IA e Giustizia

STRUMENTI DI "PREDICTIVE POLICING" E RISCHI DI PROFILAZIONE: QUANDO L'INTELLIGENZA ARTIFICIALE È POSTA AL SERVIZIO DELLE ATTIVITÀ DI POLIZIA GIUDIZIARIA

Paolo Pepe*

SOMMARIO: 1.- "Predictive policing" e "predictive sentencing": le due macro-aree di intervento dell'IA in campo processual-penalistico; 2.- La prevenzione del crimine attraverso l'individuazione degli "hotspots" e la ricerca del "crime-linking". Cenni sull'esperienza italiana; 3.- Un efficace "tool" di riconoscimento facciale italiano: il S.A.R.I.; 3.1.- Alcune analoghe esperienze di biometria facciale in Europa; 4.- Le problematiche poste dal S.A.R.I. "Real Time" anche a seguito dell'approvazione dell'"AI Act"-; 5.- Rischi di profilazione e attività investigativa proattiva. Il pericoloso arretramento delle indagini da strumenti di repressione a strumenti di prevenzione.

1.- **"Predictive policing" e "predictive sentencing": le due macro-aree di intervento dell'IA in campo processual-penalistico.**

Malgrado negli ultimi quarant'anni l'interesse per l'IA sia stato discontinuo[1], è già da qualche tempo che se ne prospettano applicazioni significative in diversi settori del diritto.

Nel campo della giustizia penale le interazioni dei sistemi di IA sembrano essere in continua evoluzione e interessano, oltre che il lavoro dei tribunali[2], anche più direttamente il settore della prevenzione del crimine[3].

---

* Dottorando di ricerca presso l'Unical e Avvocato del Foro di Cosenza.

[1] V., a tal proposito, A. Krausovà, *Intersections Between Law and Artificial Intelligence*, in *International Journal of Computer (IJC)* (2017) 55; E. Nissan, *Digital technologies and artificial intelligence's present and foreseeable impact on lawyering, judging, policing and law enforcement*, in *AI § Society* (2015) 3 nonchè R.E. Susskind, *Artificial Intelligence, Expert Systems and Law*, in *Denning Law Journal* (1990) 190ss.

[2] Secondo J. Nieva-Fenoll, *Intelligenza artificiale e processo* (trad. e cur. Paolo Comoglio), Torino, 2019, 12 l'utilizzo dei sistemi di IA nei tribunali sarebbe dovuto alla circostanza che gran parte del lavoro di essi è meccanico e ripetitivo e, per tale ragione, si presta agevolmente all'impiego di algoritmi intelligenti.

[3] Sul versante penalistico il ventaglio delle possibili applicazioni è, in realtà, assai ampio a seguito del progredire della tecnologia. Secondo R. E. Kostoris, *Intelligenza artificiale, strumenti predittivi e processo penale*, in *disCrimen* (2024) 3 «Si va da strumenti di ricerca e di accesso a dati e informazioni, comprese quelle normative e giurisprudenziali, assai più potenti e sofisticati di quelli tradizionali, a strumenti in grado di utilizzare tecniche di scienza dei dati per contribuire a migliorare l'efficienza della giustizia, consentendo, ad esempio, di svolgere valutazioni quantitative e di effettuare proiezioni in rapporto a future risorse umane e di bilancio, a strumenti che possano coadiuvare il giudice nella sua stessa attività di sentencing, offrendo migliori parametri di controllo dei passaggi logico inferenziali del suo ragionamento (per tali ultime considerazioni vds. L. Luparia Donati, *Notazioni controintuitive su intelligenza artificiale e libero coinvolgimento*, Atti del convegno del Dipartimento di Scienze Giuridiche "Cesare Beccaria" dell'Un. Milano tenutosi online in data 15/10/2020, Milano, 2021, 117ss.). Così come sono pure utilizzabili impieghi dell'IA volti a potenziare le risorse e le capacità conoscitive del difensore, tali da ridurre l'asimmetria che tradizionalmente caratterizza il rapporto tra accusa e difesa (G. Lasagni, *Difendersi dall'intelligenza artificiale o difendersi con l'intelligenza artificiale? Verso un cambio di paradigma,* in G. Di Paolo, L. Pressacco (curr.), *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, Napoli, 2022, 65ss.). A questi strumenti si aggiunge poi la variegata galassia degli strumenti di tipo specificamente predittivo e degli strumenti che potremmo definire 'misti' in quanto combinano caratteristiche proprie degli strumenti predittivi con altre diverse, compresi i nuovissimi rivoluzionari strumenti di IA di tipo "generativo", rappresentati soprattutto da Chat GPT (v. A. Garapon-J. Lassegue, *La giustizia digitale. Determinismo tecnologico e libertà*, ed. it. (cur.) M. Rosaria Ferrarese, 2021)».

