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, in particolare con riferimento a un identificativo come il nome, un

---

[214] L'Italia ha attuato la Direttiva con il d.lgs. 18 maggio 2018, n. 51. Per un'analisi, v. RICCI, *Il trattamento di dati personali per finalità di prevenzione, indagine, accertamento e perseguimento di reati. Riflessioni sul d.lgs. 18 maggio 2018, n. 51, di attuazione della Dir. 2016/680/UE*, in *Nuove leggi civ. comm.*, 2019, 3, 579 ss.

[215] V. art. art. 2, comma 2, lett. d) del Regolamento che esclude dal relativo raggio operativo il trattamento di dati personali «effettuati dalle autorità competenti a fini 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». V. sul punto GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Dir. pen. cont.*, 29 maggio 2019, 16.

numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di tale persona fisica» (così l'art. 3, n. 1). Esulano invece dal perimetro della Direttiva le informazioni anonime, «vale a dire le informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi e tali da non consentire più l'identificazione dell'interessato»[216].

Ebbene, è evidente che i dati di cui si alimentano i *software* di polizia predittiva volti all'individuazione di potenziali criminali rientrano in tale definizione, riguardando la storia criminale di un soggetto identificato e altri aspetti inerenti alla sua persona. Tuttavia, come è stato osservato[217], lo stesso potrebbe valere per i dati impiegati nei sistemi *place-based* laddove si aderisse a un'interpretazione particolarmente estensiva del requisito di riferibilità del dato a una persona identificata o identificabile: si potrebbe cioè sostenere che i dati trattati riguardano uno specifico soggetto a causa dell'effetto che questi determinano, ovverosia avere un impatto su coloro che si trovano negli *hot spots*. In senso opposto, si potrebbe argomentare che collegare i dati relativi all'ubicazione di un reato a un individuo è sì ipoteticamente possibile, ma non soddisfa il *'likely reasonable' standard*, il quale rappresenta il metro indicato dalla stessa Direttiva al Considerando n. 21 per stabilire l'identificabilità di una persona fisica.

Quanto al 'trattamento', esso è definito dall'art. 3, n. 2 come «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali»; inoltre, la disposizione opera una serie di esemplificazioni[218]. Anche in questo caso ci troviamo al cospetto di un *all-encompassing concept*[219] capace di ricomprendere ampiamente le attività di *predictive policing*, che si risolvono senza dubbio in un trattamento di dati personali.

Nel concetto di 'autorità competente'[220], sono poi naturalmente riconducibili le forze di polizia; così come le finalità dell'analisi algoritmica compiuta dai *software* di polizia predittiva rispecchiano perfettamente quelle che giustificano l'entrata in gioco della Direttiva.

---

[216] V. Considerando n. 21 della Direttiva UE/2016/680.

[217] LYNSKEY, *Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing*, in *International Journal of Law in Context*, 2019, vol. 15, 171 s.

[218] Si indicano: «la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione» (così l'art. 3, n. 2 della Direttiva UE/2016/680).

[219] LYNSKEY, *Criminal Justice Profiling and EU Data Protection Law*, cit., 168.

[220] Questa è intesa, *ex* art. 3, n. 7, lett. a), come «qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica» ovvero come qualsiasi organismo da queste incaricato (lett. b).

Chiarito che i sistemi di nostro interesse sono 'coperti' dalla disciplina euronitaria in esame, possiamo ora addentarci nell'analisi del principale meccanismo di protezione a favore di colui che possa subire una decisione frutto dei *predictive policing systems*.

L'art. 11 della Direttiva[221] impone agli Stati membri di introdurre il divieto di decisioni basate unicamente su un trattamento automatizzato di dati, compresa la profilazione, che producano effetti giuridici negativi o incidano significativamente sull'interessato[222].

In prima battuta, occorre specificare che l'*Article 29 Working Party*, ovverosia il gruppo di lavoro che riuniva le autorità nazionali deputate alla protezione dei dati personali (poi sostituito dall'*European Data Protection Board*), ha affermato[223] che l'inciso «decisione basata unicamente sul trattamento automatizzato di dati» impone di riferire il divieto ai soli casi in cui la decisione si fondi *esclusivamente* su un *automated-decision system*, in assenza cioè di ogni ingerenza dell'essere umano; sicché, laddove quest'ultimo intervenga, la decisione non sarà più *solely automated* e il divieto di cui all'art. 11 non sarà applicabile[224].

Per evitare di incorrere in un simile divieto, il titolare del trattamento dovrà dunque garantire un *controllo umano*, il quale non potrà risolversi in un 'gesto simbolico', bensì dovrà trattarsi di un controllo significativo, cioè «effettuato da una persona che dispone dell'autorità e della competenza per modificare la decisione»[225].

---

[221] GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., 16, lo definisce come una norma fondamentale (che peraltro riprende una garanzia tradizionale, già contemplata dall'art. 15 della Direttiva CE/1995/46), il quale, tuttavia, al pari dell'art. 22 del GDPR presenta una formulazione ambigua. Si consideri che l'Italia ha previsto un simile divieto all'art. 8 del citato decreto attuativo della Direttiva (d.lgs. n. 51/2018), il quale, al comma 1, recita: «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».

[222] Una previsione analoga, costruita però in termini di diritto a favore dell'interessato, è contenuta nell'art. 22 del GDPR. V. però LYNSKEY, *Criminal Justice Profiling and EU Data Protection Law*, cit., 173 che sottolinea come sia preferibile leggere anche la disposizione del Regolamento in termini di divieto, in modo che sia assicurata una maggiore protezione a favore dell'individuo.

[223] V. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, 3 ottobre 2017 (agg. 6 febbraio 2018), 23 (https://dpo.infn.it/wp-content/uploads/2022/03/Linee-guida-sul-processo-decisionale-automatizzato-relativo-alle-persone-fisiche-e-sulla-profilazione-ai-fini-del-regolamento-2016679.pdf). Sebbene tali considerazioni sul suddetto inciso si riferiscano all'art. 22 del GDPR, esse possono essere estese anche all'art. 11 della Direttiva, nella misura in cui le disposizioni sono sovrapponibili in relazione a questo specifico aspetto. Ciò peraltro è stato sottolineato in GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere su alcune questioni fondamentali della Direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giustizia*, 29 dicembre 2017, 11 (https://ec.europa.eu/newsroom/article29/items/610178), in cui l'organismo, nel fornire indicazioni sugli aspetti maggiormente complessi della Direttiva, ha rinviato, per le parti corrispondenti, a quanto già disposto nelle Linee Guida relative al GDPR.

[224] Al riguardo, v. LYNSKEY, *Criminal Justice Profiling and EU Data Protection Law*, cit., 174.

[225] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale*

Si specifica inoltre che, nell'ambito di tale analisi, costui dovrebbe tenere conto di tutti i dati pertinenti. Per assicurare un effettivo ed efficace coinvolgimento umano, l'*Article 29 Working Party* raccomanda che il titolare del trattamento individui e registri, nella valutazione d'impatto sulla protezione dei dati (che incombe su costui ai sensi dell'art. 27 della Direttiva), il grado di un siffatto coinvolgimento nel processo decisionale e la fase nella quale quest'ultimo deve intervenire[226].

