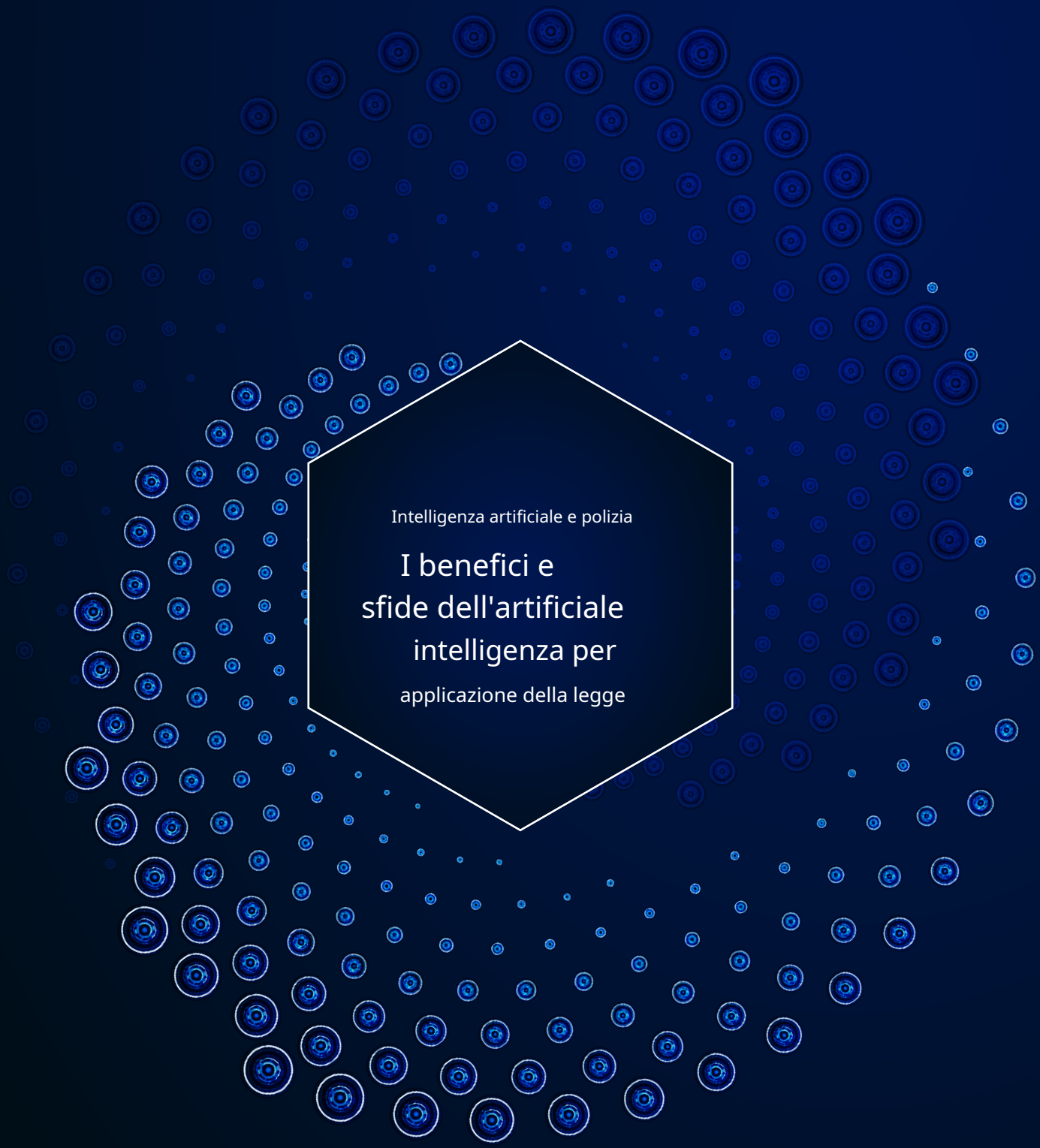
EUROPOL



Intelligenza artificiale e polizia

I benefici e sfide dell'artificiale intelligenza per applicazione della legge

Un rapporto dell'osservatorio dell'Europol Innovation Lab

IA E POLIZIA
I VANTAGGI E LE SFIDE DELL'INTELLIGENZA ARTIFICIALE PER LE FORZE DELL'ORDINE Un rapporto dell'osservatorio dell'Europol Innovation Lab

PDF | ISBN 978-92-95236-35-6 | ISSN 2600-5182 | DOI: 10.2813/0321023 | QL-01-24-000-IT-N

Lussemburgo: Ufficio delle pubblicazioni dell'Unione europea, 2024

Citare questa pubblicazione: Europol (2023), La seconda rivoluzione quantistica – L'impatto dell'informatica quantistica e delle tecnologie quantistiche sulle forze dell'ordine, rapporto dell'osservatorio dell'Europol Innovation Lab, Ufficio delle pubblicazioni dell'Unione europea, Lussemburgo.

Questa pubblicazione e ulteriori informazioni su Europol sono disponibili su Internet.

www.europol.europa.eu

Contenuto

Prefazione

L'Intelligenza Artificiale (IA) cambierà profondamente il panorama delle forze dell'ordine, offrendo strumenti e opportunità innovativi per migliorare le nostre capacità di tutelare la sicurezza pubblica. Questo fiorente campo tecnologico promette di rivoluzionare il modo in cui analizziamo set di dati complessi, miglioriamo le metodologie forensi e sviluppiamo canali di comunicazione sicuri.

Tuttavia, parallelamente a questi progressi, l'intelligenza artificiale introduce nuove sfide e potenziali vulnerabilità, in particolare in ambiti quali la privacy dei dati e l'integrità delle decisioni basate sull'intelligenza artificiale.
È fondamentale affrontare questi progressi con un approccio strategico, bilanciando l'innovazione con le implicazioni etiche e l'impatto sociale.

Poiché Europol è in prima linea nell'adozione dell'innovazione tecnologica nell'ambito delle forze dell'ordine, siamo pienamente consapevoli della necessità di rimanere al passo con questi sviluppi. Questo rapporto dell'Osservatorio dell'Innovazione dell'Europol non è solo una testimonianza del nostro impegno nell'adottare l'IA in modo responsabile, ma anche una guida per la comunità europea delle forze dell'ordine mentre entriamo in questa nuova era di polizia digitale.

Spero che questo rapporto contribuisca a far luce sulle complesse dinamiche dell'intelligenza artificiale per le attività di polizia, fornendo spunti preziosi ai nostri stakeholder e aiutando le forze dell'ordine nel loro percorso verso un'adozione responsabile del potenziale dell'intelligenza artificiale. Insieme, intraprendiamo questo viaggio, pronti ad affrontare le sfide e a cogliere le opportunità che la rivoluzione dell'intelligenza artificiale presenta, garantendo la nostra capacità di continuare a proteggere e servire le nostre comunità in un mondo sempre più digitale.

Catherine De Bolle
Direttore esecutivo dell'Europol

Esecutivo Riepilogo

Questo rapporto mira a fornire alle forze dell'ordine una comprensione completa delle varie applicazioni e utilizzi dell'intelligenza artificiale (IA) nelle loro operazioni quotidiane. Si propone di fungere da manuale per i professionisti della sicurezza interna, offrendo indicazioni su come implementare le tecnologie di IA in modo responsabile e conforme. Oltre a illustrare i potenziali vantaggi e le applicazioni innovative dell'IA, come l'analisi dei dati basata sull'IA, il rapporto mira anche a sensibilizzare sulle potenziali insidie e sulle considerazioni etiche dell'uso dell'IA nelle forze dell'ordine. Affrontando queste sfide, il rapporto si propone di fornire ai professionisti delle forze dell'ordine le conoscenze necessarie per affrontare le complessità dell'IA, garantendone un impiego efficace ed etico nel loro lavoro. Il rapporto si concentra su set di dati di grandi dimensioni e complessi, sull'intelligence open source (OSINT) e sull'elaborazione del linguaggio naturale (NLP). Approfondisce inoltre il campo dell'informatica forense, della visione artificiale, della biometria e accenna al potenziale dell'IA generativa.

L'uso dell'IA da parte delle forze dell'ordine è sempre più esaminato a causa delle sue dimensioni etiche e sociali. Il rapporto cerca di affrontare le preoccupazioni relative a distorsioni dei dati, equità e potenziali violazioni della privacy, della responsabilità, della tutela dei diritti umani e della discriminazione. Queste preoccupazioni diventano particolarmente rilevanti nel contesto della legge sull'intelligenza artificiale dell'UE (Legge UE sull'IA), di cui questa relazione fornisce una panoramica, nonché del suo contesto più ampio. La relazione sottolinea l'importanza del prossimo regolamento, descrivendone dettagliatamente gli obiettivi, la portata e le principali disposizioni. Vengono inoltre discusse le implicazioni della legge per le forze dell'ordine, sottolineando l'equilibrio tra la promozione dell'innovazione e la garanzia di un uso etico che vada oltre la conformità.

Al centro del rapporto c'è la valutazione di come le forze dell'ordine possano mantenere un delicato equilibrio tra lo sfruttamento dei vantaggi dell'IA e la gestione delle sue limitazioni intrinseche. Vengono elaborate strategie per affrontare pregiudizi, problemi di privacy e il ruolo fondamentale dei quadri normativi di responsabilità. Il rapporto sottolinea l'importanza di contesti normativi innovativi.

La sezione conclusiva prevede la traiettoria dell'IA nelle forze dell'ordine, sottolineando i potenziali progressi tecnologici all'orizzonte. Sottolinea inoltre la necessità di ottenere fiducia e accettazione da parte del pubblico, nonché l'importanza della collaborazione e della condivisione delle conoscenze. Questo documento completo funge sia da guida che da strumento di riflessione per le parti interessate interessate alla confluenza tra IA e forze dell'ordine nel panorama europeo.

Introduzione

Sfondo

Nel panorama in continua evoluzione delle forze dell'ordine, l'intelligenza artificiale (IA) si è affermata come uno strumento trasformativo, apportando capacità che potrebbero rivoluzionare completamente le attività di polizia. Le forze dell'ordine (LEA), sia nell'Unione Europea (UE) che a livello globale, si trovano ad affrontare sfide sempre più complesse. Dalla crescita esponenziale dei dati generati dai dispositivi digitali e dai servizi online alla natura complessa delle moderne attività criminali, è evidente che i metodi di polizia tradizionali da soli non sono sufficienti come risposta. Inoltre, la globalizzazione della criminalità[1], caratterizzato da minacce informatiche, traffici transfrontalieri e terrorismo internazionale, presenta uno scenario sempre più impegnativo che richiede soluzioni avanzate e innovative.