Due, in effetti, sono le principali estrinsecazioni - che corrispondono a due specifiche e ben definite aree di intervento - che sono in grado di assumere gli strumenti intelligenti a seconda che questi incidano sull'attività della polizia giudiziaria o su quella svolta dall'organo giurisdizionale.
Mentre le tecniche di polizia predittiva ("predictive policing")[4] sono finalizzate a produrre i loro effetti sul piano investigativo, e servono dunque per prevenire la commissione dei reati[5], quelle di giustizia predittiva ("predictive sentencing") sono previste invece ad ausilio del giudice nell'elaborazione delle proprie decisioni[6].
Entrambe le suddette forme di intervento di IA, sebbene differenti, sono accomunate dalla elaborazione e l'incrocio di una vastissima mole di informazioni; a tal proposito si sente spesso parlare di "big data" provenienti da fonti diverse quali banche dati, "social networks", "databrokers", internet, impianti di videosorveglianza a circuito chiuso e così via[7].
A differenza di quelli a sostegno delle attività giurisdizionali in tutti i momenti del decidere, i modelli di "predictive policing" risulterebbero essere pienamente in linea tanto alle funzioni che l'art. 55, co. 1, c.p.p. attribuisce alla polizia giudiziaria la quale è chiamata al dovere, anche di propria iniziativa, di «prendere notizia dei reati, impedire che vengano portati a conseguenze ulteriori, ricercarne gli autori, compiere gli atti necessari per assicurare le fonti di prova e raccogliere quant'altro possa servire per l'applicazione della legge penale», quanto ancora a quelle indicate dall'art. 348, co. 1, c.p.p., secondo cui la polizia giudiziaria, successivamente alla comunicazione della notizia di reato al pubblico ministero, continua a svolgere le ricordate funzioni di cui all'art. 55 c.p. attraverso la raccolta di «ogni elemento utile alla ricostruzione del fatto e alla individuazione del colpevole».
Dietro queste molteplici e promettenti applicazioni dell'IA nel campo delle indagini si celano, però, alcune evidenti perplessità che sembrano mettere in crisi la classica ripartizione di competenze tra polizia di sicurezza e polizia giudiziaria[8].

[4] Il fenomeno della cd. "predictive policing" è già da diverso tempo diffuso nei "police deparments" americani; tra gli studiosi contemporanei che se ne occupano vds., senza pretesa di esaustività, J. McDaniel, K. Pease (curr.), *Predictive Policing and Artificial Intelligence*, Oxon-New york, 2021, *passim*; A. G. 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* 94.5 (2017) 1109; Id., *Illuminating Black Data Policing*, in *Ohio State Journal of Criminal Law*, 15 (2018) 503ss.; E. E. Joh, *Artificial Intelligence and Policing: First Questions,* in *Seattle University Law Review* 41 (2018) 1139ss.; Id., *Feeding the Machine: Policing, Crime Data, & Algorithms*, in *William & Mary Bill of Rights Journal*, 26 (2017) 287ss. Storicamente, il merito per aver realizzato il primo modello di polizia predittiva deve attribuirsi a William J. Bratton, commissario della polizia di New York, ed al suo vice, Jack Maple, i quali idearono nell'aprile dell'anno 1994 *CompStat*, un modello di gestione informatico che, sulla base di alcuni questionari sottoposti settimanalmente a capitani, tenenti ed altri vertici della polizia e, dunque, attraverso calcoli statistici che gli permettevano di tracciare i crimini commessi in città, rendeva possibile la realizzazione di una strategia efficace di prevenzione del crimine. Per qualche riferimento sullo strumento in commento cfr. J.J. Willis, S.D. Mastrofski, D. Weisburd, *Compstat in Practice: An In-Depth Analysis of Three Cities*, in *National Policing Institute*, 4 (2003) nonché C. Smith, *The controversial crime-fighting program that changed big-city policing forever. Is Compstat's main legacy safe street – or stop and frisk?,* in *Intelligencer* (2018).
[5] F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Dir. pen. cont*. (2019) 10.
[6] L'espressione giustizia predittiva, infatti, si può senz'altro riferire anche alla decisione giudiziale adottata da un computer che apprende dalla propria esperienza; così M. Barberis, *Giustizia predittiva: ausiliare e sostitutiva. Un approccio evolutivo*, in *Milan Law Review* (2022) 7.
[7] Circa l'impiego dei *big data* a tale scopo si veda anche A. Bonfanti, *Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in *Rivista di diritto dei media – MediaLaws* (2018) 207.
[8] R. Orlandi, *Il sistema di prevenzione tra esigenze di politica criminale e principi fondamentali*, in *DisCrimen* (2015) 5ss.

2.- **La prevenzione del crimine attraverso l'individuazione degli "hotspots" e la ricerca del "crime-linking". Cenni sull'esperienza italiana.**

I sistemi di polizia predittiva in grado di prevedere il crimine possono essere annoverati in due grandi categorie a seconda che gli stessi ricerchino il luogo o più direttamente gli individui.