Inoltre, tale disposizione reclamerà applicazione solo nei casi in cui la decisione «produca effetti giuridici negativi o incida significativamente sull'interessato»[227]; dunque il divieto non entrerà in azione in presenza di *trivial effects*, ovverosia ripercussioni marginali, trascurabili[228]. Al riguardo, l'*Article 29 Working Party*, nel parere dedicato ad alcune questioni fondamentali poste dalla Direttiva, ha individuato un tipico effetto negativo nel rafforzamento delle misure di sicurezza o della sorveglianza da parte delle autorità competenti[229].

Il legislatore europeo fa tuttavia salva un'eccezione, ammettendo un simile trattamento allorché sia autorizzato dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, il quale preveda garanzie adeguate per i diritti e le libertà dell'interessato; in questo senso, lo *standard* minimo è individuato dalla Direttiva nel diritto di ottenere l'*intervento umano* da parte del titolare del trattamento[230]. In proposito è stato osservato come una simile previsione possa ridimensionare notevolmente la portata del divieto poiché sarà sufficiente prevedere un'apposita legge che autorizzi siffatto trattamento[231]; riteniamo tuttavia che sarà decisivo il rispetto di determinati livelli di protezione dell'interessato, il quale ben potrebbe fungere da argine a potenziali abusi.

Il secondo paragrafo prosegue poi statuendo che siffatte decisioni non possono basarsi «sulle categorie particolari di dati personali di cui all'articolo 10», quelli cioè che rivelino «l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, e il trattamento di dati genetici, di

---

automatizzato, cit., 23. Sulla difficile attuabilità di un effettivo controllo umano, v. LASAGNI, *Difendersi dall'intelligenza artificiale o difendersi con l'intelligenza artificiale? Verso un cambio di paradigma*, in *Riv. it. dir. proc. pen.*, 2022, 1552 ss.

[226] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato*, cit., 23.

[227] V. la previsione speculare dell'art. 22 del GDPR che si riferisce più genericamente a una decisione «che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona».

[228] LYNSKEY, *Criminal Justice Profiling and EU Data Protection Law*, cit., 174.

[229] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere su alcune questioni fondamentali della Direttiva (UE) 2016/680*, cit., 12 s.

[230] Tale soggetto è definito all'art. 3, n. 8) della Direttiva come «l'autorità competente che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o dello Stato membro, il titolare del trattamento o i criteri specifici applicabili alla sua nomina possono essere previsti dal diritto dell'Unione o dello Stato membro».

[231] LYNSKEY, *Criminal Justice Profiling and EU Data Protection Law*, cit., 173.

dati biometrici intesi a identificare in modo univoco una persona fisica o di dati relativi alla salute o di dati relativi alla vita sessuale della persona fisica o all'orientamento sessuale»[232]. Anche in questo caso si fa salva l'ipotesi in cui siano previste misure adeguate a salvaguardia dei diritti, delle libertà e dei legittimi interessi dell'interessato. Sarà dunque responsabilità dello Stato membro individuare un compendio di garanzie che consentano di ricorrere a trattamenti automatizzati di *sensitive data* senza ledere l'interessato[233].

Il terzo paragrafo, infine, pone un divieto generalizzato di tecniche di profilazione che determinino la discriminazione di individui sulla base delle categorie particolari di dati appena menzionate (quindi, ad esempio, in relazione alla razza o all'etnia)[234]. In nessun caso, dunque, gli Stati membri potranno autorizzare attività di profilazione che portino a discriminazione, se basate sul trattamento di dati sensibili; mentre, come si è visto, il processo decisionale automatizzato basato su dati sensibili è consentito, purché in presenza di una base giuridica eurounitaria o nazionale che preveda le adeguate garanzie[235].

A delineare un simile quadro soccorrono diverse disposizioni della Direttiva attraverso l'imposizione di obblighi al titolare del trattamento (Capo IV) ovvero l'attribuzione di diritti all'interessato (Capo III).

Sotto il primo versante, come messo in risalto dall'*Article 29 Working Party*, un requisito essenziale è rappresentato dalla preventiva valutazione d'impatto del trattamento sulla protezione dei dati. In particolare, l'art. 27 della Direttiva impone agli Stati membri di disporre che il titolare vi provveda quando un tipo di trattamento, specie se implichi l'uso di nuove tecnologie, presenti un rischio elevato

---

[232] Così l'art. 10 della Direttiva, prevedendo che il trattamento di tali categorie di dati personali è ammesso solo se strettamente necessario. Lo stesso deve inoltre essere soggetto a garanzie adeguate per i diritti e le libertà dell'interessato e deve poi essere, alternativamente: autorizzato dal diritto dell'Unione o dello Stato membro; volto a salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica; riferito a dati resi manifestamente pubblici dall'interessato. L'art. 8, comma 3, del d.lgs. n. 51/2018 rispecchia la disposizione di cui all'art. 11, par. 2 della Direttiva.

[233] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere su alcune questioni fondamentali della Direttiva (UE) 2016/680*, cit., 14, enfatizza l'importanza della previsione da parte degli Stati membri, in sede di attuazione della Direttiva, di garanzie rigorose a tutela dei diritti delle persone, in considerazione «della natura particolare dei dati e degli ovvi rischi di discriminazione derivanti dalle decisioni automatizzate fondate su di essi».

[234] Sull'importanza di tale divieto, v. BONFANTI, Big data *e polizia predittiva*, cit., 7. La definizione di profilazione è ricavabile dall'art. 3, n. 4, ove essa viene individuata in «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». Lo stesso prescrive l'art. 8, comma 4, d.lgs. n. 51/2018, a mente del quale: «Fermo il divieto di cui all'articolo 21 della Carta dei diritti fondamentali dell'Unione europea, è vietata la profilazione finalizzata alla discriminazione di persone fisiche sulla base di categorie particolari di dati personali di cui all'articolo 9 del regolamento UE».

[235] V. sul punto GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere su alcune questioni fondamentali della Direttiva (UE) 2016/680*, cit., 14.

per i diritti e le libertà delle persone fisiche in considerazione della sua natura, dell'ambito di applicazione, del contesto e delle finalità.

Così facendo, sarà possibile individuare in anticipo eventuali effetti distorsivi e porre rimedio con apposite misure di carattere più specifico a garanzia dell'individuo, «che non sono state enunciate in atti legislativi (più generali) che permettono tale processo decisionale automatizzato»[236]. In questo contesto, inoltre, assumerà un peso centrale l'obbligo di consultazione preventiva dell'autorità di controllo di cui all'art. 28 della Direttiva.

Ancor prima della valutazione di impatto, occorrerà adottare, a mente dell'art. 20 della Direttiva, misure tecniche e organizzative adeguate, quali la pseudonimizzazione[237], che assicurino efficacemente il rispetto dei principi di protezione dei dati (come la minimizzazione) e l'integrazione nel trattamento delle garanzie a favore degli interessati richieste dalla Direttiva. Inoltre, ai sensi del paragrafo 2, ulteriori misure dovranno garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento e che questi non siano resi accessibili a un numero indefinito di persone fisiche senza un apposito intervento. Ricordiamo poi che è necessario che il titolare predisponga dei registri delle attività *ex* art. 24 della Direttiva.

