1. **Sommario: L'impiego dell'IA per la prevenzione dei reati, - 2 I software e la loro brevettazione: nuove forme di garanzia ?- 3. Diritto di libertà vs tutela della collettività. -4.Il riconoscimento facciale: l'intervento del Garante e quello (limitato) del legislatore.- Lo sguardo sovranazionale….**

1. L'impiego dell'IA per la prevenzione dei reati,

Nell'ambito dell'impiego dell'I.A. nel settore penale, se molte incertezze circondano, ancora, il suo possibile impiego nel processo - tanto richiamandoci ad una concezione forte, quanto debole dell'I.A.- è, invece, da tempo che il suo utilizzo, sta vivendo una felice stagione, nell'ambito della prevenzione e sicurezza pubblica. La progressiva importanza assunta da tali nuovi strumenti è emersa, da ultimo, alla IX Conferenza sulla cooperazione internazionale, tenutasi a Venezia, tra le forze di polizia il cui i lavori si sono conclusi facendo fede, quanto al piano della cooperazione non soltanto su lo scambio di informazioni e dati, ma soprattutto sullo scambio di "esperienze", e dal Law Enforcement Forum che ha unito tutti i paesi dell'Unione in un confronto volto alla prevenzione dei rischi di infiltrazione della criminalità organizzata, a fronte dell' implementazione delle risorse del Pnrr e, in ambito Interpol, con la conduzione del progetto I-CAN (Interpol Cooperation Against Ndrangheta), che si potrà avvalere anche del primo algoritmo predittivo di intelligenza artificiale per intercettare le strategie espansionistiche dell'organizzazione criminale e anticipare le sue future minacce.

2. I software e la loro brevettazione: nuove forme di garanzia ?

In termini generali, il rinvio va alla cd. cd. polizia predittiva, già ampiamente sviluppata nei Paesi stranieri, che ha trovato, indubbiamente, terreno fecondo anche in Italia. Da anni, ormai, la polizia utilizza il software KeyCrime**,** un software che non impiega solo un algoritmo di elaborazione statistica, ma opera in maniera tale da individuare anche i tratti psicologici del potenziale autore del reato, che in questi anni d'utilizzo ha dato buona prova di sé, originando una sensibile diminuzione dei reati. Ma analogo effetto ha comportato l'impiego, presso le Questure, del software X-Law che non lavora su base statistica, ma probabilistica, trattasi, infatti, di un sistema di data e algoritmo euristico.

Nonostante il largo e fruttuoso impiego di questi due sistemi, non si sono, tuttavia, non riscontrate alcune deficienze, tipiche di tali strumenti, legati ora alla loro modalità di raccolta dei dati elaborati, alla natura e carattere dei dati inseriti che, troppo spesso avviene in modo generalizzato, utilizzando i vasti archivi di dati personali, anche attraverso banche dati deputate ad altri scopi, o facendo ricorso a dati su larga scala detenuti dal settore privato. La cd. polizia predittiva muove, infatti, dall'analisi di grandi quantità di dati in base a "criteri predeterminati" (come il Paese d'origine, il sesso e così via), ossia mediante algoritmi di autoapprendimento basati sull'intelligenza artificiale per individuare le persone sospette.

3. Diritto di libertà vs tutela della collettività

Questo tipo di trattamento dei dati soffre di difetti ineludibili che pongono grandi rischi per i diritti e le libertà delle persone: falsi positivi, risultati discriminatori, processi opachi impossibili da contestare e una cruciale mancanza di test o verifiche scientifiche. In altre parole, si tratta di una sorveglianza di massa di intere popolazioni "senza alcuna differenziazione, limitazione o eccezione", senza tener conto dei gravi pericoli e delle carenze intrinseche delle tecnologie di estrazione dei dati. In ogni caso, sotto tale aspetto, va ricordato come X-Law è stato, ad ottobre scorso, oggetto di brevettazione: è questo un passaggio importante, non soltanto per la verificabilità, in parte, del suo sistema di funzionamento che è, com'è noto, uno degli aspetti critici legati all'impiego dell'IA anche in seno alle attività di prevenzione e controllo, ma costituisce un primo passo anche verso la sua possibile certificazione di garanzia ed affidabilità. Certamente rimane invariata la questione, aggravata, nell'epoca post-pandemica (si pensi al triage dei pazienti nel settore sanitario), dall'immenso bacino di dati disponibili. Anche in Italia è da tempo che sono state sollevate ampie perplessità sulla creazione di database (piccoli o grandi) contenenti le impronte biometriche dei cittadini, con lo spettro della giustizia predittiva, del controllo a distanza e dell'analisi comportamentale.