Alla prima categoria appartengono tutti quei sistemi che individuano le cd. zone calde ("hotspots"), cioè quei luoghi che potrebbero costituire un potenziale teatro di commissione di reati.

Quando la macchina considera una zona a rischio criminale le forze di polizia fanno convogliare su di essa specifici servizi di pattugliamento[9], agevolati dallo sviluppo di alcune mappe in formato digitale che evidenziano a questi ultimi le aree che corrispondono esattamente a quelle verso cui sarà indirizzato il personale[10].

Sul fronte delle indagini italiane, nel 2013, l'ispettore superiore della polizia di Stato Elia Lombardo creava "X-Law", strumento in grado di individuare quelle che nel gergo poliziesco sono chiamate riserve di caccia, ossia quei territori che con una certa ciclicità[11] più si prestano, per gli individui che li frequentano, ad essere colmi di "prede appetibili" (per la presenza di turisti, studenti, professionisti ecc.) in quanto particolarmente affollati (scuole, uffici di lavoro, esercizi commerciali, mercati, stazioni ecc.)[12].

A differenza di quelli focalizzati sugli "hotspots", i sistemi di polizia predittiva che si concentrano direttamente sulle persone fisiche al fine di ridurre il livello di criminalità appartengono, invece, ai modelli cd. "person-based" poiché in grado di indagare se e quando determinati soggetti, che presentano alcune caratteristiche, commetteranno il prossimo reato[13].

Con riguardo all'esperienza italiana può essere ricordato che, anche in questo caso, e nemmeno molte recentemente, esattamente nel 2008, Mario Venturi, ex assistente capo della questura di Milano, progettava il software chiamato *"*Keycrime", strumento all'avanguardia nel campo della "predictive policing" capace di individuare (o di provare a farlo) - prendendo in considerazione molti elementi spesso tralasciati dagli investigatori che non fanno ricorso a tali strumentazioni - la serialità dei reati commessi da uno stesso individuo o da un gruppo criminale ai danni di diversi esercizi commerciali della città meneghina[14]; il risultato ottenuto da "Keycrime", che ora si tenta di sostituire con il più avanguardistico software Giove[15], è infatti quello di scoprire il nominativo di un possibile colpevole

---

[9] L. Grossi, *Software predittivi e diritto penale*, in A. Giraldi, L. Grossi, A. Massaro, L. Notaro, P. Sorbello (curr.), *Intelligenza artificiale e giustizia penale* Roma, 2020, 163; sullo stesso tema vds. anche G. Tavella, *Polizia predittiva e smart city: vecchie e nuove sfide per il diritto penale,* in *Fondazione Leonardo Civiltà delle Macchine Umanesimo Digitale* (2021) 12.

[10] Pietrocarlo, *Predictive policing* cit., 7.

[11] La cd. riserva di caccia è infatti una zona che nel tempo conserva determinate caratteristiche in quanto presenta delle circostanze favorevoli per chi vi delinque che ne agevolano l'impunità e la reiterazione delle condotte criminose; cfr. A.F. Uricchio, G. Riccio, U. Ruffolo (curr.), *Intelligenza Artificiale tra etica e diritti. Prime riflessioni a seguito del libro bianco dell'Unione europea*, Bari 2020, 93ss.

[12] F. Corona, *La decisione del giudice tra precedente giudiziale e predizione artificiale*, in *Democrazia e Diritti Sociali* (2023) 94.

[13] Diversi gli autori che se ne occupano, tra i quali Basile, *Intelligenza artificiale e diritto penale* cit., 12; C. Parodi, V. Sellaroli, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Dir. Pen. Cont.* (2019) 56; E. Esposito, *Nuovi strumenti di lotta all'illegalità, riflessioni nell'era dell'intelligenza artificiale*, in *Riv. Pen. Diritto e Procedura* (2024) 7; Polidoro, *Tecnologie informatiche e procedimento penale* cit., 8.

[14] Per una accurata descrizione di "Keycrime" proveniente dal suo ideatore M. Venturi*, Keycrime- La chiave del crimine*, in *Profiling- I profili dell'abuso* 4 (2014).

[15] Vds., a tal proposito, K. Carboni, *Cosa sappiamo di Giove, il software italiano di polizia predittiva*, in *Wired* (2023).

attraverso un algoritmo che avrà individuato e selezionato (al posto degli operatori) tutte le eventuali e possibili correlazioni tra l'individuo ed il fatto di reato verificatosi[16].

3.- **Un efficace "tool" di riconoscimento facciale italiano: il S.A.R.I.**

Una particolare tipologia di software di IA che opera con modelli cd. "person-based", che poggia dunque anch'essa in buona parte sulla tecnica del "crime-linking", è quella che applica le tecnologie di riconoscimento facciale[17], così definite perché in grado di identificare un individuo sulla sola base delle caratteristiche del suo volto.