Una sezione di particolare rilevanza del provvedimento è dedicata alla sicurezza dei dati personali, ove si prevedono una serie di obblighi preventivi a carico del titolare al fine di prevenire possibili violazioni[238] nonché le procedure e gli adempimenti da ottemperare nel caso di effettiva occorrenza delle stesse[239].

Quanto invece al versante dei diritti dell'interessato, questi sono principalmente di tre tipi: diritti di carattere informativo; diritto di accesso; diritto di rettifica o cancellazione[240]. Ad ogni modo, tali diritti possono essere limitati dagli Stati membri in nome di esigenze di preservazione delle indagini penali, di protezione della sicurezza nazionale, etc.

---

[236] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere su alcune questioni fondamentali della Direttiva (UE) 2016/680*, cit., 14.

[237] *Ex* art. 3, n. 5), la Direttiva si riferisce al «trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile».

[238] V. art. 29 della Direttiva che indica le misure preventive da adottare.

[239] V. art. 30, che disciplina la notifica di violazioni dei dati personali all'autorità di controllo, nonché art. 31, relativo alla comunicazione di tale violazione all'interessato.

[240] Con riferimento ai primi (artt. 12 e 13 della Direttiva), in sintesi si prevede che costui sia messo a conoscenza, da parte del titolare, delle informazioni principali inerenti al trattamento e dei suoi diritti, tra cui quello di accesso e di rettifica o cancellazione. Il primo riguarda la possibilità di sapere dal titolare che è in atto un trattamento di dati personali e di ottenere l'accesso a questi ultimi. Il secondo consente invece all'interessato di chiedere la rettifica dei dati personali inesatti che lo riguardano ovvero la cancellazione di dati personali qualora il relativo trattamento violi i principi della Direttiva (art. 4), non rispetti le condizioni di liceità *ex* art. 8 ovvero riguardi dati sensibili e non siano adottati i prescritti accorgimenti.

Completato l'esame della *Law Enforcement Directive*, è giunto il momento di dedicarsi all'analisi della proposta di Regolamento sull'intelligenza artificiale.

7.2. La proposta di Regolamento europeo sull'intelligenza artificiale.

Il 21 aprile 2021 la Commissione europea ha pubblicato la proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi dell'Unione[241]. Segnaliamo che il 14 giugno 2023, il Parlamento ha approvato una nuova versione del testo normativo in parola (che sarà ora oggetto di negoziazione con i governi prima di divenire definitivo), apportando modifiche significative, alcune delle quali, come vedremo, riguardano proprio l'inquadramento della polizia predittiva.

In generale, si tratta di un ricco *corpus* normativo che si propone di disciplinare in modo organico la materia con l'obiettivo di affrontare i rischi associati a determinati impieghi di questa nuova scienza, preservando così la *leadership* tecnologica dell'Unione e assicurando un ambiente sicuro per i diritti dei cittadini.

Come abbiamo avuto modo di accennare, la proposta si caratterizza per un approccio normativo orizzontale dell'intelligenza artificiale, equilibrato, proporzionato e flessibile che si basa sul rischio, limitandosi quindi a fissare requisiti minimi necessari per affrontare i problemi da essa posti, senza 'imbrigliare' lo sviluppo tecnologico o altrimenti appesantire il costo dell'immissione sul mercato di simili sistemi.

Prima di addentrarci nel cuore della proposta e di verificare se la disciplina sia riferibile ai *software* di *predictive policing*, è opportuno soffermarci brevemente sul suo perimetro applicativo e sulla definizione di 'sistemi di intelligenza artificiale' agli effetti del futuro regolamento.

Quanto al primo profilo, l'art. 2 individua come destinatari della normativa tre principali categorie di soggetti: a) i *providers* (fornitori) che introducono nel mercato o mettono in servizio sistemi di intelligenza artificiale nel territorio dell'Unione, indipendentemente dal fatto che ivi siano stabiliti ovvero in un Paese terzo; b) i *deployers* di sistemi di IA che hanno sede o che si trovano all'interno dell'Unione[242]; c) i fornitori e i *deployers* di simili sistemi che hanno la loro sede o che

---

[241] COMMISSIONE EUROPEA, *Proposta per un Regolamento che stabilisce regole armonizzate sull'intelligenza artificiale*, COM(2021) 206 final, 21 aprile 2021 (https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence). Per un commento, v. LAVORGNA-SUFFIA, *La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale*, in *Dir. pen. cont. – Riv. trim.*, 2/2021, 89 ss.

[242] Questi soggetti sono definiti, ai sensi del nuovo art. 3, par. 1, n. 4 del Regolamento come «any natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal nonprofessional activity». Nella bozza iniziale presentata dalla Commissione, si faceva riferimento agli utenti (*users*) dei sistemi di IA collocati nell'Unione.

sono situati in un Paese terzo, in cui la legge dello Stato membro si applica in virtù del diritto internazionale pubblico o il risultato prodotto dal sistema è destinato a essere utilizzato nell'Unione[243]. A seguito degli emendamenti apportati dal Parlamento, alla lettera c) sono state aggiunge tre sottocategorie di destinatari[244].

Al riguardo, è stato osservato che, analogamente al GDPR, l'*Artificial Intelligence Act* si presta a un'applicazione extraterritoriale[245]. Sono invece espressamente sottratti alla operatività del Regolamento i sistemi di intelligenza artificiale sviluppati o utilizzati a fini militari.

Con riferimento al secondo aspetto, il 'sistema di intelligenza artificiale' è oggi definito, ai sensi dell'art. 3, n. 1, come «a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments»[246].

Chiariti questi aspetti preliminari, possiamo ora concentrarci sulle disposizioni precettive della proposta e, in particolare, sulla suddivisione dei sistemi di intelligenza artificiale in distinte classi di rischio. Essa si riflette sulla struttura dell'atto normativo che dedica a ciascuna di esse un diverso titolo: in particolare, al Titolo II si collocano le *pratiche vietate*; il Titolo III è dedicato ai *sistemi ad alto rischio*; il Titolo IV si occupa invece degli obblighi di trasparenza per i sistemi che comportano *rischi specifici di manipolazione*. Per i sistemi che presentano un rischio minimo non è contemplato un apposito titolo, ma si prescrivono esclusivamente meri obblighi di indicazione dell'utilizzo nella fornitura di un servizio.

Dalla nostra prospettiva, rileva in particolare la disciplina prevista per le prime due categorie: ciò in quanto, nella proposta iniziale, le applicazioni di polizia predittiva ricadevano all'interno dei sistemi di intelligenza artificiale ad alto rischio, sicché soggette a particolari prescrizioni ma comunque ammesse; di contro, ad oggi, le stesse sono state trasposte tra le pratiche vietate. Vediamo dunque di ricostruire i

---

[243] Secondo il testo della proposta originaria, si consideravano i fornitori e gli utenti di simili sistemi situati in un Paese terzo, laddove l'*output* prodotto dal sistema fosse utilizzato nell'Unione.