Alla luce di ciò, l'IA offre un'alternativa promettente. Impiegando tecnologie all'avanguardia, le forze dell'ordine possono affrontare molte di queste urgenti sfide. La potenza dell'IA nell'elaborazione di enormi quantità di dati e nel filtraggio di contenuti rilevanti, le sue capacità di modellazione dei dati e la sua capacità di identificare modelli e tendenze precedentemente non rilevabili dagli investigatori umani ne evidenziano il potenziale trasformativo. Oltre a ciò, l'uso dell'IA per compiti ripetitivi e ad alto consumo di risorse consente alle forze dell'ordine di lavorare in modo più efficiente con le loro risorse limitate e consente agli agenti di polizia di concentrarsi e dare priorità ai compiti più importanti.

Tuttavia, ciò ha un costo, poiché alcune applicazioni dell'IA nelle attività di polizia sollevano preoccupazioni in materia di privacy, pregiudizi e discriminazioni. Si teme che questi sistemi complessi e in qualche modo opachi possano arrecare più danni che benefici. Ad aggravare ulteriormente la complessità di questa nuova realtà è il nuovo quadro normativo dell'UE, denominato EU AI Act.[1]Questo quadro normativo introduce una serie di nuove linee guida e standard che avranno un impatto sui sistemi di intelligenza artificiale in uso nell'Unione Europea. Sebbene la legge miri a stabilire pratiche solide ed etiche a tutti i livelli, le forze dell'ordine dovranno rivedere, ed eventualmente modificare, i loro strumenti di intelligenza artificiale esistenti e futuri per garantirne la conformità. Alcune applicazioni dell'intelligenza artificiale, come l'identificazione biometrica – una pratica consolidata delle forze dell'ordine – dovrebbero essere rigorosamente limitate.[2]La legge UE sull'intelligenza artificiale influenzerà anche lo sviluppo dei sistemi futuri, rendendo indispensabile per la polizia collaborare strettamente con i ricercatori e gli sviluppatori di intelligenza artificiale, nonché con gli esperti di etica e privacy, per garantire che i nuovi sistemi siano in linea con le linee guida normative.

In questa prospettiva, metodi innovativi come sandbox regolatori e spazi dati[3]può servire come un

1 Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce norme armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (legge sull'intelligenza artificiale)

meccanismo adattivo nei casi in cui l'applicazione di tecnologie basate sull'intelligenza artificiale potrebbe ledere i diritti e le libertà degli interessati. Creando ambienti controllati in cui i nuovi strumenti di intelligenza artificiale possono essere testati e perfezionati utilizzando dati rappresentativi, senza conseguenze nel mondo reale, le forze dell'ordine possono garantire che tali strumenti soddisfino gli standard operativi e normativi prima di essere implementati. Questo approccio flessibile consente adeguamenti in tempo reale e promuove un ambiente innovativo di miglioramento continuo, posizionando le forze dell'ordine europee all'avanguardia nelle attività di polizia basate sull'intelligenza artificiale.

Obiettivi

L'obiettivo principale di questo rapporto è fornire una panoramica dei vantaggi e delle sfide associati all'adozione dell'IA da parte delle forze dell'ordine. Il rapporto intende fungere da risorsa informativa principalmente per le forze dell'ordine che operano in tutta l'UE, sebbene i principi fondamentali debbano essere applicabili a livello globale. Ciononostante, il rapporto rappresenta una risorsa preziosa per una vasta gamma di lettori.
Tra questi rientrano decisori politici, sviluppatori tecnologici, accademici, difensori dei diritti civili e il grande pubblico, sia all'interno dell'UE che a livello globale. Analizzando i potenziali vantaggi dell'integrazione dell'IA, questo rapporto mira a evidenziare come questa tecnologia in rapida evoluzione possa contribuire a migliorare l'efficienza, l'efficacia e le prestazioni complessive delle operazioni di polizia, nel rispetto degli standard etici e legali.

Sebbene l'enfasi di questo rapporto sia posta sulla comprensione delle applicazioni, delle implicazioni, dei vantaggi e delle sfide dell'IA nelle forze dell'ordine, non esplora gli intricati dettagli tecnici su come gli algoritmi o i sistemi di IA vengono sviluppati, addestrati e gestiti. Questa decisione è stata presa per mantenere l'accessibilità del rapporto e per dare priorità ai suoi obiettivi primari. I lettori interessati a un'analisi tecnica più approfondita dei sistemi di IA, delle loro architetture e dei meccanismi sottostanti sono invitati a consultare risorse tecniche specifiche. Tali fonti sono reperibili nelle note finali.

Punti chiave per applicazione della legge

L'intelligenza artificiale ha la capacità di trasformare in modo significativo le attività di polizia: dall'analisi criminale avanzata che rivela tendenze in enormi quantità di dati, alla biometria che consente l'identificazione rapida e univoca dei criminali.

L'integrazione di set di dati ampi e complessi e dell'elaborazione del linguaggio naturale nelle applicazioni di polizia consente di estrarre informazioni utili da vasti set di dati, migliorando la previsione delle risorse e l'efficienza operativa. Allo stesso tempo, queste tecnologie possono proteggere e tutelare i diritti alla privacy individuali.

Gli strumenti basati sull'intelligenza artificiale, anche nel contesto di OSINT e SOCMINT, elaborano dati non strutturati per fornire informazioni in tempo reale e migliorare la capacità di affrontare situazioni urgenti, come i crimini contro i minori e il terrorismo, in modo più efficace ed efficiente.

Tecnologie come la traduzione automatica sono fondamentali per facilitare la collaborazione internazionale tra le forze dell'ordine.

La fusione di intelligenza artificiale e dati biometrici può migliorare l'accuratezza dell'identificazione dei criminali, proteggendo al contempo la privacy degli individui non rilevanti.

L'intelligenza artificiale generativa rappresenta il passo successivo, passando dall'analisi passiva alla creazione attiva. Per le forze dell'ordine, offre una miniera di possibilità. Tuttavia, come ogni strumento, il suo potere risiede nella sua applicazione giudiziosa ed etica, bilanciando innovazione e responsabilità.

Lo sviluppo e l'implementazione efficaci delle tecnologie di intelligenza artificiale richiedono infrastrutture e competenze tecnologiche sostanziali, il che presenta sfide significative, in particolare per le agenzie di polizia più piccole.

Le forze dell'ordine devono districarsi in scenari legali ed etici complessi, investendo al contempo nella formazione e nella sensibilizzazione del personale per garantire un'adeguata gestione dei dati e pratiche di elaborazione responsabili.

Il rispetto della legge UE sull'intelligenza artificiale rappresenta un fondamentale atto di equilibrio, poiché impone alle forze dell'ordine di rispettare rigorosi standard etici, legali e di privacy, rendendo potenzialmente necessaria la rivalutazione degli strumenti di intelligenza artificiale esistenti.

La legge UE sull'intelligenza artificiale sfida le forze dell'ordine ad allocare risorse aggiuntive e a destreggiarsi tra le complessità della conformità. Ciò è particolarmente rilevante per le agenzie che sviluppano internamente strumenti di intelligenza artificiale, sottolineando la necessità di un approccio responsabile ed etico all'integrazione dell'intelligenza artificiale nelle forze dell'ordine.

Le forze di polizia, che potrebbero già utilizzare determinati sistemi di intelligenza artificiale, dovranno affrontare il difficile compito di rivalutare questi strumenti. Qualora una di queste tecnologie operative rientrasse nella categoria vietata dalla legge UE sull'intelligenza artificiale, dovrebbe essere disattivata, con potenziali difficoltà nel mantenimento della continuità operativa.

È fondamentale affrontare i pregiudizi nell'intelligenza artificiale, con la necessità di sistemi che non siano solo tecnicamente validi, ma che incarnino anche equità, giustizia e imparzialità, garantendo che la raccolta e l'archiviazione dei dati rispettino rigorose linee guida sulla privacy.

Responsabilità, trasparenza e spiegabilità sono essenziali non solo per un utilizzo etico e responsabile dell'IA, ma anche per garantire che le prove raccolte e analizzate dai sistemi di IA resistano all'esame, rispettino il diritto a un giusto processo e siano considerate accettabili nei procedimenti giudiziari.

Sono essenziali verifiche periodiche dei sistemi di intelligenza artificiale per garantire la conformità agli standard stabiliti in materia di privacy e protezione dei dati, mantenendo un equilibrio tra lo sfruttamento delle informazioni basate sull'intelligenza artificiale e la salvaguardia dei diritti fondamentali e delle libertà individuali.

Applicazioni

dell'intelligenza artificiale nel diritto

applicazione

La tecnologia AI ha la capacità di trasformare radicalmente le attività di polizia: dall'analisi criminale avanzata che rivela tendenze in enormi quantità di dati, alla biometria che consente l'identificazione rapida e univoca dei criminali. Questa sezione esplora alcune delle principali applicazioni dell'AI nel campo delle forze dell'ordine. In questo modo, intendiamo fornire una panoramica delle capacità presenti e future che l'AI offre alle forze dell'ordine, tracciando un percorso verso un modello di polizia più efficiente, reattivo ed efficace.

Analisi dei dati

La capacità di analizzare enormi quantità di informazioni e di prendere decisioni efficaci e tempestive è diventata essenziale nell'era digitale. In settori come le forze dell'ordine, le decisioni devono spesso essere prese con risorse limitate e in contesti in cui il fattore tempo è determinante (ad esempio durante un'irruzione della polizia, un rapimento o una presa di ostaggi). Pertanto, l'incapacità di prendere decisioni ponderate potrebbe avere un profondo impatto sociale e conseguenze negative per le libertà e i diritti dei cittadini.

In sostanza, l'analisi dei dati implica l'estrazione di conoscenze e informazioni fruibili da dati grezzi e non elaborati. Fornisce un modo per identificare modelli, tendenze e collegamenti in vasti set di dati. L'avvento dell'intelligenza artificiale ha notevolmente potenziato le capacità dell'analisi tradizionale dei dati criminali. La capacità dei sistemi di intelligenza artificiale di apprendere e adattarsi in base ai dati, inclusi dati storici e altri dati criminali disponibili alle forze dell'ordine, consente agli analisti criminali di esplorare, elaborare e analizzare enormi quantità di informazioni in modo più efficiente e accurato di quanto qualsiasi essere umano potrebbe mai fare senza questo tipo di assistenza tecnica.

Ad esempio, utilizzando strumenti di analisi basati sull'intelligenza artificiale, gli investigatori possono analizzare milioni di transazioni finanziarie e rilevare anomalie, come movimenti sospetti di fondi, per identificare frodi.[4] Per le forze dell'ordine, ciò si traduce in una maggiore capacità di analizzare e comprendere i modelli di criminalità, individuare collegamenti tra indagini internazionali e sviluppare strategie su misura per sfide specifiche.

Questo potere trasformativo dell'IA non solo facilita l'elaborazione dei dati, ma arricchisce anche la qualità dei lead di intelligence generati. Ad esempio, laddove l'analisi tradizionale potrebbe semplicemente evidenziare il verificarsi di un picco di criminalità, l'analisi basata sull'IA potrebbe potenzialmente identificare cause sottostanti, correlazioni tra eventi esterni e non correlati, o persino modelli sottili che passerebbero inosservati nell'analisi manuale. Va notato che questo viene in genere fatto in casi d'uso mirati nel contesto di set di dati ben preparati e chiusi.