Più nel dettaglio, tali sistemi sarebbero in grado di riconoscere, attraverso l'incrocio di immagini fotografiche raccolte in precedenza ed inserite in un enorme database, l'identità di un soggetto ignoto, anche attraverso il confronto con immagini appartenenti a persone fisiche note.

L'associazione tra i volti che questi software compiono parte dall'esame delle cd. impronte facciali, ossia di quei tratti fisici che, sebbene comuni, sono diversi ed originali in ciascuno di noi[18]. Ogni corpo, inoltre, nell'attuale era tecnologica, può essere considerato «una miniera a cielo aperto dalla quale attingere dati ininterrottamente»[19].

Proprio da questa idea di fondo nasce il Sistema Automatico di Riconoscimento d'Immagini (il cui acronimo è S.A.R.I.), "facial recognition tool" italiano trai i più all'avanguardia al mondo e creato nel 2017 dalla azienda italiana Parsec 3.26 srl[20], vincitrice della gara d'appalto indetta dal dipartimento di pubblica sicurezza del Ministero dell'Interno.

Il S.A.R.I. è progettato per operare secondo due differenti modelli.

Mentre il S.A.R.I. "Enterprise" è "più banalmente" un applicativo che giunge ad un risultato, l'identificazione, attraverso il confronto del volto della persona sconosciuta non fotosegnalata con i volti di soggetti noti contenuti all'interno di una banca dati ministeriale denominata Casellario Centrale d'Identità (C.C.I.) – archivio nel quale sarebbero custoditi, per ciascun soggetto sottoposto a fotosegnalamento, circa diciotto milioni di elementi comprensivi di dati biometrici, fotografici e impronte digitali[21] -, il S.A.R.I. "Real Time" analizza, in tempo reale, i volti ripresi dai sistemi a circuito chiuso installati in determinati luoghi, confrontandoli con quelli già presenti in una banca

[16] Fin dalle sue primissime applicazioni nella città di Milano "Keycrime" ha fatto registrare successi inaspettati e, dopo diversi anni dal suo utilizzo, si sono potuti raggiungere risultati considerevoli; se, ad esempio, nel 2008 il numero di rapine compiute era stato pari a seicentosessantaquattro, nel 2016 si sono potute registrare invece solo duecentottantatre episodi.

[17] Tra i tanti, R. Lopez, *La rappresentazione facciale tramite software*, in A. Scalfati (cur.), *Le indagini atipiche*, II ed., Torino 2019, 239 ss.; J. Della Torre, *Algoritmi di* facial recognition *e procedimento penale italiano*, Trieste 2023, 168ss.

[18] Si pensi a tutti i componenti del viso, partendo dai lineamenti per arrivare alla forma della fronte, naso, orecchie, bocca, posizione degli occhi e così via; cfr. M. Torre, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Riv. Dir. Pen. Proc*., 8 (2021) 1049. Secondo F. Di Matteo*, La riservatezza dei dati biometrici nello Spazio europeo dei diritti fondamentali: sui limiti all'utilizzo delle tecnologie di riconoscimento facciale,* in *Freedom, Security & Justice: European Legal Studies*, Napoli, 1 (2023) 74, la raccolta dei dati biometrici di un dato individuo si estende anche all'immagazzinamento all'interno del sistema di tratti peculiari ed altamente variopinti ed individuali come la voce, la firma, l'andatura, il modo di gesticolare o di camminare.

[19] L'espressione è di S. Rodotà, *Trasformazioni del corpo*, in *Pol. Dir*. (2006) 6.

[20] Per la specifica occasione la ditta italiana ha collaborato con il Centro di ricerca Istituto di Scienze Applicate e Sistemi Intelligenti (ISASI).

[21] Vds. A. Fonsi, *Prevenzione dei reati e riconoscimento facciale: il parere sfavorevole del Garante Privacy sul sistema SARI Real Time*, in *Riv. Pen. Dir. proc*. (2021) 6. Per qualche osservazione di carattere tecnico cfr. L. Saponaro, *Le nuove frontiere tecnologiche dell'individuazione personale*, in *Arch. Pen*., 7.

dati più ristretta di persone ricercate, una "watch list", capace di immagazzinare un massimo di diecimila volti, e genera infine un "alert" nel caso in cui è rilevata una corrispondenza con taluno dei volti "sospetti"[22].

3.1.- **Alcune analoghe esperienze di biometria facciale in Europa.**

Oltre che l'Italia, anche altri Paesi dell'Unione Europea hanno adottato sistemi di riconoscimento facciale che lavorano in maniera simile al S.A.R.I., tanto nella sua veste statica che dinamica.

In Francia, ad esempio, già da diverso tempo la polizia utilizza strumenti di riconoscimento facciale negli spazi pubblici e ad oggi si serve di un software biometrico chiamato A.L.I.C.E.M.[23] capace di creare un database nazionale con all'interno l'identità digitale di tutti i cittadini francesi[24].