[244] Si tratta di: ca) i fornitori che immettono sul mercato o in servizio dei sistemi di IA di cui all'articolo 5 [ossia rientranti nelle pratiche vietate] al di fuori dell'Unione, se il fornitore o distributore di tali sistemi si trova all'interno dell'Unione; cb) gli importatori e i distributori di sistemi di IA nonché i rappresentanti autorizzati dei fornitori di sistemi di IA, qualora tali importatori, distributori o rappresentanti autorizzati abbiano sede o si trovino nell'Unione; cc) '*affected persons*', che si trovano nell'Unione e la cui salute, sicurezza o diritti fondamentali sono influenzati negativamente dall'uso di un sistema di IA immesso sul mercato o messo in servizio nell'Unione.

[245] Così MALASCHINI, *Regolare l'intelligenza artificiale. Le risposte di Cina, Stati Uniti, Unione europea, Regno Unito, Russia e Italia*, in SEVERINO (a cura di), *Intelligenza artificiale. Politica, economia, diritto, tecnologia*, cit., 135.

[246] V. la definizione della proposta iniziale: «un *software* sviluppato con una o più delle tecniche e 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».

termini dell'una e dell'altra classificazione, per poi dedicarci, in un secondo momento[247], ai relativi riflessi.

Le pratiche vietate sono indicate in un elenco contenuto all'art. 5, nella misura in cui il relativo livello di rischio è considerato inaccettabile poiché contrastante con i valori fondamentali dell'Unione (ad esempio, sistemi che sfruttino tecniche subliminali o tecniche manipolative o ingannevoli, con l'obiettivo o l'effetto di distorcere materialmente il comportamento di una persona).

Gli artt. 6 e ss. si occupano invece della disciplina dei sistemi ad alto rischio[248].

Ai sensi dell'art. 6, par. 1, la qualificazione *high-risk* si basa essenzialmente sulla funzione del sistema nonché sulle relative finalità e modalità specifiche di utilizzo. In particolare, la disposizione richiede che siano soddisfatte due condizioni affinché un sistema possa ricadere in detta categoria[249]. In aggiunta a questi, rientrano nella categoria in parola i sistemi indicati nell'allegato III, purché rappresentino un pericolo per la salute, la sicurezza, i diritti fondamentali delle persone fisiche o l'ambiente[250].

Come si diceva, l'utilizzo di sistemi di tal fatta è ammesso, purché subordinato al rispetto delle rigorose prescrizioni che subito vedremo.

Al riguardo, si prevede in primo luogo l'istituzione di un sistema di gestione dei rischi che si sostanzia in un processo, eseguito nel corso dell'intero ciclo di vita dell'*AI system* e costantemente aggiornato, che si articola principalmente nel *risk assessment* e nel *risk management*, con conseguente adozione di misure appropriate per minimizzare i pericoli rilevati.

Si fissano poi specifici requisiti in relazione ai dati e alla *governance* dei dati, alla documentazione tecnica che deve essere elaborata prima dell'immissione del sistema sul mercato e alla conservazione delle registrazioni degli eventi occorsi durante il funzionamento del sistema medesimo. Tale ultima previsione contribuisce naturalmente ad assicurare la tracciabilità nonché la trasparenza, la quale peraltro è oggetto di una autonoma disposizione (l'art. 13), ove si stabilisce che i sistemi in parola debbano essere sviluppati e progettati al fine di consentire agli utenti di interpretare l'*output* e di utilizzarlo in maniera adeguata. A tal proposito, è complementare la previsione di un compendio di istruzioni d'uso di accompagnamento che siano sufficientemente comprensibili per gli utilizzatori.

---

[247] V. *infra* § 7.3.

[248] Si tratta di sistemi che presentano un alto rischio per la salute e la sicurezza ovvero per i diritti fondamentali delle persone.

[249] Deve cioè trattarsi di un sistema usato come componente di sicurezza di un prodotto, ovvero sia esso stesso un prodotto, disciplinato da precedenti direttive dell'Unione indicate nell'Allegato II; inoltre, è necessario che il prodotto, la cui componente di sicurezza è il sistema di IA, o il sistema di IA stesso in quanto prodotto, sia soggetto a una valutazione di conformità da parte di terzi in relazione ai rischi per la salute e la sicurezza ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi delle direttive di cui all'allegato II.

[250] Nella proposta della Commissione quanto indicato nell'Allegato III era considerato *sempre* 'ad alto rischio'.

Per assicurare l'*accountability*, si richiede inoltre la registrazione dei sistemi in un *database* dell'Unione con l'indicazione di un rappresentante autorizzato, qualora essi provengano da Paesi terzi.

Un aspetto essenziale riguarda poi il requisito della *sorveglianza umana*, volto a prevenire o quantomeno minimizzare i rischi per la salute, la sicurezza o i diritti fondamentali attraverso misure preventive che consentano al soggetto deputato al controllo di comprendere appieno le capacità e i limiti del sistema, nonché di rilevare e gestire prontamente eventuali anomalie e disfunzioni; di governare la tendenza a porre eccessivo affidamento all'intelligenza artificiale (c.d. distorsione dell'automazione) e, dunque, di interpretare correttamente e autonomamente l'*outcome*; e, infine, di arrestare il sistema allorquando necessario.

Naturalmente, dovrà poi essere assicurato che i sistemi rispettino adeguati *standard* di accuratezza, robustezza e cibersicurezza; così come i soggetti coinvolti nei diversi *steps* del ciclo di vita del sistema (fabbricatori, fornitori, utenti, etc.) dovranno adempiere agli obblighi posti a loro carico dalla proposta.

7.3. I riflessi dello scenario normativo europeo sulla predictive policing.

Una volta delineato il quadro regolatorio generale emergente dagli atti eurounitari sin qui analizzati, siamo in grado di ricostruire lo statuto di disciplina della polizia predittiva tra presente e (possibile) futuro.

Innanzi tutto, abbiamo visto come i diversi documenti esaminati – la Carta etica della CEPEJ, lo studio commissionato dal Parlamento europeo, il *report* FRA e la Risoluzione del 6 ottobre 2021 – si siano, a vario titolo, confrontati con le principali problematiche originate dai sistemi di *predictive policing* (o, più in generale, degli algoritmi di intelligenza artificiale in campo penale) nella prassi americana, segnalando ai *policy-makers* la strada da seguire per governare i relativi rischi. Ricapitolando qui i punti di fondo, si tratterà di: assicurare il rispetto dei diritti umani fondamentali, secondo un approccio *human-rights-by-design*; prevedere il divieto di discriminazione, predisponendo misure per rilevare e gestire simili eventualità nonché utilizzando le capacità degli stessi *software* per evitare esiti discriminatori; garantire adeguati *standard* di qualità e sicurezza, prestando particolare attenzione nella fase di selezione dei dati di cui alimentare la macchina e operando in un ambiente tecnologico sicuro; salvaguardare la trasparenza, l'imparzialità e l'equità, consentendo la piena accessibilità (e comprensibilità) da parte sia dell'agente di polizia sia del soggetto sottoposto alla decisione algoritmica del percorso logico compiuto e individuando, di conseguenza, un punto di equilibrio con la tutela del segreto industriale; istituire il controllo umano dell'utilizzatore, che dovrà sempre mantenere la propria autonomia di giudizio e mai adagiarsi sul risultato elaborato dall'algoritmo[251].