Inoltre, nei settori della criminalità che coinvolgono dispositivi digitali come gli smartphone, la quantità di dati da analizzare e su cui intervenire è enorme e complessa. In questi scenari, l'analisi dei dati basata sull'intelligenza artificiale diventa indispensabile per un'analisi efficace. Senza l'assistenza dell'intelligenza artificiale, le forze dell'ordine potrebbero trovarsi ad affrontare sfide significative nel decifrare vaste quantità di dati, con conseguenti potenziali...

Sviste, indagini prolungate e occasioni mancate di arrestare i criminali. Ad esempio, analizzare il volume di dati generato da un singolo smartphone è impossibile senza assistenza tecnica.

Nelle sezioni seguenti verranno approfonditi i concetti di set di dati ampi e complessi, OSINT/SOCMINT (Open Source Intelligence/Social Media Intelligence) e Natural Language Processing (NLP) e il modo in cui possono rimodellare le moderne pratiche di applicazione della legge.

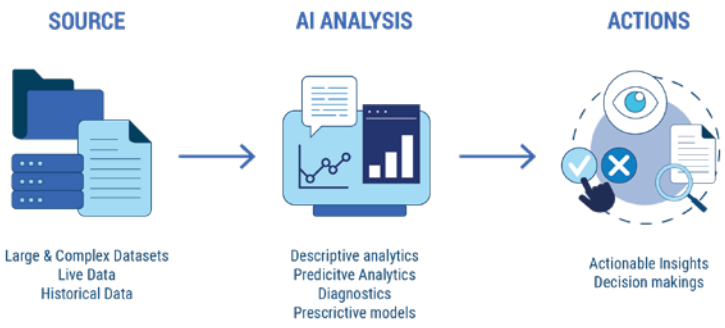
SET DI DATI GRANDI E COMPLESSI

Le forze dell'ordine si trovano sempre più spesso ad affrontare la sfida di navigare tra set di dati ampi e complessi, difficilmente gestibili ed elaborabili con i tradizionali strumenti di elaborazione dati. Gestire la complessità di tali set di dati richiede tecniche specifiche. Sistemi avanzati di gestione di database e soluzioni di ricerca scalabili, elaborazione parallela[5]e le infrastrutture di cloud computing sono spesso impiegate per archiviare, elaborare e accedere a enormi volumi di dati. Inoltre, i modelli di intelligenza artificiale, inclusi gli algoritmi di apprendimento automatico, svolgono un ruolo cruciale nell'analisi e nella comprensione di questi dati, soprattutto quando l'analisi umana sarebbe troppo lenta o inefficiente.

L'obiettivo finale dell'esplorazione di set di dati ampi e complessi è estrarre informazioni utili. Per le forze dell'ordine, questo potrebbe significare trascrivere migliaia di ore di file audio, estrarre entità come nomi e numeri di telefono da messaggi di testo senza necessariamente esaminarne il contenuto, limitando così potenziali violazioni della protezione dei dati e riducendo al minimo la quantità di dati personali trattati. Altre applicazioni rilevanti in ambito di polizia includono:

- individuare schemi nelle attività criminali;
- identificare correlazioni tra diversi tipi di dati (come modelli meteorologici o stagionali e tassi di criminalità, ad esempio il tasso di furti con scasso aumenta durante i mesi più caldi);
- prevedere le esigenze di risorse in base alle tendenze passate (ad esempio, un dipartimento di polizia sta cercando di determinare quanti agenti dovrebbe schierare nei diversi distretti durante i diversi momenti della giornata e della settimana).

Questo elenco non è esaustivo. Nuovi casi d'uso di analisi di set di dati ampi e complessi all'interno delle forze dell'ordine emergeranno man mano che



Set di dati grandi e complessi nelle operazioni:

Nel 2020, gli sforzi congiunti delle forze dell'ordine francesi e olandesi, supportati da Europol[6], ha portato allo smantellamento dello strumento di comunicazione crittografata EncroChat. Questa operazione non solo ha inferto un duro colpo alle reti criminali, ma ha anche dimostrato il ruolo cruciale dell'analisi di set di dati ampi e complessi nello smantellare l'intricata rete di attività criminali su scala globale.

EncroChat, concepita come una rete per garantire agli utenti un perfetto anonimato, discrezione e nessuna tracciabilità, ha rappresentato uno strumento chiave per i gruppi criminali organizzati (COG) in tutto il mondo. I telefoni abilitati per EncroChat, dal prezzo di circa 1.000 euro ciascuno, offrivano funzionalità come l'eliminazione automatica dei messaggi e la cancellazione remota dei dispositivi, rendendoli indispensabili per i criminali che cercavano comunicazioni sicure. Dopo lo smantellamento, gli investigatori sono riusciti a intercettare, condividere e analizzare oltre 115 milioni di conversazioni criminali, per un numero stimato di oltre 60.000 utenti. Gli hotspot degli utenti erano diffusi nei paesi di origine e di destinazione del traffico di droghe illecite, nonché nei centri di riciclaggio di denaro.[7].

Il successo di questa operazione sottolinea l'impatto trasformativo dell'analisi di set di dati ampi e complessi. L'enorme set di dati, composto da milioni di messaggi, è diventato una risorsa fondamentale per smantellare le reti criminali. Grazie ad analisi avanzate, le forze dell'ordine sono state in grado di identificare modelli, connessioni e punti critici, portando all'arresto di 6.558 sospettati, tra cui 197 obiettivi di alto valore. La portata di questo approccio basato sui dati è evidente nel sequestro di fondi criminali per un totale di 739,7 milioni di euro, nel congelamento di 154,1 milioni di euro di beni e nella confisca di ingenti quantità di droga, veicoli, armi e proprietà.

La rimozione di EncroChat funge da paradigma per l'integrazione efficace di analisi di dataset ampi e complessi nella lotta alla criminalità organizzata. L'impegno e la collaborazione di Europol con diverse parti interessate dimostrano la potenza degli sforzi collaborativi e dell'intelligence basata sui dati nel contrastare le attività criminali in tutto il mondo. Dimostra che ciò può essere fatto nel rispetto degli standard europei in materia di protezione dei dati e diritti umani, con la consulenza del Garante europeo della protezione dei dati (GEPD). Questa operazione testimonia l'evoluzione del panorama delle forze dell'ordine, in cui l'analisi avanzata svolge un ruolo fondamentale nello smantellamento delle reti criminali e nel rispetto dello stato di diritto.

Sfruttare al meglio le potenzialità delle soluzioni di intelligenza artificiale non si basa esclusivamente sulla tecnologia in sé. È fondamentale che i sistemi di intelligenza artificiale funzionino correttamente solo su un'infrastruttura tecnologica adeguata ed estesa. Ciò richiede budget significativi e competenze specifiche per la creazione e il funzionamento, il che può essere difficile da ottenere, soprattutto per le agenzie più piccole8.

Inoltre, è fondamentale considerare le implicazioni dell'ottenimento, dell'elaborazione e dell'analisi dei dati ed essere consapevoli di fare scelte legali ed etiche sensate in ogni fase del processo.[9]In pratica, l'UE ha adottato normative e linee guida rigorose per garantire la tutela del diritto alla privacy degli individui e il trattamento corretto e lecito dei dati per finalità specifiche, esplicite e legittime, come la Direttiva generale sulla protezione dei dati (GDPR) e la Direttiva sulle attività di contrasto (LED). Il rispetto di queste normative è fondamentale, sebbene a volte possa risultare restrittivo per l'analisi dei dati.

Infine, lo scambio di informazioni tra diverse agenzie e unità all'interno delle forze dell'ordine può essere una sfida[10]I sistemi di dati frammentati, i silos informativi e l'interoperabilità limitata tra i database possono ostacolare l'analisi completa di dati di grandi dimensioni e

set di dati complessi. La collaborazione e la condivisione dei dati tra le agenzie, così come lo sviluppo e l'adozione di standard comuni, sono fondamentali per sfruttare appieno il potenziale delle informazioni basate sui dati, ma raggiungere questo obiettivo nella pratica si rivela spesso difficile.

Per superare queste sfide, le forze dell'ordine potrebbero dover investire in formazione e infrastrutture per migliorare le proprie capacità di gestione dei dati. Devono inoltre costantemente districarsi nel complesso panorama di considerazioni legali ed etiche, garantendo che le loro pratiche di gestione dei dati rimangano responsabili ed efficaci.

Infine, promuovere una migliore comunicazione e collaborazione tra diverse agenzie e unità è fondamentale per sfruttare appieno il potenziale dell'analisi di set di dati ampi e complessi nelle forze dell'ordine, nel rispetto dei limiti della protezione dei dati e dell'etica.

POLIZIA PREDITTIVA

Nell'ambito delle forze dell'ordine, i processi decisionali si basano sempre più sull'intelligence derivata da set di dati ampi e complessi[11]Un recente progresso è la "polizia predittiva", che impiega sofisticati metodi statistici per estrarre nuove preziose informazioni da vasti set di dati, ad esempio su registri di reati, eventi e fattori ambientali identificati nelle analisi criminologiche. Questo approccio consente alle forze di polizia di identificare modelli correlati al verificarsi di reati e situazioni pericolose e di schierare le forze in base a tali informazioni per ridurre al minimo i rischi.

Polizia predittiva[12], sfrutta le capacità dell'intelligenza artificiale per migliorare l'efficacia e l'efficienza delle attività di polizia. Implementato principalmente attraverso modelli di apprendimento automatico basati su regole.[2], la polizia predittiva prevede due fasi fondamentali: (a) raccolta dati e (b) modellazione dei dati (previsione). Nella fase di raccolta dati, i dipartimenti di polizia accumulano dati strutturati e non strutturati da diverse fonti, tra cui dati storici sui reati (tempo, luogo e tipo), dati socio-economici e variabili di opportunità.[13]In alcuni casi, queste informazioni vengono integrate con dati provenienti da servizi di libertà vigilata e servizi sociali, tra le altre fonti pertinenti. Successivamente, algoritmi di apprendimento automatico vengono impiegati per analizzare questi dati nelle fasi di addestramento e previsione. Il modello di intelligenza artificiale identifica pattern all'interno dei dati storici, associando indicatori alla probabilità che si verifichi un reato, e quindi genera punteggi di rischio come output predittivi.