In Germania ancora aperto è il dibattito sull'utilizzo della tecnologia di riconoscimento facciale nei luoghi pubblici e le autorità di alcuni stati federali, tra cui la Sassonia e Berlino, hanno iniziato a utilizzare modelli di riconoscimento all'avanguardia in grado di elaborare le immagini facciali quasi in tempo reale[25].

In molti altri Stati Membri, oltre a quelli considerati, le autorità giudiziarie o di polizia utilizzano sistemi di riconoscimento biometrico all'interno delle loro indagini[26]. Uno studio commissionato dal gruppo dei Verdi del Parlamento europeo circa l'impatto della tecnologia sui diritti fondamentali ha infatti individuato nella Finlandia, Austria, Grecia, Ungheria, Lettonia, Lituania, Slovenia e Paesi Bassi gli Stati che impiegano tecnologie di riconoscimento facciale a scopo investigativo-identificativo e si stima che presto anche la Croazia, Cipro, Cechia, Estonia, Portogallo, Romania, Spagna e Svezia adotteranno la stessa tecnologia all'interno dei loro protocolli investigativi[27].

4.- **Le problematiche poste dal S.A.R.I. "Real Time" anche a seguito dell'approvazione dell'"AI Act".**

Con specifico riguardo allo Stato italiano il Garante della privacy ha svolto, per entrambi i modelli di S.A.R.I., due approfondite istruttorie allo scopo di indagare le loro compatibilità con i diritti fondamentali dell'individuo.

Le conclusioni cui quest'ultimo è addivenuto non sono particolarmente sorprendenti se si considera il fatto che esse si fondano sulla sostanziale differenza che esiste tra le due ricordate differenti tipologie di attività.

Quanto al S.A.R.I. "Enterprise" dev'essere evidenziato che un provvedimento del 26 luglio 2018, n. 440 del Garante della Privacy ne ha sancito sin da subito l'inesistenza di «criticità sotto il profilo della protezione dei dati»[28]. All'interno dello stesso è stato infatti osservato che questo primo applicativo

[22] M. Soffientini, *Riconoscimento facciale: nuova disciplina*, in *Dir. e prat. lav*., 9 (2022) 34.
[23] Acronimo di "Application de lecture de l'identitè d'un citoyen en mobilitè".
[24] Su tale sofisticato progetto vds. D. Conti, *ALICEM: la nuova Identità Digitale per i cittadini francesi*, 3 agosto 2023, in www.investigazioni-italia.com.; M. Mazzarella, *Tra Francia e Italia: Alicem e SPID da confronto*, 23 aprile 2020, reperibile all'indirizzo www.irpa.eu.
[25] La fonte è tratta da *Allarme Privacy: Germania sotto il Fuoco del Dibattito sul Riconoscimento Facciale*, 17 maggio 2024, reperibile al sito www.redhotcyber.com.
[26] Vds. *Studio Verdi, riconoscimento facciale già in uso in 11 Stati membri. Altri 8 Stati membri seguiranno l'esempio, preoccupa diffusione 'progetti pilota'*, 29 ottobre 2021, in www.ansa.it.
[27] *Ibidem*.
[28] Cfr. il provvedimento del Garante della Privacy, Sistema automatico di ricerca dell'identità di un volto, 26/7/2018, n. 440.

di IA si limiterebbe ad automatizzare alcune operazioni che prima richiedevano l'inserimento manuale di connotati identificativi[29] e, per tale ragione, non si sostanzierebbe in un nuovo trattamento di dati personali ma solo in una nuova modalità di trattamento dei dati biometrici che agevola l'operare delle forze dell'ordine. Un «mero ausilio [cioè] dell'agire umano avente lo scopo di velocizzare l'identificazione, da parte dell'operatore di polizia, di un soggetto ricercato della cui immagine facciale si disponga, ferma restando l'esigenza dell'intervento dell'operatore per verificare l'attendibilità dei risultati prodotti dal sistema automatizzato»[30]. Stante, dunque, la presenza di modalità applicative piuttosto elementari, a livello normativo il S.A.R.I. "Enterprise" si è da sempre giovato (e così ancora oggi) di una solida base normativa in grado di sollevarlo da eventuali profili di illegittimità[31], anche rispetto al Regolamento generale sulla protezione dei dati 2016/679 del Parlamento europeo e del Consiglio datato 27 aprile 2016 (nell'acronimo anglosassone G.D.P.R.)[32], il cui contenuto non sembra in effetti porsi in alcuna contraddizione con il modo in cui tale modello di IA opera che si mostra pienamente compatibile con le garanzie procedurali previste dalla disciplina europea a protezione dei diritti delle persone fisiche in occasione del trattamento dei propri dati personali; quest'ultimo, in effetti, risulterebbe lecito; comunque limitato a scopi specifici di prevenzione, indagine, accertamento e perseguimento di reati nonché all'esecuzione di sanzioni penali e alla salvaguardia della sicurezza pubblica; trasparente circa il motivo, il metodo e la finalità stessa del trattamento dei dati sensibili; adeguatamente protetto.