[251] Ne sottolinea, in generale, l'importanza GALLI, *Law Enforcement and Data-Driven Predictions at the*

Inoltre, abbiamo dato conto di specifici atti normativi dell'Unione vigenti (*Law Enforcement Directive*) o di prossima entrata in vigore (*AI Act*), che si apprestano ad avere incisivi riflessi sulla disciplina dei sistemi di identificazione dei potenziali criminali – e, in generale, sulla polizia predittiva – di cui subito diremo.

Quanto alla Direttiva del 2016, il divieto di cui all'art. 11 comporta anzitutto che la decisione sulla qualificazione di un soggetto quale potenziale autore di reati – decisione che produce senz'altro degli effetti giuridici negativi nei confronti dell'interessato, se pensiamo agli esempi dei *software* utilizzati negli Stati Uniti[252] – non può essere basata unicamente sul calcolo algoritmico, ma è necessario che un agente di polizia intervenga in siffatto processo decisionale, in termini non simbolici, eventualmente modificando il risultato. Ciò è senz'altro importante poiché si può in questo modo limitare il margine di errore in cui può incorrere l'algoritmo, specie se il 'controllore' ha la competenza di rilevare e correggere il vizio dell'*outcome*.

Il fatto poi che, ai sensi del par. 2 di tale disposizione, non è ammesso il trattamento automatizzato di dati sensibili o che comunque esso impone la previsione di specifiche garanzie per l'interessato può in generale minimizzare il rischio di discriminazioni ed effetti distorsivi. Inoltre, rispetto ai *software person-based*, dando luogo quest'ultimo a una profilazione dell'interessato (*sub specie*, a un'analisi di dati personali per prevedere il suo comportamento), entra in gioco il generale divieto di discriminazioni sulla base dell'utilizzo di dati sensibili prescritto al par. 3.

Al di là della protezione offerta dall'art. 11, riteniamo che le altre previsioni di cui si è detto – valutazioni di impatto, obblighi di adozione di specifiche misure da parte del titolare del trattamento e diritti dell'interessato – contribuiscano a ridimensionare la portata degli effetti distorsivi della *predictive policing* registratisi nell'esperienza statunitense, laddove consentono, da un lato, di rilevare i rischi per la *data protection* dell'interessato e di intervenire preventivamente, nonché di consentire a costui di essere informato dei propri diritti in materia e di esercitarli concretamente.

Rimane il fatto che la Direttiva esaminata si occupi soltanto di un tassello del più ampio mosaico di criticità riguardante la polizia predittiva e, in generale, l'intelligenza artificiale. Ciò del resto non sorprende, trattandosi di atti emanati in epoca nella quale questi temi si affacciavano appena nel dibattito scientifico e pubblico; da qui l'esigenza che si proceda a costruire, come sta accadendo in altri ambiti influenzati dall'impetuoso processo di digitalizzazione (si pensi alla *cybersecurity*), un compiuto quadro normativo.

È in questa prospettiva che si muove la proposta di Regolamento sull'intelligenza artificiale, potendo rappresentare un decisivo passo nella direzione appena auspicata. Occupiamoci allora delle ricadute che la futura entrata in vigore dell'*AI Act* potrà avere sulla *predictive policing*.

National and EU Level. A Challenge to the Presumption of Innocence and Reasonable Suspicion?, in MICKLITZ-POLLICINO-REICHMAN-SIMONCINI-SARTOR-DE GREGORIO (a cura di), *Constitutional Challenges in the Algorithmic Society*, Cambridge, 2022, 127: «the ultimate decision should always be human».

[252] Sembra più difficile sostenere che l'individuazione di *crime hot spot* rappresenti una decisione con effetti negativi per l'interessato. V. LYNSKEY, *Criminal Justice Profiling and EU Data Protection Law*, cit., 174.

L'ultima versione del provvedimento, che è stata licenziata dal Parlamento europeo nel giugno 2023, colloca gli strumenti di polizia predittiva che identificano i potenziali criminali tra le pratiche vietate. Invero, tra queste, figurano i sistemi di AI utilizzati «for making risk assessments of natural persons or groups thereof in order to assess the risk of a natural person for offending or reoffending or for predicting the occurrence or reoccurrence of an actual or potential criminal or administrative offence based on profiling of a natural person or on assessing personality traits and characteristics, including the person's location, or past criminal behaviour of natural persons or groups of natural persons».

Laddove, pertanto, una simile previsione dovesse entrare definitivamente in vigore, i *person-based systems* su cui abbiamo focalizzato la nostra attenzione non sarebbero ammessi.

Il medesimo destino, peraltro, sembrerebbe prospettarsi anche per i *place-based systems*, laddove, tra le pratiche vietate, sono oggi altresì inclusi i sistemi utilizzati per predire «the occurrence or reoccurrence of an actual or potential criminal or administrative offence based on profiling of a natural person or on assessing personality traits and characteristics, including the person's location, or past criminal behaviour of natural persons or groups of natural persons».

Sono invece considerati 'ad alto rischio' – e sono dunque consentiti – i sistemi di IA «intended to be used by or on behalf of law enforcement authorities or by Union agencies, offices or bodies in support of law enforcement authorities for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences or, in the case of Union agencies, offices or bodies, as referred to in Article 3(5) of Regulation (EU) 2018/1725», così come quelli utilizzati dagli stessi soggetti per le attività di '*crime analytics regarding natural persons*', che consentono alle autorità di cercare insiemi di dati complessi, correlati e non, disponibili in fonti o formati diversi, al fine di identificare modelli sconosciuti o scoprire relazioni nascoste nei dati[253]. In questo senso, dunque, sembrerebbe che i sistemi di *crime linking* in precedenza menzionati[254] – come *KeyCrime* o *Giove* – non rientrino nel divieto di cui all'art. 5 del Regolamento, non comportando in alcuno modo attività di *risk assessment*.

La proposta, come dicevamo, è ancora in fase di discussione e vedremo dunque quale sarà l'approdo. In attesa di sapere se prevarrà l'impostazione avanzata dal Parlamento, pare utile esaminare lo scenario che sin qui si era prospettato all'esito della diversa scelta classificatoria operata dalla Commissione nel 2021.

Questa, infatti, collocava i *person-based systems* tra i sistemi 'ad alto rischio' di cui all'Allegato III, che, al paragrafo 6, dedicato ai sistemi relativi alle attività di *law enforcement*, si riferiva, alla lett. a), ai «sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per effettuare *valutazioni individuali dei rischi delle persone fisiche*

[253] V. Allegato III, punto 6, lett. f) e g).

[254] V. *supra* § 2.1.

al fine di determinare il rischio di reato o recidiva in relazione a una persona fisica o il rischio per vittime potenziali di reati» [corsivo aggiunto].

Ne consegue che, secondo il disposto al tempo elaborato dalla Commissione, l'utilizzo di tali *tools* era ammesso purché subordinato al rispetto delle rigorose prescrizioni sopra illustrate[255].