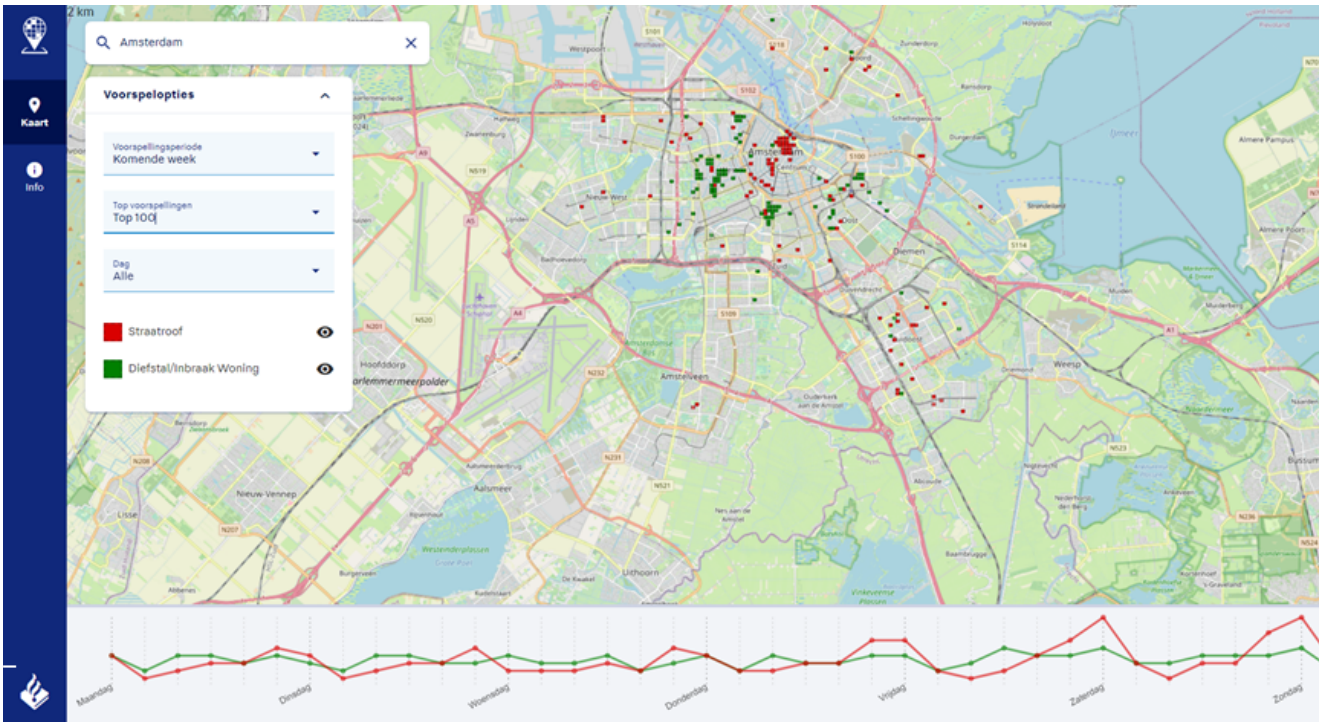
La polizia predittiva si manifesta in due tipi principali: (a) polizia basata sull'area e (b) polizia basata sull'individuo. Gli algoritmi basati sull'area identificano

2 Un sistema progettato per raggiungere l'Intelligenza Artificiale (IA) attraverso un modello basato esclusivamente su regole predeterminate. Due elementi importanti dei modelli di IA basati su regole sono "un insieme di regole" e "un insieme di fatti" e, utilizzando questi, gli sviluppatori possono creare un modello di Intelligenza Artificiale di base. Questi sistemi possono essere visti come una forma più avanzata di automazione robotica dei processi (RPA). I modelli di IA basati su regole sono deterministici per loro stessa natura, il che significa che operano secondo la semplice ma efficace metodologia "causa ed effetto". Questo modello può eseguire solo i compiti e le funzioni per cui è stato programmato e nient'altro. Per questo motivo, i modelli di IA basati su regole richiedono solo dati e informazioni di base per funzionare correttamente (Fonte: https://wearebrain.com/blog/rule-based-ai-vs-machine-learningwhats-the-difference/).

Connessioni tra luoghi, eventi e statistiche storiche sulla criminalità per prevedere la probabilità che si verifichino reati in momenti e luoghi specifici. Ad esempio, possono prevedere un aumento dei tassi di criminalità in determinate condizioni meteorologiche o durante importanti eventi sportivi. La polizia predittiva basata sugli individui prevede le persone più propense a commettere reati. Questo approccio ha guadagnato terreno in diversi Stati membri dell'UE, tra cui Paesi Bassi, Germania, Austria, Francia, Estonia e Romania, mentre altri ne stanno esplorando la potenziale implementazione.[14].

Applicazioni nel mondo reale:

La polizia olandese ha sviluppato e reso operativo il Sistema di Anticipazione dei Crimini (CAS)15 per affrontare una serie di reati che vanno oltre gli obiettivi iniziali, tra cui furti in abitazione, rapine, borseggi, furti d'auto, reati violenti, furti in attività commerciali e furti di biciclette. Il sistema effettua analisi settimanali utilizzando dati locali e recenti, integrandoli con informazioni esterne sui quartieri e sui loro abitanti. Il sistema è ulteriormente arricchito dalle informazioni fornite dalla polizia stessa sulle attività criminali, sulle condizioni locali e sui dati statistici dei Paesi Bassi. Il sistema mira a identificare modelli di criminalità, come una maggiore frequenza di furti di biciclette in una specifica area tra le 21:00 e mezzanotte. Grazie a queste informazioni, la polizia può allocare le proprie risorse in modo più efficiente e contrastare questi reati in modo più efficace, come riportato dalle notizie locali16.



Fonte dell'immagine: https://nl.wikipedia.org/wiki/Criminaliteits_Anticipatie_Systeem

Nonostante i potenziali benefici della polizia predittiva, a livello globale sono state sollevate preoccupazioni da parte di decisori politici e associazioni per i diritti umani in merito alla sua potenziale violazione dei diritti umani fondamentali. La legge UE sull'intelligenza artificiale cerca di affrontare queste preoccupazioni; le disposizioni pertinenti saranno discusse nel Capitolo 5.

In conclusione, la polizia predittiva rappresenta un approccio trasformativo all'applicazione della legge attraverso l'integrazione delle tecnologie di intelligenza artificiale. Con la sua continua evoluzione, i decisori politici devono trovare il delicato equilibrio tra lo sfruttamento dei potenziali benefici e la risposta alle problematiche etiche e legali associate a questo innovativo strumento di polizia.

OSINT E SOCMINT

Una sottocategoria di set di dati ampi e complessi proviene da fonti di Open-Source Intelligence (OSINT), soprattutto in un'epoca in cui l'impronta dei dati di Internet si sta espandendo rapidamente.

Dopo il 2020, il traffico online è aumentato in modo significativo. I lockdown imposti dalla pandemia globale hanno contribuito a un'impennata degli utenti Internet in tutto il mondo. Questa nuova definizione di "normalità" ha anche aperto la strada a un'impennata della criminalità informatica.[17]e ha portato a un aumento significativo della propaganda estremista violenta e dei contenuti terroristici online[18]Nella vasta distesa del mondo digitale, dove i criminali informatici agiscono rapidamente, i metodi OSINT tradizionali spesso faticano, confrontandosi con il dilemma di "dati schiaccianti, tempo limitato".[19]L'analisi di set di dati ampi, diversificati e non strutturati per estrarre informazioni preziose richiede risorse significative, come tempo, personale e denaro.

– risorse non sempre disponibili a molte forze dell'ordine.

La tendenza si sta spostando sostanzialmente verso l'automazione, ottimizzando l'uso delle risorse e migliorando la precisione nel processo decisionale. Nell'ambito dell'OSINT, l'automazione aiuta l'utente a scoprire e sfruttare fonti precedentemente non identificate. Di conseguenza, un numero crescente di agenzie di polizia a livello globale sta adottando strumenti OSINT automatizzati a fini investigativi. Dall'indagine e ricostruzione delle tracce criminali online all'analisi delle applicazioni web e al rilevamento delle minacce informatiche sulle piattaforme social, le applicazioni di un paradigma OSINT automatizzato sono infinite. Gli strumenti OSINT automatizzati forniscono informazioni che rafforzano le indagini in fase iniziale, aiutando gli investigatori a passare dalla semplice reazione alla prevenzione attiva.

Inoltre, come già discusso, rimane una sfida importante: la gestione dei dati non strutturati. Per far fronte a questa sfida, le forze dell'ordine possono utilizzare strumenti OSINT e Social Media Intelligence (SOCMINT) automatizzati, basati sull'intelligenza artificiale e multi-sorgente, in grado di gestire sia i dati strutturati che quelli non strutturati. Grazie a modelli di apprendimento automatico autoapprendenti, questi strumenti possono riformattare i dati non strutturati, supportare ricerche e indagini open source mirate e offrire informazioni in tempo reale. Fondamentalmente, tutto ciò deve essere fatto a una velocità superiore a quella con cui i criminali possono cancellare le loro tracce digitali.

Inoltre, i fornitori di servizi online (OSP) e le unità di riferimento Internet (IRU) possono sfruttare la potenza dell'intelligenza artificiale per rilevare e contrastare la propaganda terroristica, la disinformazione, l'incitamento all'odio e i contenuti online illeciti.[20] Utilizzando algoritmi avanzati di intelligenza artificiale e apprendimento automatico, possono analizzare grandi quantità di dati ad alta velocità per identificare modelli, parole chiave o contenuti visivi associati a comportamenti estremisti.

ideologie. Inoltre, i sistemi basati sull'intelligenza artificiale possono essere addestrati su materiali di propaganda noti per individuare proattivamente nuovi contenuti che condividono caratteristiche simili e segnalarli alle forze dell'ordine, garantendo una rimozione più reattiva ed efficiente dei contenuti dannosi prima che si diffondano. È opportuno notare che, ai sensi del nuovo Digital Services Act (DSA), gli OPS non solo sono incoraggiati, ma sono tenuti a migliorare le proprie capacità di monitoraggio per garantire ambienti digitali più sicuri.[21]Il DSA impone un livello più elevato di responsabilità e trasparenza alle piattaforme, spingendo gli OSP a divulgare le loro pratiche e i risultati della moderazione dei contenuti.[22].

Tuttavia, l'uso dell'IA per la moderazione dei contenuti presenta una sfida complessa, in particolare per quanto riguarda l'equilibrio tra il diritto alla libertà di espressione e alla libertà di pensiero, coscienza e religione (articolati negli articoli 10 e 11 della Carta dei diritti fondamentali dell'Unione europea) e l'imperativo di contrastare la disinformazione, l'incitamento all'odio e i contenuti illeciti online. Questo equilibrio è delicato, poiché l'impiego dell'IA potrebbe inavvertitamente limitare le espressioni legittime sotto le mentite spoglie della moderazione dei contenuti, rappresentando una minaccia per queste libertà fondamentali.