Al contrario, alcuni dubbi solleva la seconda versione del S.A.R.I., quella più avanzata che interagisce in "Real Time".

Nonostante l'art. 5, lett. h, del Regolamento in materia di IA ("AI Act"), approvato il 21 maggio dello scorso anno dal Consiglio dell'Unione Europea, contenga un apposito divieto di utilizzo del riconoscimento facciale in "real time" in luoghi aperti al pubblico[33], sono al suo interno inserite una molteplicità di deroghe, tutte incentrate su finalità *lato sensu* penalistiche, che rendono quel divieto particolarmente vago. In primo luogo, infatti, sebbene ne sia consentito l'utilizzo per la ricerca di

[29] *Ibidem.*

[30] *Ibidem*.

[31] Ad esempio, gli artt. 4 e 7 del T.U.L.P.S. permettono all'autorità di pubblica sicurezza di ordinare l'esecuzione di rilievi segnaletici, descrittivi, fotografici, dattiloscopici e antropometrici nei confronti di persone pericolose o sospette e di coloro che non sono in grado o si rifiutano di provare la loro identità; l'art. 5, co. 2 bis, D.lgs. 286 del 1998 prevede il necessario compimento dei rilievi dattiloscopici nei confronti dello straniero che richiede il permesso di soggiorno; sotto il profilo *strictu sensu* processuale penale, ancora, l'art. 349, co. 2, c.p.p. consente a tali dispositivi di rientrare tra gli strumenti di identificazione delle persone nei cui confronti vengono svolte le indagini, quale attività compiuta dalla polizia giudiziaria anche attraverso rilievi fotografici.

[32] Come noto, il citato regolamento europeo, che provvedeva a sostituire la previgente disciplina dettata dalla direttiva 95/46/CE, è stato recepito con il d.lgs. 10 agosto 2018, n. 101 recante disposizioni per l'adeguamento della normativa nazionale a quella comunitaria. Per riferimenti in dottrina, anche con riguardo alle precedenti discipline in vigore nella stessa materia, tra i tanti, Destito, *Dati personali (tutela penale dei)*, in *Dig. Disc. Pen*., I agg., 2008, 1-3.

[33] Sull'impiego del S.A.R.I. nella sua veste dinamica, peraltro, il Garante della privacy italiano aveva espresso il 25 marzo 2021 uno specifico parere negativo che ne sconsigliava l'utilizzo perché in violazione della disciplina di cui al D.lgs. 51 del 2018 sull'adozione della direttiva (UE) 2016/80 in materia di trattamento di dati personali. Celebre la sanzione, pari a venti milioni di euro, che, nel 2022, il Garante italiano infliggeva alla società americana "Clearview AI" per avere sviluppato una piattaforma di riconoscimento facciale che coinvolgeva persone che si trovano anche sul territorio italiano. Per un primo commento sull'"AI Act" v. G. Cassano, E.M. Tripodi (curr.), *Il Regolamento Europeo sull'Intelligenza Artificiale*, Rimini, 2024. Per qualche commento sul caso "Clearview", cfr. invece I.N. Rezende, *Facial recognition in police hands: Assessing the "Clearview case" from a European perspective*, in *New Journal of European Criminal Law* (2020) 375ss.

vittime di gravi reati[34], il S.A.R.I. "Real Time" è impiegato anche per la ricerca di persone scomparse che potrebbe non avere alcun profilo di aggancio con la sfera penalistica[35]. Con una logica tutta preventiva e securitaria, poi, l'utilizzo di sistemi di identificazione biometrica dinamica è consentito per la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico; e ciò fa intendere come quest'ultima specifica possibilità sia verosimilmente concessa ad ausilio di investigazioni già in corso per altri fatti[36]. In ultimo, stando sempre al dato euro-normativo, sistemi come il S.A.R.I. "Real Time" potrebbero essere utilizzati - a fini investigativi e per l'esercizio dell'azione penale o per l'esecuzione di una condanna a pena detentiva non inferiore a quattro anni - per la localizzazione o l'identificazione di persone sospettate di aver commesso uno tra i reati compresi nell'Allegato II tra i quali sono indicati, oltre a quelli di terrorismo e tratta di esseri umani su ricordati, anche quelli di «sfruttamento sessuale di minori e pornografia minorile, traffico illecito di stupefacenti o sostanze psicotrope, traffico illecito di armi, munizioni ed esplosivi, omicidio volontario, lesioni gravi, traffico illecito di organi e tessuti umani, traffico illecito di materie nucleari e radioattive, sequestro, detenzione illegale e presa di ostaggi, reati che rientrano nella competenza giurisdizionale della Corte penale internazionale, illecita cattura di aeromobile o nave, violenza sessuale, reato ambientale, rapina organizzata o a mano armata, sabotaggio, partecipazione a un'organizzazione criminale coinvolta in uno o più dei reati elencati sopra»[37].