In definitiva, è evidente come l'eventuale entrata in vigore della proposta di regolamento europeo sull'intelligenza artificiale sia destinata a riflettersi sul futuro della *predictive policing*, in quanto, dalla sua attuale classificazione tra le pratiche vietate (ad eccezione dei *suspect-based systems*), potrebbe discendere un insuperabile ostacolo al relativo utilizzo.

Pur non volendo per nulla sottovalutare le criticità che specie i sistemi basati sul *risk assessment* presentano, ci sembra che l'opposizione di un divieto generalizzato non rappresenti la soluzione ottimale. Come avremo modo di argomentare, crediamo che la diffusione dei *software* di polizia predittiva rappresenti un'occasione – una volta dettata una robusta regolamentazione – per rinnovare l'operato delle forze dell'ordine e la disciplina abbozzata nella proposta della Commissione, unitamente alla normativa in tema di *data protection*, potrebbero rappresentare un primo passo verso questa direzione.

8. Condizioni e ambiti di applicazione dei *person-based systems* nell'ordinamento italiano.

La polizia predittiva costituisce la frontiera più innovativa tra i diversi campi di intersezione tra sistema penale e algoritmi predittivi. Invero l'idea di prevedere, attraverso l'impiego di siffatti strumenti, e, di conseguenza, prevenire la commissione di reati mediante l'individuazione di luoghi o persone 'a rischio' esercita un notevole fascino sul giurista.

L'indagine condotta sulle diverse applicazioni di *predictive policing* ha però messo in evidenza come non manchino lati oscuri legati all'impiego di detti strumenti.

L'analisi comparatistica ha innanzi tutto permesso di rilevare come i profili di maggiore criticità siano originati dai sistemi basati sull'identificazione dei potenziali autori di reati attraverso la *social network analysis* e la predisposizione di 'liste calde'[256]. Sebbene, infatti, i diversi *tools* presentino comuni tratti problematici – relativi ai dati di cui si alimentano (sia in termini di qualità, sia di errori che possono occorrere nelle diverse fasi di raccolta, selezione e inserimento), alla potenzialità discriminatoria degli algoritmi in questione, all'opacità circa il funzionamento e all'*accountability* –, i *person-based systems* sollevano ulteriori questioni rispetto ai c.d. *place-based systems*[257].

---

[255] V. *supra* § 7.2.

[256] Per una ricostruzione preliminare dei *person-based systems* v. *supra* § 2.1.

[257] Si rinvia *supra* § 2 per l'inquadramento dei *place-based systems*.

L'esame dell'esperienza maturata nei *police departments* di Kansas City e Chicago[258] ha messo in evidenza diversi aspetti che mal si conciliano con il patrimonio di principi della nostra tradizione penalistica.

Anzitutto i rilievi si appuntano sui criteri di classificazione di rischio degli individui: costoro sono sovente identificati quali *target* poiché sono state vittime ovvero sulla base di legami indiretti con autori di reati e, anche quando presentano precedenti penali, questi di frequente non giustificano la qualificazione di pericolosità associata ai soggetti di cui si tratta. Inoltre, la regolamentazione prevista non contempla meccanismi di contestazione, da parte dell'interessato, dell'attribuzione del *risk score*.

Vi è poi, come abbiamo visto, la previsione in capo alle persone inserite nelle liste sopra richiamate, sulla base dei dati processati dagli algoritmi, di un significativo aumento di pena allorché commettano un qualunque reato, indipendentemente dalla sua gravità e soprattutto dalla sua 'connessione' con il giudizio di pericolosità formulato. Eppure, abbiamo avuto modo di vedere[259] che esistono nel nostro sistema istituti, certo diversi da quelli appena evocati, fondati su analoghe valutazioni di pericolosità individuale.

Da un lato, viene in rilievo la misura di prevenzione personale dell'avviso orale che, come noto, consiste nella diffida da parte del questore, a un soggetto riconducibile a una delle fattispecie di c.d. pericolosità generica di cui all'art. 1 del Codice Antimafia e che manifesti una pericolosità per la pubblica sicurezza, a tenere un comportamento conforme alla legge. Un'intimazione, dunque, di carattere generico – come accade per quella prevista nel modello americano prima analizzato – che, pur essendo suscettibile di determinare dei riflessi sanzionatori negativi nei confronti dell'avvisato, li circoscrive a una cerchia predeterminata di fattispecie, sebbene non si possa certo nascondere che la lista è variegata (se solo si considera che tra le ipotesi di reato richiamate dall'art. 71 del Codice Antimafia si spazia da reati contro la pubblica amministrazione, ordine pubblico, persona, patrimonio fino a includere talune contravvenzioni). Si aggiunga altresì che è comunque garantita una ampia possibilità di contestazione della misura da parte dell'interessato.

Dall'altro lato, viene in considerazione l'ammonimento previsto in materia di atti persecutori dall'art. 8 del d.l. n. 11/2009. Qui si registra un aggravamento della risposta sanzionatoria del soggetto – come noto, è contemplata una circostanza aggravante a effetto comune nel caso in cui l'ammonito commetta poi il delitto di *stalking*, il quale diviene altresì procedibile d'ufficio (e non più a querela della persona offesa); anche qui, però, a differenza dell'ordinamento statunitense, ricorrono presupposti e condizioni che ci sembrano pienamente legittimare l'inasprimento del trattamento riservato all'ammonito.

Sono tre i profili di disciplina, come abbiamo cercato di evidenziare, che ci paiono mettere al riparo la normativa in questione.

---

[258] Per l'analisi di tali sistemi si rinvia *supra* § 2.1.1; le relative criticità sono state invece affrontate nel § 3.

[259] V. *supra* § 6.

In primo luogo, l'aggravamento di pena è legato alla realizzazione non di un qualunque reato ovvero di un comportamento non conforme alla legge, bensì di quelle specifiche condotte per le quali lo stesso soggetto era stato precedentemente diffidato.

In secondo luogo, l'operatività dell'inasprimento sanzionatorio (nonché la procedibilità d'ufficio) è subordinata al fatto che le condotte di minaccia o molestia siano perpetrate a danno della medesima persona offesa su richiesta della quale il questore aveva proceduto all'ammonimento.

Infine, è riconosciuta all'ammonito la possibilità di contestare la misura in sede giurisdizionale; un aspetto questo imprescindibile allorché si vogliano far discendere dalla violazione della misura simili riflessi negativi.

Un possibile impiego dei *person-based systems* dovrebbe replicare i modelli sopra schematizzati. In particolare, alla luce di quanto emerso dalla comparazione con l'avviso orale e l'ammonimento ci sembra possibile ipotizzare, a certe condizioni, un legittimo ambito di operatività per strumenti algoritmici di questa tipologia con riferimento alla valutazione prognostica di pericolosità richiesta ai fini dell'adozione di siffatte misure di prevenzione, la quale, peraltro, è per sua natura «basata su dati indiziari e[d è] strutturalmente incline ad essere "integrata" da indici di carattere predittivo»[260].