4. Il riconoscimento facciale: l'intervento del Garante e quello (limitato) del legislatore

Proprio l'impiego di quest'ultimi è molto forte e una delle tecniche più usate è il riconoscimento facciale. E' a tutti noto l'utilizzo, a livello interno, del cd. sistema Sari che, a sua volta attinge parte dei dati dal sistema Afis, (*Automated Fingerprint Identification System*, in italiano "Sistema Automatizzato di Identificazione delle Impronte".), che è l' hardware e software molto impiegato nel settore dell'immpigrazione, atteso che per mezzo di esso le impronte digitali vengono codificate attraverso un algoritmo- gestito dal Sistema- che consente di ridurre i normali tempi di acquisizione e catalogazione dei cartellini decadattilari ed effettuare una ricerca rapida ed efficace delle impronte sconosciute. Anche quello della "circolarità" dei dati biometrici è, certamente, un aspetto sul quale, al pari di molti altri, va posta l'attenzione a livello di normazione, primaria e secondaria, anche a livello europeo.

D'altro canto, sul versante interno, è intervenuta l'autorità Garante per la tutela dei dati personali che ha ammonito circa l'impiego del sistema Sari Real Time da parte del Ministero dell'interno. Il sistema, oltre ad essere privo di una base giuridica che legittimi il trattamento automatizzato dei dati biometrici per il riconoscimento facciale a fini di sicurezza, realizzerebbe, secondo il Garante, per come è progettato una forma di sorveglianza indiscriminata/di massa. Il Garante, in linea con quanto stabilito dal Consiglio d'Europa, ritiene di estrema delicatezza l'utilizzo di tecnologie di riconoscimento facciale per finalità di prevenzione e repressione dei reati. Va considerato, in particolare, - afferma il Garante - che Sari Real Time realizzerebbe un trattamento automatizzato su larga scala che può riguardare anche persone presenti a manifestazioni politiche e sociali, che non sono oggetto di "attenzione" da parte delle forze di Polizia. Ed anche se nella valutazione di impatto presentata il Ministero spiega che le immagini verrebbero immediatamente cancellate, l'identificazione di una persona sarebbe realizzata attraverso il trattamento dei dati biometrici di tutti coloro che sono presenti nello spazio monitorato, allo scopo di generare modelli confrontabili con quelli dei soggetti inclusi nella "watch-list": si determinerebbe così una evoluzione della natura stessa dell'attività di sorveglianza, che segnerebbe un passaggio dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale.

È proprio a causa della loro forte interferenza con la vita privata delle persone che la L. n. 205 del 2021 ha sospeso fino al 31 dicembre 2023 l'installazione e l'utilizzazione

di impianti di video sorveglianza con riconoscimento facciale, attraverso l'uso dei dati biometrici di cui all'articolo 4, numero 14), del citato regolamento (UE) 2016/679 in luoghi pubblici o aperti al pubblico, da parte delle autorità pubbliche o di soggetti privati, tuttavia, il testo prevede un'eccezione posto che il comma 12 del provvedimento prevede che il divieto non si applica "ai trattamenti (di dati personali per il riconoscimento biometrico, *ndr*) effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali di cui al d. lgs. 18 maggio 2018, n. 51, in presenza, salvo che si tratti di trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali nonché di quelle giudiziarie del pubblico ministero.