5.- **Rischi di profilazione e attività investigativa proattiva. Il pericoloso arretramento delle indagini da strumenti di repressione a strumenti di prevenzione.**

Le poche considerazioni che precedono inducono a ritenere che, tra quelli nei quali può esplicarsi l'IA, il terreno investigativo è di certo uno dei più proficui dell'interazione uomo-macchina[38].

A tal riguardo basti solo ricordare la particolare efficacia che strumenti di "predictive policing" e di riconoscimento facciale sono in grado di sprigionare sul fronte delle indagini. Questi ultimi avrebbero perfino la capacità di assolvere ad una tra le attività più basilari svolte dalla polizia giudiziaria, l'identificazione.

Quando è assistita dal lavoro dei software predittivi quella centrale attività di identificazione si tramuta in un qualcosa di più completo, in una vera e propria attività di profilazione costituita da un insieme di operazioni più complesse come la raccolta dei dati personali e delle abitudini caratteristiche di qualcuno[39]. Anche a livello europeo i già ricordati "tools" di riconoscimento facciale sono stati definiti come meccanismi che consentono di analizzare «immagini digitali contenenti volti

[34] Quali sottrazione, tratta e sfruttamento sessuale.
[35] Cfr. S. Quattrocolo, *Intelligenza artificiale e processo penale: le novità dell'Ai Act*, in *Diritto di Difesa*, Milano (2025).
[36] *Ibidem*.
[37] Vds. Regolamento (UE) 2024/1689, Allegato II.
[38] Nella fase delle indagini si fa un uso sempre più ampio di sistemi fondati sull'IA e questo impiego sarà destinato a crescere notevolmente con la diffusione dell'*Internet of Things*; cfr. per queste considerazioni M. Gialuz, *Prove fondate sull'Intelligenza Artificiale e diritti fondamentali*, in *Diritto di Difesa,* Milano (2025) nonché U. Pagallo, S. Quattrocolo, *The impact of AI on criminal law, and its twofold procedures*, in W. Barfield, U. Pagallo (curr.), *Resarch Handbook on the Law of Artificial Intelligence*, Cheltenham-Northampton, 2018, 385; S. Quattrocolo, *Equo processo penale e sfide della società algoritmica*, in *BioLaw Journal*, 1 (2019) 138.
[39] La definizione è tratta dalla voce profilazione, in www.treccani.it.

di individui, per scopi di identificazione, autenticazione/verifica, o categorizzazione di suddetti individui»[40].

Tecnologie particolarmente invasive come quella utilizzata dal S.A.R.I. corrono il rischio di trasformare l'attività di sorveglianza svolta da quest'ultimo da adempimento specifico nei confronti di taluni soggetti (che, peraltro, in base all'art. 349 c.p.p., dovrebbero essere solo la persona nei cui confronti sono svolte le indagini e le persone in grado di riferire su circostanze rilevanti per la ricostruzione dei fatti) ad osservazione *tout court* per finalità di pubblica sicurezza rivolta indistintamente a tutti i consociati[41].

È proprio in casi come questi – ma si pensi anche alle poderose operazioni di "web scraping" eseguite dagli investigatori - che più aumenta il pericolo di intersezioni tra attività pre-investigative affidate alla polizia in funzione di sicurezza e attività preliminari del procedimento penale di esclusiva competenza della polizia giudiziaria[42]. Più, infatti, accrescono gli spazi di intervento delle forze dell'ordine e degli organi di intelligence, più sembra affermarsi quel *tertium genus* di attività investigativa cd. proattiva[43] in grado di avvalersi di strumenti tecnologici di inedita invasività anche prima della acquisizione della notizia di reato.

Malgrado, dunque, sia innegabile lo sforzo profuso dal legislatore unitario nella regolamentazione di alcuni tra i più insidiosi strumenti di IA, come quelli di identificazione biometrica, l'uso poliziesco dell'IA sembrerebbe prestare il fianco ad un consistente arretramento dell'asse delle indagini penali dalla tradizionale sfera repressiva a quella preventiva col rischio di trascinare con sé evidenti ricadute nei rapporti tra attività amministrativa e attività giurisdizionale[44].

Abstract.- Tra tutti i settori della giustizia penale, quello della prevenzione del crimine è di certo uno fra i più battuti dall'Intelligenza Artificiale.

Nel campo delle attività investigative gli strumenti che si servono di sistemi esperti sono infatti in grado di semplificare le funzioni della polizia giudiziaria a partire dal momento della ricerca della

[40] V. Gruppo di lavoro "Articolo 29", parere 2/2012 – WP 192, adottato il 22 marzo 2012.