ELABORAZIONE DEL LINGUAGGIO NATURALE (PNL)

L'elaborazione del linguaggio naturale, comunemente abbreviata in NLP, è una branca dell'informatica e della linguistica che si concentra sull'interazione tra computer e linguaggio umano[23]L'obiettivo è consentire alle macchine di interpretare e generare il linguaggio umano in modo significativo e utile. La ricerca indica che i metodi di PNL sono impiegati dalle forze dell'ordine e dai dipartimenti di polizia in varie attività, tra cui compiti amministrativi, indagini forensi, analisi di dati sui reati, conversione del parlato in testo per la segnalazione e documentazione di attività criminali.[24]L'enorme quantità di dati testuali, che spaziano dalle trascrizioni delle interviste alle dichiarazioni dei testimoni, dalle comunicazioni online ai post sui social media, estratti nell'ambito delle indagini penali, può essere analizzata in modo rapido ed efficiente utilizzando l'elaborazione del linguaggio naturale (NLP). Questa efficienza è particolarmente cruciale quando sono necessarie informazioni rapide in situazioni in tempo reale, come rapimenti o prese di ostaggi, durante o dopo attacchi terroristici e nelle indagini su casi di abuso e sfruttamento minorile. I principali compiti svolti dall'elaborazione del linguaggio naturale nelle attività di polizia includono:

- Classificazione del testo[25]: Un analista che elabora dati testuali spesso contrassegna i reati con parole chiave per comprendere meglio le circostanze che li hanno generati, ad esempio se l'autore fosse sotto l'effetto di alcol o droghe. Poiché la criminalità è in continua evoluzione, queste etichette potrebbero non essere complete. Un esempio di classificazione testuale è l'assegnazione di etichette diverse ai sottogruppi di riciclaggio di denaro.
- Raggruppamento[26]: A differenza dell'analisi del testo che si basa su caratteristiche predefinite, il clustering può aiutare a raggruppare crimini simili. Il clustering mappa i testi in uno spazio ad alta dimensionalità in modo che

Testi simili sono vicini tra loro. In questo compito, non sono necessarie etichette. Inoltre, il clustering può anche considerare fattori come il tempo e il luogo, per fornire una visione olistica delle tendenze criminali. Ad esempio, in scenari di furto con scasso, il clustering potrebbe rivelare metodi emergenti, come agganciare le chiavi attraverso le cassette delle lettere o sfruttare particolari punti deboli delle serrature.

- Riassunto del testo:La sintesi testuale è un metodo utilizzato per produrre un riassunto conciso e accurato di testi lunghi, preservandone il significato complessivo. Nell'ambito della PNL, si distinguono due approcci principali.[27]Vengono impiegate le seguenti tecnologie: (a) basate sull'estrazione e (b) basate sull'astrazione. La sintesi basata sull'estrazione comporta l'estrazione di un sottoinsieme di parole o frasi che racchiudono i punti chiave del testo, con il rischio di inesattezze grammaticali. D'altra parte, la sintesi basata sull'astrazione utilizza tecniche avanzate di deep learning per parafrasare e condensare il documento originale, in modo simile alla sintesi umana. Generando nuove frasi e frasi che racchiudono informazioni essenziali dal testo di partenza, gli algoritmi di apprendimento automatico astrattivo si dimostrano un prezioso aiuto nell'affrontare le limitazioni grammaticali associate alle tecniche basate sull'estrazione. Questa tecnologia è fondamentale per assistere le forze dell'ordine nel loro lavoro di analisi di ampi rapporti di polizia e altre informazioni. Questa tecnologia può fornire alle forze dell'ordine riassunti concisi che catturano dettagli cruciali senza sacrificare l'accuratezza.

- Traduzione automatica:I sistemi di traduzione automatica facilitano la conversione di testo da una lingua all'altra. Questi modelli prendono in input il testo in una lingua di partenza designata e producono il testo corrispondente in una lingua di destinazione specificata come output. Google Translate si distingue come un esempio ben noto di tale applicazione diffusa. I sistemi di traduzione automatica svolgono un ruolo fondamentale nelle forze dell'ordine consentendo un'analisi efficiente dei dati di comunicazione multilingue. Questi sistemi accelerano l'elaborazione di grandi volumi di informazioni, aiutando gli investigatori a scoprire potenziali minacce e a identificare attività criminali al di là delle barriere linguistiche. La tecnologia migliora la collaborazione globale tra le forze dell'ordine, consentendo una comunicazione più fluida e una condivisione di informazioni durante le indagini internazionali. Inoltre, la traduzione automatica contribuisce alla raccolta di prove traducendo accuratamente diverse forme di prove, riducendo così i pregiudizi linguistici.

> L'applicazione di rete per lo scambio sicuro di informazioni (SIENA) di Europol, lo strumento di comunicazione all'avanguardia che collega le forze dell'ordine di 51 paesi e 14 organizzazioni internazionali, consente già agli utenti finali di tradurre testi dalla propria lingua madre all'inglese in tempo reale. Lo strumento di traduzione automatica fornisce traduzioni rapide, accurate e contestuali, abbattendo le barriere linguistiche e migliorando la comunicazione all'interno di questa rete di forze dell'ordine in rapida evoluzione.

Le applicazioni pratiche dell'NLP nelle attività di polizia sono molteplici e in continua evoluzione. Nelle unità di criminalità informatica, l'NLP aiuta ad analizzare

comunicazione criminale, decifrazione di significati nascosti o segnalazione di contenuti online potenzialmente dannosi. Ad esempio, le principali preoccupazioni nella lotta alla criminalità informatica includono l'individuazione di comunicazioni predatorie, l'identificazione dei criminali informatici e la prevenzione degli abusi sui minori e dell'adescamento online. La PNL può rappresentare un punto di svolta per le attività di polizia in questo ambito.[28]Un sotto-compito dell'NLP, il Named Entity Recognition (NER), aiuta gli analisti a etichettare le entità nei rapporti di reato, in base alla loro tipologia, come persone, organizzazioni e veicoli. Ciò consente un raggruppamento e un'analisi più accurati dei reati. Nel contesto dei furti con scasso, ad esempio, il NER potrebbe distinguere tra diversi metodi di accesso, come la rottura di una finestra rispetto alla manomissione di uno specifico tipo di serratura. Inoltre, esaminando enormi database di testo non strutturato, gli strumenti di NLP possono estrarre informazioni cruciali (estrazione di entità), consentendo alla polizia di intervenire in situazioni critiche come minacce alla vita, in modo tempestivo ed efficiente.

In sostanza, la PNL funge da ponte tra le comunicazioni umane, fortemente dipendenti dal contesto, e le prestazioni dell'analisi computazionale, dotando le forze dell'ordine di un potente strumento nel loro arsenale digitale.

Informatica forense

L'informatica forense si è affermata come disciplina fondamentale nell'ambito delle forze dell'ordine, in un mondo sempre più digitalizzato. Con enormi quantità di informazioni archiviate, comunicate ed elaborate digitalmente, la capacità di indagare con precisione l'impronta digitale dei criminali è fondamentale per la polizia. Fondamentale per i progressi nell'informatica forense è il ruolo dell'intelligenza artificiale nelle moderne indagini digitali. L'intelligenza artificiale offre una capacità avanzata di setacciare vasti archivi di dati, automatizzando processi che tradizionalmente richiederebbero molto tempo agli esperti umani.[29]Ad esempio, mentre un investigatore umano potrebbe ordinare manualmente migliaia di file, l'intelligenza artificiale può rapidamente categorizzare, filtrare ed evidenziare informazioni rilevanti in base a criteri o modelli predefiniti (ad esempio classificazione delle immagini o hash[3]valori).

Sono stati sviluppati diversi strumenti e tecniche per il recupero e l'analisi dei dati basati su componenti di intelligenza artificiale. Questi strumenti possono recuperare file cancellati, accedere ai dati da dispositivi danneggiati e ripristinare informazioni frammentate in formati coerenti. La loro efficienza risiede nella capacità di adattarsi e apprendere da ogni caso, migliorando l'accuratezza nel tempo.

Una preoccupazione significativa nello spazio digitale è il rilevamento dei reati informatici. Le attività dannose, dall'hacking ai tentativi di phishing, spesso lasciano tracce sottili o sono mascherate nel normale traffico web. L'intelligenza artificiale eccelle nell'identificare modelli e anomalie all'interno di questi dati.[30].

3 I valori hash sono simili alle impronte digitali dei file. Eseguendo il contenuto di un file attraverso un algoritmo crittografico, viene generato un identificatore numerico distinto, il valore hash, che rappresenta il contenuto del file. Qualsiasi modifica al contenuto modificherebbe drasticamente questo valore hash. Attualmente, gli algoritmi MD5 e SHA-256 sono i metodi predominanti per generare questi valori hash.

Grazie all'apprendimento continuo da nuovi dati, i modelli di intelligenza artificiale sono in grado di distinguere il normale traffico di rete dalle potenziali minacce, anche se le attività dannose si evolvono o utilizzano nuove tattiche.

La decifratura dei dati è un altro ambito in cui l'intelligenza artificiale si è dimostrata promettente. Le tecniche di crittografia avanzate possono rappresentare seri ostacoli per gli investigatori. Mentre la decifratura tradizionale potrebbe comportare tentativi di forza bruta,[4] o cercando chiavi di crittografia, l'intelligenza artificiale può prevedere potenziali modelli di crittografia o accelerare il processo di decrittazione restringendo le possibili chiavi di crittografia in base al riconoscimento dei modelli.

Infine, analizzare le impronte digitali su dispositivi e piattaforme è diventato fondamentale, soprattutto con la proliferazione di dispositivi interconnessi nell'Internet delle cose (IoT). Un singolo individuo potrebbe interagire quotidianamente con più dispositivi, dagli smartphone e laptop ai dispositivi per la smart home. L'intelligenza artificiale può tracciare queste interazioni, creando un profilo digitale completo che aiuta gli investigatori a comprendere le connessioni di un soggetto o persino a proporre elementi aggiuntivi per ulteriori analisi.

L'informatica forense, potenziata dalle capacità di intelligenza artificiale, ha trasformato il panorama investigativo, offrendo una profondità e una velocità senza precedenti nell'analisi dei dati digitali. Questo non solo amplifica l'efficacia delle indagini, ma consente anche alle forze dell'ordine di affrontare proattivamente le minacce digitali in continua evoluzione.

Visione artificiale e biometria

In questo panorama in rapida evoluzione, la visione artificiale e la biometria sono emerse come elementi rivoluzionari per le forze dell'ordine, sia dal punto di vista della prevenzione che delle indagini. Poiché città e comunità si trovano ad affrontare un'ondata di immagini digitali provenienti da fonti come le telecamere a circuito chiuso e i dispositivi personali, è essenziale utilizzare questa vasta quantità di dati visivi.[31] In modo efficace. Abbinate a tecniche biometriche che sfruttano le caratteristiche fisiologiche uniche degli individui, queste tecnologie promettono una nuova frontiera nelle attività di polizia. La fusione di biometria e intelligenza artificiale può offrire un mix di efficienza e accuratezza, offrendo informazioni approfondite per identificare rapidamente ed efficacemente i criminali, proteggendo al contempo la privacy degli individui non rilevanti. Mentre le forze dell'ordine affrontano le sfide e le opportunità dell'era digitale, la visione artificiale e la biometria si distinguono come alleati inestimabili.

MONITORAGGIO E ANALISI VIDEO

4 Un attacco brute force impiega un metodo di tentativi ed errori per decifrare le credenziali di accesso, chiavi di crittografia o individuare pagine web nascoste. Gli aggressori provano sistematicamente ogni possibile combinazione nella speranza di indovinare. Tali attacchi vengono eseguiti utilizzando la "forza bruta", che comporta continui e violenti tentativi di accedere ad account privati.