Nonostante tale distinzione e la copiosa normativa in materia di privacy stabilisca rigorose cautele per i trattamenti di dati biometrici e per particolari categorie di dati (ad esempio, quelli idonei a rivelare opinioni politiche, sindacali, religiose, orientamenti sessuali), i quali devono trovare giustificazione in una adeguata base normativa, non rinvenuta nella documentazione fornita dal Ministero dell'interno, è palese come tale deroga susciti ampi dubbi e molte perplessità.

Secondo il Garante, infatti, una base normativa adeguata dovrebbe tener conto di tutti i diritti e le libertà coinvolte e definire le situazioni in cui è possibile l'uso di tali sistemi, senza lasciare una discrezionalità ampia a chi lo utilizza. Ciò vale anche per aspetti fondamentali dell'impiego della tecnica di riconoscimento facciale, come i criteri di individuazione dei soggetti che possono essere inseriti nella watchlist, le conseguenze in caso di falsi positivi o la piena adeguatezza del sistema nei confronti di persone appartenenti a minoranze etniche. Di qui, dunque, il mantenimento delle perplessità circa il carattere fortemente invasivo del mezzo. Va, d'altro canto, ricordato come in seno al Parlamento europeo è stata avanzata una particolare raccomandazione volta ad aggiungere la cosiddetta "polizia predittiva" all'elenco delle tecnologie vietate, affermando che la tecnologia "*viola la presunzione di innocenza e la dignità umana*": così, si è raccomandato di classificare ad alto rischio i sistemi impiegati dall'Italia.

5. Lo sguardo sovranazionale….

La questione incrocia, peraltro, una diversa vicenda qual è quella dell'adeguatezza dei dati e della loro "storicità" allorchè questi vengano impiegati da importanti istituzioni volte a garantire, anche, la prevenzione dei reati. Il rinvio va al caso che ha investito **l**'Agenzia di Europol che utilizza, infatti, il *software* della società statunitense di analisi dei *big data* Palantir (coinvolta in diversi scandali e criticata per la sua assistenza all'Immigration and Customs Enforcement degli Stati Uniti) per "l'analisi operativa di tutti i dati relativi all'antiterrorismo". Ebbene proprio il possibile impiego di dati acquisiti prima dell'istituzione dell'Agenzia ha condotto il Garante europeo per la protezione dei dati ha sollevare una censura in merito al loro utilizzo considerata la delicatezza delle tante problematiche afferenti alla tutela diritti fondamentali, alla trasparenza dei sistemi algoritmici, ai rischi di discriminazione e la preoccupazione che l'uso degli strumenti di sorveglianza di massa sollevano, a maggior ragione quando si tratta di elementi già presenti nelle diverse banche dati ed estranee, al momento della loro acquisizione, alla segnalata finalità. E' questo un terreno sul quale ancora molto occorre lavorare.

Sulla scorta di tale allarme, il Garante europeo della privacy (Edps) ha, infatti, ordinato all'Agenzia comunitaria di polizia, l'Europol**,** di cancellare tutti i dati di persone che non erano collegate a indagini o reati**,** al termine di un'inchiesta avviata nel 2019, ma l'Europol non ha accolto la richiesta atteso che la rimozione di quelle informazioni avrebbe potuto compromettere la sua capacità di analisi di grandi database, non assolvendo, in tal modo, al mandato conferitogli dagli Stati dell'Unione: è questa una questione aperta da cui traspare, lucidamente, come la materia *de qua* rimane ancora, e purtroppo, terreno di scontro fra le polizie, anche europee, che avvertono fortemente la necessità di poter fare uso anche dei dati personali di cittadini del tutto svincolati da casi criminali e il Garante che si fa tutore dei diritti, delle libertà della persona. E', dunque, verso questi organi così come alle Corti nazionali e sovranazionali che occorre rivolgere lo sguardo per ricercare il punto di equilibrio di contrapposti interessi che anche nel campo della prevenzione, vigilanza e sicurezza convergono**.**