Occorre invero prendere atto di come, nella prassi applicativa, l'accertamento di tale pericolosità viva uno stato di crisi, per un duplice ordine di ragioni. Innanzi tutto, si pongono non pochi problemi riguardo all'individuazione dei parametri di riferimento di un simile scrutinio[261], cui spesso consegue la sua sostanziale obliterazione. E ciò sebbene questa valutazione, quantomeno nelle intenzioni del legislatore, dovrebbe svolgere una funzione di garanzia per il proposto, nella misura in cui essa impone all'autorità procedente, in un certo senso, di fornire un ulteriore e concreto riscontro alla previa classificazione di un soggetto in una determinata categoria 'di rischio', evitando che da questa possa automaticamente discendere l'applicazione della misura. Tuttavia, come è stato osservato, si tratta di «una garanzia più apparente che reale», poiché, mancando «un'adeguata indicazione normativa circa il modo di esercizio e gli esiti apprezzabili di tale giudizio»[262], una siffatta

---

[260] Così MANES, *L'oracolo algoritmico e la giustizia penale*, cit., 10.

[261] Sul punto, v. BASILE, *Manuale delle misure di prevenzione*, cit., 77 s.; PELISSERO, *I destinatari della prevenzione* praeter delictum*: la pericolosità da prevenire e la pericolosità da punire*, in *Riv. it. dir. proc. pen.*, 2017, 457; MARTINI, *Il mito della pericolosità. Alla ricerca di un senso compiuto del sistema della prevenzione personale*, in *Riv. it. dir. proc. pen.*, 2017, 547 ss. V. anche MAUGERI, *L'uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra* evidence based practices *e tutela dei diritti fondamentali*, in *Arch. pen. web*, 17 maggio 2021, 8, che evidenzia le problematicità dell'accertamento di tale forma di pericolosità. Sulla generale criticità degli accertamenti prognostici relativi alla propensione dell'individuo alla commissione di reati, previsti in vari segmenti del sistema penale, e sulla possibilità di impiegare algoritmi predittivi, v. CAIANIELLO, *Dangerous Liaisons. Potentialities and Risks Deriving from the Interaction between Artificial Intelligence and Preventive Justice*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2021, vol. 29, 14 ss.

[262] V. testualmente MARTINI, *Il mito della pericolosità*, cit., 547.

valutazione finisce per appiattirsi su quella che la precede. In dottrina, sono stati però valorizzati alcuni tentativi – perlopiù isolati – della giurisprudenza volti a circoscrivere il perimetro dell'accertamento in questione «alla probabilità di commettere nuovi reati, partendo dalla valutazione globale della personalità del proposto, quale risulta dalle manifestazioni sociali della sua vita nella quale acquista rilevanza anche la commissione di fatti di reato»[263].

Ad ogni modo – e veniamo così alla seconda problematica – la valutazione della pericolosità è rimessa alla discrezionalità del questore[264]. Ne deriva che, nonostante i menzionati sforzi della giurisprudenza di ancorare a parametri più definiti il contenuto di un simile accertamento, quest'ultimo nella prassi rimane comunque lasciato all'apprezzamento dell'autorità di pubblica sicurezza, in assenza di una cornice normativa che possa fungere da reale guida e secondo schemi che rimangono in ogni caso caratterizzati da una insopprimibile elasticità[265], con il rischio – anche in considerazione, come diremo subito, del limitato sindacato giurisdizionale – di determinare disparità di trattamento nella applicazione delle misure preventive in questione, in spregio del principio di uguaglianza di cui all'art. 3 Cost.[266]. A conferma di ciò basta scorrere i repertori giurisprudenziali ove ci si imbatte in pronunce che ribadiscono che «l'autorità amministrativa competente […] gode di ampia discrezionalità nell'accertamento e nella valutazione dei presupposti richiesti dalla legge, ossia dei sospetti, dovendo il sindacato del giudice amministrativo limitarsi solo ad aspetti di manifesta irragionevolezza od arbitrarietà dell'*iter* logico seguito dall'amministrazione o della motivazione adottata»[267].

Si consideri poi che, nell'ambito qui in esame, risultano per definizione carenti le garanzie proprie del procedimento giurisdizionale. Prendiamo ad esempio il piano probatorio, in relazione al quale la giurisprudenza non manca di sottolineare che, diversamente da quanto richiesto in relazione ad altre misure più invasive, la

---

[263] Così PELISSERO, *I destinatari della prevenzione* praeter delictum, cit., 457 che si riferisce a Cass. pen., Sez. I, 5 giugno 2014, n. 23641. V. però MARIANI, *Prevenire è meglio che punire. Le misure di prevenzione personali tra accertamento della pericolosità e bilanciamenti di interessi*, Milano, 2021, 298 s., la quale rileva come, al netto di 'enunciazioni di principio', tenda a mancare nella prassi una 'seria valutazione della personalità del preposto'.

[264] Su questi aspetti, v. CONSULICH, *Le misure di prevenzione personali tra Costituzione e Convenzione*, in *Leg. pen.*, 18 marzo 2019, 18.

[265] Sul punto, v. i risultati della ricerca condotta da MARIANI, *Le misure di prevenzione personale nella prassi milanese*, in *Dir. pen. cont. – Fasc.*, 10/2018, 314 s., basata sull'analisi dei provvedimenti emessi in materia di misure di prevenzione dalla Questura di Milano tra il 2012 e il 2016 nell'ambito delle Province di Milano e di Monza e Brianza (nonché dal Tribunale di Milano, Sezione Autonoma Misure di Prevenzione), i quali dimostrano che l'accertamento della pericolosità, da un lato, si è fondato esclusivamente sulla considerazione dei precedenti penali del proposto (e non anche sull'esame della sua personalità) e, dall'altro, che un tale apprezzamento – privo di criteri guida validi e positivizzati – è governato dall'intuizione dell'autorità pubblica.

[266] Si esprime in questi termini MARIANI, *Prevenire è meglio che punire*, cit., 118.

[267] Così T.a.r. Calabria Catanzaro, Sez. I, 7 marzo 2023, n. 339; v. altresì T.a.r. Piemonte Torino, Sez. I, 2 dicembre 2020, n. 791. In dottrina, v. CONSULICH, *Le misure di prevenzione personali*, cit., 18; MARIANI, *Prevenire è meglio che punire*, cit., 119.

valutazione degli elementi di fatto in grado di fondare il giudizio di pericolosità alla base dell'avviso orale sono meno stringenti, poiché si tratta di provvedimenti aventi «natura ed efficacia meramente monitoria ed infra-procedimentale» e, pertanto, non direttamente incidenti sulle libertà individuale. Sicché, un simile scrutinio può fondarsi anche su meri sospetti circa determinate circostanze fattuali, che siano «tali da indurre l'Autorità di polizia a ritenere sussistenti le condizioni di pericolosità sociale che possono dar luogo, da parte del giudice, all'applicazione delle misure di prevenzione»[268].

In questo scenario, la previsione, a supporto della valutazione di competenza del questore, di una verifica mediante un algoritmo predittivo dei dati relativi ai precedenti penali e alle vicende personali dell'individuo potrebbe rivelarsi di particolare utilità anzitutto ai fini dell'applicazione dell'avviso orale. Sarebbe cioè in grado di dare sostanza alla valutazione del mero sospetto mediante una base di giudizio più consistente.