Il progresso della tecnologia di imaging, unito all'intelligenza artificiale e agli sviluppi del machine learning, ha trasformato il mondo delle forze dell'ordine. Alcune delle potenziali applicazioni per le forze dell'ordine includono:

- Elaborazione in tempo reale e rilevamento delle anomalie:Il monitoraggio video si è evoluto oltre l'osservazione passiva. Grazie all'integrazione di algoritmi basati sull'intelligenza artificiale, i feed video possono essere elaborati in tempo reale, rilevando pattern o anomalie predefiniti. Questa capacità è particolarmente utile nelle zone sensibili per la sicurezza. Il sistema può avvisare tempestivamente il personale di sicurezza di attività sospette, come veicoli in prossimità di luoghi sensibili, oggetti incustoditi come un bagaglio dimenticato in un nodo di transito o accessi non autorizzati. Inoltre, questa elaborazione in tempo reale può essere fondamentale nella gestione del traffico, rilevando immediatamente incidenti o interruzioni e facilitando risposte immediate e informate.

- Sicurezza pubblica e gestione degli eventi:Per eventi come celebrazioni pubbliche, concerti o festival, la sicurezza e il benessere dei partecipanti sono fondamentali. La salvaguardia di questi eventi è fondamentalmente diversa dalle normali attività di controllo. Invece di semplici panoramiche visive tradizionali, l'analisi video potenziata dall'intelligenza artificiale può fornire informazioni dettagliate sul flusso generale dei partecipanti. Ciò consente di individuare tempestivamente potenziali aree di congestione e di pianificare in modo proattivo. Inoltre, il sistema è in grado di identificare situazioni che potrebbero richiedere attenzione, garantendo che tutti possano godersi l'evento in tutta tranquillità.

- Segnalazione automatica degli incidenti[32]:Una delle caratteristiche distintive dell'integrazione dell'IA nell'analisi video è la sua capacità di segnalare autonomamente gli incidenti. Se vengono rilevate condizioni o scenari predefiniti, come disordini pubblici o potenziali rischi per la sicurezza, il sistema di IA può generare automaticamente report dettagliati sugli incidenti e/o inviare avvisi agli agenti per valutare la situazione. Questo non solo velocizza il processo di documentazione, ma garantisce anche che anche gli incidenti minori, che potrebbero essere trascurati nel monitoraggio manuale, vengano registrati e gestiti accuratamente.

In sostanza, il monitoraggio e l'analisi video moderni amplificano le capacità delle forze dell'ordine. Gli agenti di polizia non si limitano a osservare, ma comprendono e interpretano attivamente le enormi quantità di dati visivi a loro disposizione. Dal miglioramento della gestione del traffico in tempo reale alla garanzia della sicurezza pubblica in occasione di eventi su larga scala, l'analisi video basata sull'intelligenza artificiale rappresenta un balzo in avanti radicale nelle capacità delle forze dell'ordine, offrendo una velocità e un'accuratezza senza precedenti nel rilevamento e nella risposta agli incidenti, promuovendo così un ambiente più sicuro per tutti.

CLASSIFICAZIONE DELLE IMMAGINI

Nell'ambito della visione artificiale, la classificazione delle immagini sta emergendo sempre più come un campo critico. In sostanza, gli strumenti di intelligenza artificiale addestrati a categorizzare le immagini in base al contenuto o agli oggetti dominanti che rilevano, aiutano le forze dell'ordine, sommerse da immagini, a rispondere in modo rapido ed efficace.

Analizzare questi dati. La classificazione delle immagini aiuta a ordinare rapidamente tali dati, categorizzando le immagini in gruppi come "sospette" o "non sospette" o persino organizzandole in base a temi, eventi o intervalli di tempo diversi. Questo approccio semplificato velocizza notevolmente i processi investigativi.

L'evoluzione dei moderni strumenti di classificazione delle immagini, in particolare quelli basati su algoritmi di apprendimento automatico, ha consentito l'elaborazione rapida di enormi volumi di dati. Tali strumenti non solo separano le immagini con un intervento manuale minimo, ma garantiscono anche che nessuna prova visiva essenziale passi inosservata. Inoltre, la precisione intrinseca di questi sistemi garantisce una categorizzazione accurata, con conseguenti risultati investigativi più efficaci. Oltre alle applicazioni tradizionali, la classificazione delle immagini è rilevante in diversi ambiti delle forze dell'ordine. Ad esempio, durante eventi pubblici o luoghi affollati, la classificazione delle immagini può identificare potenziali minacce o interruzioni, aiutando le forze dell'ordine ad adottare misure preventive.

Uno scenario degno di nota che evidenzia il potenziale della classificazione delle immagini è la sua applicazione nelle indagini forensi, ovvero l'analisi dei dati estratti dai dispositivi di comunicazione mobile. Spesso, questi dispositivi memorizzano migliaia di immagini, il che rende la loro consultazione complessa e dispendiosa in termini di tempo. Inoltre, questa situazione solleva notevoli preoccupazioni in merito alla protezione dei dati durante l'elaborazione di immagini personali. Grazie alla classificazione delle immagini basata sull'intelligenza artificiale, le immagini estratte in ambito forense dai dispositivi mobili possono essere rapidamente ordinate, riducendo al minimo la necessità di revisione manuale e la quantità di dati personali elaborati.
Concentrandosi solo sulle immagini rilevanti, gli investigatori possono non solo risparmiare tempo prezioso, ma anche svelare informazioni cruciali che altrimenti sarebbero state trascurate nell'enorme volume di dati, nel rispetto dei principi di minimizzazione dei dati, privacy-by-design e sicurezza-by-design. In sostanza, la classificazione delle immagini sta plasmando il futuro delle indagini digitali nelle forze dell'ordine, offrendo un mix di velocità, precisione ed efficienza.

BIOMETRIA

In un'epoca in cui l'identificazione e la verifica personale sono di fondamentale importanza, le tecnologie biometriche si sono affermate come strumenti chiave nel kit di strumenti delle forze dell'ordine. Le tecnologie biometriche consentono l'identificazione degli individui, utilizzando i loro attributi fisiologici unici (ad esempio tratti del viso, impronte digitali, pattern dell'iride) o comportamentali (ad esempio andatura).[5], scrittura a mano).

Riconoscimento facciale:La tecnica di utilizzo delle immagini facciali per l'identificazione dei criminali è antica quanto le moderne attività di polizia. Fino ai primi anni '60, la procedura era principalmente manuale e si basava sulla percezione individuale e sulla capacità umana di riconoscere i volti familiari. Tuttavia, i progressi nella tecnologia di imaging e nell'informatica[33]

5 L'andatura si riferisce al modo o allo schema di movimento degli arti durante la locomozione su un substrato solido. In sostanza, è il modo in cui un individuo cammina o si muove. L'analisi dell'andatura è spesso utilizzata in ambito medico, sportivo e riabilitativo per comprendere e affrontare diverse problematiche legate al movimento.

consentito il riconoscimento facciale automatico (AFR)[34]; gli algoritmi informatici ora assistono la polizia e le immagini digitali acquisite tramite vari mezzi hanno da tempo sostituito le fotografie stampate.

Questa tecnologia utilizza algoritmi per estrarre e analizzare determinati tratti del viso da immagini o video per abbinarli e verificarne l'identità. È diventata uno strumento prezioso per le forze dell'ordine. Ad esempio, la tecnologia aiuta a identificare rapidamente i sospettati confrontando i dati facciali raccolti nel corso di un'indagine penale con i dati storici o i database dei criminali a disposizione della polizia. Inoltre, svolge un ruolo cruciale nella localizzazione di persone scomparse e bambini, abbinando le immagini di individui non identificati ai database di persone segnalate come scomparse. Inoltre, al di fuori del contesto delle forze dell'ordine, il riconoscimento facciale offre una maggiore sicurezza in ambienti controllati, eliminando la necessità di metodi di autenticazione tradizionali come il controllo degli accessi fisici.

Tuttavia, l'ascesa del riconoscimento facciale è stata accompagnata anche da preoccupazioni. In particolare, i pregiudizi rimangono un argomento di dibattito. Alcuni studi hanno evidenziato discrepanze nell'efficienza del sistema, in particolare nell'identificazione di individui di specifiche origini etniche, generi o fasce d'età.[35]La privacy e la protezione dei dati rappresentano un'altra preoccupazione significativa. Con la crescente diffusione dei sistemi di riconoscimento facciale, soprattutto nei domini pubblici, si innescano dibattiti sui limiti etici della sorveglianza e sul potenziale uso improprio. Inoltre, i repository di dati che alimentano il riconoscimento facciale – vasti database di dati facciali – possono rappresentare obiettivi interessanti per gli attacchi informatici, il che sottolinea l'importanza di solide misure di protezione dei dati.

In questo contesto, è fondamentale distinguere tra sistemi utilizzati in tempo reale negli spazi pubblici (Live Face Recognition, LFR) e sistemi utilizzati retrospettivamente (riconoscimento facciale post-evento). Quando utilizzato retrospettivamente, l'AFR aiuta gli investigatori a confrontare immagini di persone sconosciute, come una persona ripresa da una telecamera di sorveglianza, sospettata di aver commesso un reato o la foto segnaletica di un arrestato, con un database di riferimento. Questo database di riferimento è in genere supervisionato e conservato legalmente, come le immagini di custodia cautelare o le immagini raccolte durante un procedimento penale.

Anziché concentrarsi su un singolo individuo in immagini preregistrate, LFR esegue una lettura in tempo reale di tutte le persone che passano davanti a una telecamera, indipendentemente dalla loro capacità, e le confronta con una lista di controllo chiusa predeterminata di persone di interesse. In alcuni scenari, il sistema scarterà immediatamente le immagini che non hanno generato risultati per evitare indebite violazioni delle leggi applicabili in materia di protezione dei dati. Le applicazioni LFR pongono sfide significative sia dal punto di vista tecnico che umano (carico del sistema, capacità umana e distorsioni, ecc.). Le forze di polizia nel Regno Unito e in alcuni paesi dell'UE hanno sperimentato applicazioni LFR con vari gradi di successo.

RICONOSCIMENTO FACCIALE NELLE ATTIVITÀ DI POLIZIA: CASI D'USO NEL MONDO REALE

1. Identificazione di una persona sconosciuta

- Le tecnologie di identificazione biometrica, in particolare il riconoscimento facciale, svolgono un ruolo cruciale nelle forze dell'ordine per l'identificazione rapida ed efficiente di sconosciuti. Due scenari principali in questo contesto:

- Risoluzione di casi irrisolti: nelle indagini su un caso di omicidio, le riprese di una telecamera di sorveglianza identificano un sospettato, portando a una ricerca dell'immagine facciale in un database di individui noti e sconosciuti. I risultati iniziali sono negativi, ma l'immagine viene archiviata. Due anni dopo, una query biometrica attiva una corrispondenza durante un'altra indagine per omicidio, collegando infine il sospettato al caso precedente. Ciò dimostra l'efficacia della biometria nella risoluzione di casi irrisolti nel tempo.