[41] È appena il caso di rilevare come anche a livello ministeriale siano state tentate altre strade normative per giustificare l'impiego del S.A.R.I. a scopo investigativo. Una di esse è quella che suggerisce l'ingresso degli algoritmi di riconoscimento facciale nella scena procedimentale ai sensi dell'art. 359 c.p.p. in materia di accertamenti tecnici ripetibili del pubblico ministero; cfr. sul punto Della Torre, *Quale spazio per i* tools *di riconoscimento facciale nella giustizia penale?* cit., 41ss. il quale manifesta a proposito qualche perplessità, anche relativamente alla riconducibilità di quei sistemi agli accertamenti urgenti sulle persone della polizia giudiziaria di cui all'art. 354 c.p.p., al prelievo coattivo di campioni biologici su persone viventi compiuto dal pubblico ministero, ai provvedimenti del giudice per le perizie che compiono atti idonei ad incidere sulla libertà personale ex art. 224 bis c.p.p.

[42] La considerazione è di A. Scalfati, *Il fermento pre-investigativo*, in A. Scalfati, *Pre-investigazioni (Espedienti e mezzi)*, Torino, 2020, 4ss.; è utile osservare che, meno recentemente, M. Nobili, *Atti di polizia amministrativa utilizzabili nel processo penale e diritto di difesa: una pronunzia marcatamente innovativa*, in *Foro it*., I, 1984, 375 ss. già parlava a tal proposito di una chiara distinzione tra «atti di polizia amministrativa e di polizia giudiziaria», pur individuando la presenza di operazioni «a carattere o finalità mista».

[43] A. Nascimbeni, *«Fermento pre-investigativo» e analisi automatizzata di dati*, in *Arch. Nuova. Proc. Pen*., 6 (2024), 558. Su tale categoria di indagine cd. proattiva, che si affianca a quella tradizionale *post delictum*, R. E. Kostoris, *La lotta al terrorismo e alla criminalità organizzata tra speciali misure processuali e tutela dei diritti fondamentali nella risoluzione del XVIII congresso internazionale di diritto penale*, in *Riv. Dir. Proc*. (2010) 328 ss. Per alcuni riferimenti in giurisprudenza con particolare riguardo al ruolo svolto da alcune tipologie di attività investigativa cd. proattiva e alla necessità di non disperdere importanti prove acquisite prima ancora della instaurazione del procedimento vds. Cass., sez. VI, 27/05/2021, n. 33751, in *CED Cass.,* n. 281981; Cass., sez. V, 5/02/2021, n. 12062, *ivi*, n. 280758 nonchè Cass., sez. V, 6/10/2020, n. 31831, *ivi*, n. 279776.

[44] Nascimbeni, *«Fermento pre-investigativo»* cit., 558.

notizia di reato per arrivare alla assicurazione delle fonti di prova e alla comunicazione al pubblico ministero della *notitia criminis* acquisita.
Anche in Italia, così come è avvenuto in alcuni Paesi dell'Unione Europea, hanno fatto ingresso alcuni strumenti di riconoscimento facciale, come il S.A.R.I. che ha imposto importanti riflessioni non solo circa il suo impiego da parte del Garante della privacy ma anche sotto il versante normativo alla luce della recente disciplina contenuta nell'AI Act.
Tale sistema, soprattutto quando utilizzato nella sua versione dinamica, indubbiamente avanguardistica, promette di identificare con semplicità un soggetto ignoto attraverso l'incrocio di immagini fotografiche raccolte da telecamere installate in determinati luoghi e di giungere perfino a rilevarne corrispondenze con taluno dei volti noti "sospetti" inseriti in un database.
Dietro queste molteplici e promettenti applicazioni dell'IA nel campo delle indagini e, più nello specifico, di quella investigazione che viene definita proattiva si celano, tuttavia, evidenti perplessità che mettono a dura prova la classica ripartizione di competenze tra polizia di sicurezza e polizia giudiziaria.

Of all the areas of criminal justice, crime prevention is certainly one of the most impacted by Artificial Intelligence.
In the field of investigative activities, tools that use expert systems can streamline the functions of the judicial police, from the moment of searching for information about a crime to securing sources of evidence and communicating the acquired *notitia criminis* to the public prosecutor.
Italy, as has happened in some European Union countries, has seen the introduction of facial recognition tools, such as SARI, which has prompted significant consideration not only regarding its use by the Italian Data Protection Authority but also from a regulatory perspective, in light of the recent provisions contained in the AI Act.
This system, especially when used in its undoubtedly cutting-edge dynamic version, promises to easily identify an unknown subject by cross-referencing photographic images collected by cameras installed in specific locations and even detecting matches with some of the known "suspicious" faces stored in a database.
Behind these many promising applications of AI in investigations, and more specifically, in what is known as proactive investigations, however, lie clear concerns that severely challenge the traditional division of responsibilities between security police and judicial police.