Inoltre, l'innesto di simili strumenti potrebbe vieppiù svolgere una funzione di garanzia nei confronti del destinatario della misura ogniqualvolta, in virtù della sussistenza di esigenze di celerità ai sensi dell'art. 7 della l. 7 agosto 1990, n. 241, si ometta la comunicazione dell'avvio del procedimento, impedendo così a costui di esercitare il proprio diritto di difesa già nella fase istruttoria che precede la misura. In sostanza, anche per evitare che le istanze di speditezza finiscano per compromettere una seria e ponderata prognosi di pericolosità, si potrebbe – in queste ipotesi – imporre al questore di ricorrere all'algoritmo per un *double check* sulle risultanze a disposizione e, laddove egli ritenga comunque di disporre l'avviso orale, sebbene il sistema non abbia emesso una predizione di alto rischio, richiedere a costui una esplicita motivazione sul punto.

Un simile impiego dei *tools* in questione è suscettibile di essere altresì ammesso in relazione alla misura dell'ammonimento in materia di *stalking*, ove il ricorso all'algoritmo potrebbe essere letto, del pari, in chiave di garanzia, ossia costituire un 'contraltare' alle dichiarazioni della persona offesa che presenta la relativa richiesta, per evitare, in particolare, che la valutazione del questore si appiattisca su di esse. E ciò, a maggior ragione, quando l'interessato non sia avvisato dell'avvio del procedimento e a questi non sia stato concesso il diritto di essere ascoltato prima dell'adozione della misura – aspetto, quest'ultimo, sul quale la Corte di Strasburgo[269] ha recentemente posto l'attenzione, riscontrando la violazione dell'art. 8 CEDU, in relazione al diritto al rispetto della vita privata e familiare, in un caso in cui si era proceduto all'ammonimento senza assicurare all'interessato un

---

[268] V. ancora T.a.r. Calabria Catanzaro, Sez. I, 7 marzo 2023, n. 339, cit.; nonché, *ex multiis*, T.a.r. Lazio Roma, Sez. stralcio, 15 novembre 2022, n. 14973; T.a.r. Calabria Catanzaro, Sez. I, 12 agosto 2022, n. 1486; T.a.r. Molise Campobasso, Sez. I, 26 aprile 2022, n. 124.

[269] Il riferimento è a Corte Edu, Sez. I, *Giuliano Germano c. Italia*, n. 10794/12, 22 giugno 2023, in *Sist. pen.*, 3 luglio 2023, con nota di ALBANESE, *Ammonimento del questore in materia di* stalking*: la Corte di Strasburgo condanna l'Italia per violazione dell'art. 8 CEDU. "Molti passi indietro nel contrasto alla violenza di genere"?*.

simile diritto e in assenza di specifiche e motivate ragioni di urgenza che giustificassero siffatta limitazione di garanzie.

Naturalmente, l'utilizzo di tali strumenti dovrà essere subordinato all'osservanza di tutte le condizioni atte a contenere le problematiche tipiche degli algoritmi in punto di opacità, difetti di accuratezza, potenzialità discriminatoria e di protezione dei dati personali. Al riguardo, però, da un lato, le critiche avanzate nello scenario statunitense ci mettono in guardia dai possibili rischi e, dall'altro, le proposte elaborate dalla dottrina ci indicano le strade percorribili per assicurare il legittimo utilizzo dei *risk assessment tools*[270]. Inoltre, le indicazioni ricavabili dai diversi documenti elaborati a livello eurounitario nonché le fondamentali prescrizioni in materia di *data protection* della *Law Enforcement Directive*[271], così come attuate nel nostro ordinamento per effetto del d.lgs. 18 maggio 2018, n. 51, offrono un quadro di salvaguardie che può consentire di massimizzare i vantaggi che possiamo trarre da questi moderni sistemi e, al contempo, di governare i rischi che gli stessi pongono.

In particolare, opererà, *ex* art. 8 del d.lgs. n. 51/2018 il più volte menzionato divieto di decisioni, compresa la profilazione, che producano effetti negativi nei confronti dell'interessato, basate unicamente sul trattamento automatizzato di dati. Anche qualora, a mente del diritto interno o dell'Unione europea, le stesse siano autorizzate, il comma 2 della norma in esame richiede la previsione di «garanzie adeguate per i diritti e le libertà dell'interessato», statuendo altresì che «in ogni caso è garantito il diritto di ottenere l'intervento umano da parte del titolare del trattamento». Di regola, poi, le decisioni in parola non potranno basarsi su dati sensibili, a meno che non siano contemplate misure di salvaguardia. Infine, anche il nostro legislatore, conformemente alle prescrizioni eurounitarie, ribadisce il divieto di profilazione finalizzata alla discriminazione di persone fisiche sulla base di dati sensibili (quali, razza, etnia, orientamento sessuale, etc.).

Non meno importanti sono poi le previsioni che, ricalcando quanto disposto dalla Direttiva e già oggetto della nostra analisi[272], attribuiscono importanti diritti all'interessato (accesso, cancellazione, rettifica e altri di carattere informativo) e altrettanti obblighi agli altri soggetti coinvolti (tra cui, il titolare e il responsabile del trattamento).

A completare ulteriormente il quadro a tutela della protezione dei dati personali nelle attività delle forze dell'ordine interviene il d.p.r. 15 gennaio 2018 n. 15 – recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia – il quale contiene, tra l'altro, una serie di prescrizioni fondamentali in tema di qualità dei dati

---

[270] V. *supra* § 4.

[271] V. *supra* § 7.3 ove abbiamo dato atto dei riflessi di questi documenti e della Direttiva sulla *predictive policing*.

[272] V. *supra* § 7.2.

e termini di relativa conservazione, di configurazione dei sistemi informativi e informatici nonché dei tipi di trattamento.

In definitiva, ci sembra che la proposta di ricorrere ad algoritmi predittivi – basati sui precedenti penali e giudiziari nonché su altre informazioni a disposizione delle forze dell'ordine da cui sia possibile trarre elementi utili per delineare la personalità del proposto – potrebbe rappresentare una soluzione per superare le problematiche che si riscontrano nella prassi in relazione all'accertamento prognostico della pericolosità nel contesto delle misure di prevenzione disposte dal questore (e non solo), promettendo un innalzamento degli *standard* di valutazione. Come abbiamo più volte sottolineato, si tratterebbe di una mera funzione di supporto, essendo indispensabile, anche nelle attività di prevenzione della criminalità, assicurare che l'uomo mantenga sempre 'l'ultima parola'.

Con particolare riguardo alla polizia predittiva, non possiamo certo tacere la prospettiva – di cui peraltro abbiamo dato conto[273] – che pare profilarsi in sede eurounitaria sul suo destino e che finirebbe per condurre a un generale divieto (ad eccezione dei *suspect-based systems*, come *KeyCrime* e *Giove*).

In conclusione, riteniamo però che l'analisi sin qui condotta e le proposte avanzate potrebbero indurre a un ripensamento sul futuro dei *person-based systems*, determinandone la riclassificazione, conformemente alla proposta iniziale di regolamento elaborata dalla Commissione europea, tra i sistemi 'ad alto rischio'. Ne conseguirebbe la loro sottoposizione a requisiti e condizioni stringenti che, tuttavia, consentirebbero al contempo di sfruttare, nei termini che abbiamo chiarito, le potenzialità della *predictive policing*.

[273] V. *supra* § 7.3.