- Svelare le reti di sfruttamento minorile: in un altro scenario, la polizia confisca il computer di un molestatore sessuale su minori, avviando un'analisi biometrica delle immagini estratte. Le corrispondenze con le vittime di precedenti indagini aiutano a svelare una rete più ampia di criminali coinvolti nello sfruttamento minorile. Ciò sottolinea il ruolo significativo della biometria nella lotta contro crimini efferati e nella protezione delle popolazioni vulnerabili come i bambini scomparsi.

2. Ricerche mirate di una persona conosciuta

- Le forze dell'ordine si affidano in larga misura a ricerche mirate di persone note per convalidare l'identità e valutare un potenziale coinvolgimento criminale6. Diversi scenari evidenziano l'importanza delle tecnologie biometriche in questo ambito:

- Smascherare i legami con il terrorismo: un cittadino fornisce informazioni anonime che collegano un determinato individuo a crimini gravi e terrorismo. Le ricerche tradizionali con dati biografici non producono risultati, richiedendo una ricerca tramite immagine facciale. Questo rivela una potenziale corrispondenza con un terrorista ricercato, dimostrando come la biometria possa migliorare le piste e contribuire alle attività antiterrorismo.

- Svelare le reti criminali attraverso l'analisi dei dati mobili: gli esperti forensi analizzano lo smartphone di un sospettato, utilizzando il riconoscimento facciale per raggruppare i media e restringere il campo di ricerca. Successive ricerche nei database biometrici di persone note o sconosciute rivelano potenziali contatti, portando allo smascheramento di una rete criminale più ampia. Questo caso dimostra la sinergia tra tecnologia e analisi umana.

- Contrasto alle reti di frode finanziaria: nei casi di frode agli sportelli bancomat, le forze dell'ordine utilizzano il riconoscimento facciale per collegare un autore noto a una raccolta di immagini di truffatori sconosciuti. Questa ricerca mirata aiuta a valutare il coinvolgimento del noto truffatore.

autore di ulteriori attività criminali.

Impronte digitali:L'impronta digitale è una delle tecniche biometriche più antiche e affidabili utilizzate dalle forze dell'ordine. Il pattern delle impronte digitali di ogni individuo, costituito da creste, anse e spirali, è unico.

6 È essenziale chiarire le circostanze in cui sono consentite le ricerche biometriche, Soprattutto quando l'identità di una persona è dubbia o autodichiarata. È opportuno valutare i casi in cui incongruenze nell'identificazione, come identità autodichiarate o false, potrebbero richiedere verifiche biometriche per garantire un'identificazione accurata e prevenire potenziali minacce.

e rimane invariato per tutta la vita, rendendolo un mezzo di identificazione affidabile. L'analisi tradizionale delle impronte digitali si basava in gran parte su esperti qualificati che confrontavano manualmente le impronte, il che era dispendioso in termini di tempo e talvolta soggettivo.[36].

Impronte digitali e intelligenza artificiale[37][38]:

L'integrazione dell'intelligenza artificiale nelle impronte digitali potrebbe rivoluzionare questo settore:

- Corrispondenza automatica:I sistemi basati sull'intelligenza artificiale possono analizzare vasti database di impronte digitali in pochi secondi, fornendo corrispondenze con un elevato grado di accuratezza. Questo velocizza notevolmente il processo di identificazione ed è particolarmente utile in scenari in cui la rapidità dei risultati è fondamentale.
- Riconoscimento dei dettagli migliorato:Gli algoritmi di intelligenza artificiale sono in grado di identificare ed evidenziare minuzie (punti specifici su un'impronta digitale, come biforcazioni o terminazioni di creste) con maggiore precisione rispetto all'occhio umano, consentendo confronti più dettagliati e accurati.
- Analisi delle impronte latenti:L'intelligenza artificiale è particolarmente utile quando si tratta di impronte latenti, ovvero impronte digitali lasciate involontariamente sulle superfici. Queste impronte potrebbero essere parziali, macchiate o di bassa qualità. Algoritmi avanzati possono migliorare tali impronte, riempire spazi vuoti o persino prevedere porzioni mancanti in base a pattern riconosciuti, consentendo corrispondenze migliori anche con campioni altrimenti complessi.
- Apprendimento e adattamento:Uno dei punti di forza dei sistemi di intelligenza artificiale è la loro capacità di apprendimento. Man mano che elaborano più dati, questi sistemi perfezionano i loro algoritmi, diventando sempre più abili nel riconoscere schemi o anomalie. Questo apprendimento continuo garantisce che l'analisi delle impronte digitali rimanga all'avanguardia e si adatti a nuove sfide o tecniche.
- Integrazione/interoperabilità con altri sistemi:I sistemi di impronte digitali basati sull'intelligenza artificiale possono essere facilmente integrati con altri database digitali o sistemi biometrici, come i sistemi UE su larga scala a disposizione degli operatori della sicurezza interna (SIS, VIS, Eurodac ecc.). Ciò consente controlli biometrici multimodali e verifiche complete dei precedenti.
- Incorporare l'intelligenza artificiale nell'analisi delle impronte digitaliNon solo aumenta l'accuratezza e la velocità del processo, ma garantisce anche coerenza e obiettività, riducendo al minimo errori umani o distorsioni. Amplifica i punti di forza dell'impronta digitale tradizionale, mitigandone al contempo i limiti, rendendolo uno strumento indispensabile nei moderni contesti forensi e di polizia.

Riconoscimento vocale:Ogni individuo ha un modello vocale distinto, modellato dall'anatomia del suo tratto vocale e dal suo modo unico

del parlato. La tecnologia di riconoscimento vocale decifra queste minime differenze, convertendo le parole pronunciate in modelli digitali che possono essere confrontati con le impronte vocali memorizzate. In ambito di applicazione della legge, questa tecnologia può essere utilizzata per confrontare campioni vocali provenienti da telefonate o registrazioni, e confermare l'identità nei sistemi di sicurezza.

Scansioni dell'iride:Gli intricati motivi dell'iride, la parte colorata dell'occhio, sono unici come le impronte digitali. Catturati attraverso una semplice fotografia, questi motivi offrono un mezzo di identificazione rapido e non invasivo. Sebbene le tecnologie di identificazione dell'iride siano state inizialmente adottate per applicazioni militari, come la registrazione biometrica di popolazioni vulnerabili sui campi di battaglia,[39], i tassi di adozione da parte delle forze dell'ordine aumentano gradualmente[40].

Analisi dell'andatura:L'analisi dell'andatura è un campo emergente che studia il modo in cui un individuo cammina. Anche le più piccole differenze di postura, andatura e andatura possono essere rilevate e analizzate, offrendo un metodo non invasivo per identificare gli individui, particolarmente utile in situazioni in cui il riconoscimento facciale o di altro tipo non è fattibile.

Per distinguere tra applicazioni di identificazione biometrica retrospettiva e in tempo reale, è necessario riconoscere il ruolo di quest'ultima negli scenari di risposta rapida, in particolare la sua utilità nella prevenzione di attacchi terroristici, nella localizzazione di bambini scomparsi e nell'arresto o nella lotta contro crimini gravi. Tuttavia, è necessario anche riconoscere le sfide e le considerazioni etiche legate alla biometria in tempo reale, che evidenziano l'imperativa necessità di un'implementazione responsabile e di una panoramica normativa per garantire la privacy e prevenirne l'uso improprio.

La biometria, con le sue molteplici modalità, è la testimonianza dell'innovativa fusione tra biologia e tecnologia. Nelle forze dell'ordine, non solo promette un'identificazione accurata, ma può anche aprire la strada a servizi più efficienti che rispettino la dignità dei cittadini e ne salvaguardino la sicurezza.

CATEGORIZZAZIONE BIOMETRICA

Un'ulteriore applicazione dell'IA che presenta un potenziale per le forze dell'ordine è rappresentata dai sistemi che facilitano la categorizzazione degli individui in base alle loro caratteristiche biometriche, che stanno acquisendo sempre maggiore importanza. Questi sistemi, la cui applicazione è fondamentalmente diversa dai sistemi utilizzati per l'identificazione, rappresentano strumenti preziosi sia per la prevenzione che per le indagini.

L'obiettivo principale dell'impiego di questi sistemi di categorizzazione nelle forze dell'ordine è proteggere le fasce vulnerabili della popolazione. Ad esempio, la categorizzazione biometrica aiuta a rilevare e oscurare i dati sensibili dalle immagini, soprattutto quando riguardano minori o vittime di reati gravi come abusi sui minori o tratta di esseri umani. Tali tecnologie garantiscono la tutela della privacy e della dignità delle vittime durante le indagini.

È importante comprendere i limiti della categorizzazione biometrica. La polizia non sfrutta questi sistemi per dedurre o dedurre categorie speciali di dati personali come quelli sessuali o

orientamenti politici, convinzioni religiose, disabilità o affiliazioni sindacali. L'attenzione si concentra principalmente sulla stima di età e genere. Tuttavia, tali stime, soprattutto se integrate in sistemi ad alto rischio, richiedono una solida supervisione normativa, che garantisca che il potenziale della tecnologia sia sfruttato in modo responsabile ed etico, soprattutto tenendo conto delle problematiche relative alla protezione dei dati.

Ad esempio, la sfida di gestire enormi quantità di contenuti video, alcuni dei quali potenzialmente contenenti immagini inquietanti di abusi sui minori, sottolinea l'urgente necessità di sistemi di stima dell'età accurati. Senza strumenti di intelligenza artificiale in grado di identificare i minori nei video con maggiore accuratezza rispetto agli analisti umani, il compito di revisione manuale diventa quasi impraticabile a causa delle ingenti risorse necessarie. In questo contesto, gli strumenti di categorizzazione biometrica, in grado di categorizzare rapidamente e accuratamente gli individui in base a caratteristiche oggettive come l'età, si rivelano risorse inestimabili.

Oltre alla loro utilità, è fondamentale considerare gli aspetti relativi alla protezione dei dati. Garantire la privacy e la sicurezza delle persone, in particolare dei minori, durante il trattamento di dati così sensibili diventa fondamentale. Bilanciare l'urgenza di un'accurata moderazione dei contenuti con solide misure di protezione dei dati rimane essenziale per rispettare gli standard etici e proteggere i diritti e la privacy delle persone coinvolte.

Miglioramento dell'allocazione delle risorse e della pianificazione strategica

Il panorama sempre più complesso delle forze dell'ordine richiede un approccio strategico all'allocazione delle risorse. Con l'evolversi delle minacce e l'espansione delle città, garantire un utilizzo ottimale delle risorse, siano esse personale, attrezzature o tempo, è fondamentale. L'intelligenza artificiale ha il potenziale per trasformare l'allocazione delle risorse da un approccio reattivo a uno proattivo e strategico.

Comprendere la necessità di un utilizzo ottimale delle risorse:Le forze dell'ordine operano spesso con budget e personale limitati. Tuttavia, ci si aspetta che garantiscano la sicurezza degli spazi urbani in espansione e affrontino le minacce emergenti. Garantire che ogni risorsa sia utilizzata in modo ottimale non è solo una questione di efficienza: è fondamentale per la sicurezza e la fiducia dei cittadini.

Pianificazione strategica basata sull'intelligenza artificiale:Oltre alle implementazioni quotidiane, l'intelligenza artificiale gioca un ruolo importante anche nella pianificazione strategica a lungo termine. Ad esempio:

- Organizzazione delle pattuglie:Invece di percorsi generici, l'intelligenza artificiale può progettare percorsi di pattugliamento che cambiano in base all'ora del giorno, al giorno della settimana o a modelli di attività noti, garantendo che gli agenti siano presenti dove è più probabile che siano necessari.
- Risposta alle emergenze:L'intelligenza artificiale può aiutare a pianificare una risposta rapida alle emergenze proponendo percorsi ottimali, analizzando i dati sul traffico in tempo reale o persino prevedendo potenziali incidenti o minacce secondarie.
- Sicurezza degli eventi pubblici:I grandi raduni pubblici, dai concerti agli eventi sportivi o alle sfilate, possono rappresentare una sfida per la sicurezza. L'intelligenza artificiale può

analizzare gli eventi passati, le dinamiche della folla, i colli di bottiglia in entrata/uscita e persino le chiacchiere sui social media per contribuire a progettare un piano di sicurezza completo.

Valutazione dell'efficacia delle politiche/strategie:L'intelligenza artificiale non offre solo strumenti di pianificazione, ma è anche fondamentale per la valutazione. Le revisioni post-incidente possono essere analizzate per determinare l'efficacia delle implementazioni o delle politiche anticrimine.

Gli agenti di polizia erano posizionati in modo ottimale? I risultati dell'IA corrispondevano ai modelli reali? Tali valutazioni possono essere reimmesse nel sistema, garantendo un apprendimento continuo e la revisione di politiche e strategie.

> In conclusione, l'allocazione delle risorse e la pianificazione strategica basate sull'intelligenza artificiale migliorano la capacità delle forze dell'ordine di salvaguardare le comunità. Trasformando enormi quantità di dati in informazioni fruibili e imparando costantemente dai successi e dagli insuccessi, l'intelligenza artificiale garantisce che le forze dell'ordine rimangano agili, proattive e sempre adattabili alle sfide in continua evoluzione del mondo moderno.

IA generativa

La frontiera dell'IA non risiede solo nell'analisi di dati e informazioni esistenti, ma anche nella creazione di contenuti completamente nuovi. L'IA generativa, un dominio in rapida evoluzione, utilizza algoritmi per generare contenuti, inclusi testi, immagini e altre forme di media. Queste tecnologie apprendono modelli, strutture e complessità da vasti set di dati e quindi producono nuovi dati che aderiscono agli stessi modelli. Ad esempio, dopo aver analizzato migliaia di immagini di gatti, un modello generativo può creare una nuova immagine sintetica di un gatto che, sebbene interamente fittizia, appare indistintamente reale. Alcune delle forme più importanti di IA generativa includono le reti generative avversarie (GAN) eModelli linguistici di grandi dimensioni (LLM).

Reti generative avversarie (Le GAN (Gear Networks) sono una classe di framework di apprendimento automatico in cui una rete neurale impara a generare dati sintetici il più realistici possibile, mentre l'altra impara a rilevare dati sintetici. Mentre le reti interagiscono tra loro, entrambe migliorano costantemente le proprie prestazioni nel tempo. Le GAN, più specificamente le reti di generazione di dati sintetici, sono ampiamente utilizzate nella generazione di immagini, nella generazione di video e, sempre più, in altri ambiti come la musica.

Le reti GAN potrebbero offrire alle forze dell'ordine strumenti per valutare le prestazioni dei sistemi biometrici senza compromettere la privacy degli individui[41] Ad esempio, le reti GAN possono contribuire a generare immagini facciali sintetiche, impronte digitali e altri dati biometrici, che possono essere a loro volta utilizzati al posto di dati reali, laddove questi ultimi potrebbero non essere prontamente disponibili, per valutare l'accuratezza e la robustezza dei sistemi di riconoscimento in diverse popolazioni e condizioni. Inoltre, consentono lo sviluppo di tecnologie anti-spoofing per combattere le frodi d'identità.[42][43]Tuttavia, man mano che queste tecnologie vengono adottate, è fondamentale per le forze dell'ordine

per bilanciare i benefici con considerazioni etiche e tutela della privacy, assicurando che l'uso di media sintetici favorisca la sicurezza pubblica nel rispetto dei diritti individuali.

Modelli linguistici di grandi dimensioni(Gli LLM (Language Learning) si riferiscono a una forma di intelligenza artificiale generativa con applicazioni nell'elaborazione del linguaggio naturale (NLP). Questi modelli sono progettati per elaborare e generare il linguaggio umano. Essendo addestrati su ampi set di dati testuali, sono in grado di eseguire diverse attività orientate al linguaggio. Questi modelli segnano un progresso sostanziale nel modo in cui le macchine comprendono e producono il linguaggio umano, con ampie implicazioni in diversi settori come la tecnologia, l'intrattenimento e l'istruzione, tra gli altri.

Gli LLM possono offrire notevoli vantaggi alle forze dell'ordine. Tra questi, il supporto agli investigatori nell'indagare su aree di criminalità poco note, la facilitazione della ricerca open source e dell'analisi di intelligence, nonché lo sviluppo di strumenti investigativi tecnici.[44]Inoltre, gli LLM possono contribuire ad accelerare numerose attività amministrative, come la redazione di relazioni e la sintesi delle informazioni. Tuttavia, l'utilizzo degli LLM da parte delle forze dell'ordine richiederebbe un ambiente sicuro, a cui affidare la gestione di informazioni sensibili, nonché valutazioni approfondite sulla tutela dei diritti fondamentali e sulla mitigazione di potenziali pregiudizi.

Nonostante le loro impressionanti capacità, gli LLM presentano diversi limiti, come la tendenza a produrre contenuti fattualmente inaccurati o illogici, comunemente definiti "allucinazioni".Generazione aumentata del recupero (RAG) emerge come una potenziale soluzione ad alcune di queste sfide. Mentre molti LLM si basano principalmente su conoscenze preesistenti o informazioni accessibili al pubblico per produrre testi, RAG fa un ulteriore passo avanti integrando meccanismi di recupero delle informazioni. Ciò significa che i modelli RAG possono ricercare e incorporare attivamente informazioni rilevanti da fonti di conoscenza predeterminate e autorevoli, garantendo che il contenuto generato sia non solo coerente, ma anche contestualmente accurato e aggiornato. Le organizzazioni hanno quindi maggiore influenza sul contenuto testuale prodotto, mentre gli utenti hanno una migliore comprensione del processo attraverso il quale l'LLM genera la sua risposta.

> Esplorare le capacità del RAG nella gestione di dataset di indagini penali è essenziale, ma è necessario affrontarlo in modo metodico e conforme alle normative. Nell'era attuale, in cui l'informazione è fondamentale, vi è una domanda senza precedenti di metodi innovativi per analizzare e interpretare dati complessi.

L'intelligenza artificiale generativa rappresenta il passo successivo, passando dall'analisi passiva alla creazione attiva. Per le forze dell'ordine, offre una miniera di possibilità. Tuttavia, come ogni applicazione, il suo potere risiede in un'applicazione giudiziosa ed etica, che bilancia innovazione e responsabilità.

Tecnologico limitazioni e sfide

Nonostante i vantaggi per le forze dell'ordine, l'integrazione dell'intelligenza artificiale si scontra con diversi vincoli tecnici che ne mettono a repentaglio l'efficacia e l'efficienza:

La qualità e l'accessibilità dei dati sono fondamentali per l'efficacia dell'IA nelle forze dell'ordine, ma le sfide derivano dalle disparità nelle pratiche di raccolta e archiviazione dei dati nelle diverse giurisdizioni. Queste variazioni si traducono in set di dati incoerenti che possono essere incompleti o distorti, compromettendo l'integrità dei risultati dell'IA. Inoltre, i dati esistenti spesso non hanno la granularità richiesta per le applicazioni di IA, poiché non sono stati originariamente raccolti con l'IA in mente. Ad esempio, i rapporti di polizia, sebbene informativi, potrebbero non rilevare incidenti non segnalati o non rilevati, distorcendo la formazione e i risultati dell'IA. Protocolli di raccolta dati standardizzati, abbinati a processi di pulizia e arricchimento dei dati, sono essenziali per creare set di dati completi e imparziali. Inoltre, l'integrazione di solide misure di protezione dei dati è fondamentale per salvaguardare la privacy degli individui e garantire la conformità alle normative applicabili in materia di protezione dei dati.
Affrontando queste problematiche, è possibile migliorare l'affidabilità dell'intelligenza artificiale nelle forze dell'ordine, riflettendo e affrontando meglio la complessità delle attività criminali, nel rispetto degli standard etici e legali.

Sfide di integrazione: l'integrazione dell'IA con i sistemi di polizia e i processi di elaborazione dati esistenti presenta diversi ostacoli tecnici. L'incompatibilità tra le moderne soluzioni di IA e le infrastrutture tecnologiche più datate può portare a significativi problemi di integrazione, incidendo sullo scambio di dati e sull'efficienza operativa. Colmare questo divario richiede un duplice approccio: l'ammodernamento dei sistemi legacy per migliorarne la compatibilità con le tecnologie di IA e la progettazione di future soluzioni di IA con particolare attenzione all'interoperabilità e all'integrazione modulare.

Scalabilità e prestazioni in diverse condizioni: l'efficacia degli strumenti di intelligenza artificiale nelle forze dell'ordine deve essere mantenuta indipendentemente dalla scala dei dati o dalla complessità degli scenari operativi. La variabilità degli incidenti e delle condizioni ambientali mette alla prova l'adattabilità dei sistemi di intelligenza artificiale. Per affrontare queste sfide è necessario sviluppare modelli di intelligenza artificiale non solo scalabili, ma anche versatili, in grado di adattarsi a diversi volumi di dati ed esigenze operative senza compromettere le prestazioni.

Manutenzione e supporto tecnico: la rapida evoluzione della tecnologia di intelligenza artificiale richiede aggiornamenti e manutenzione continui per garantirne l'efficienza e la sicurezza. Tuttavia, il supporto tecnico continuo richiesto può mettere a dura prova le risorse delle forze dell'ordine, in particolare quelle con accesso limitato alle competenze informatiche. L'istituzione di framework di supporto dedicati e la collaborazione con i fornitori di tecnologia potrebbero offrire soluzioni sostenibili a queste sfide, garantendo che i sistemi di intelligenza artificiale rimangano aggiornati ed efficaci.

Affrontare queste sfide non è semplice e richiede un quadro di governance dell'IA e uno sforzo concertato da parte di più parti interessate. Collaborazione tra le forze dell'ordine,

Sviluppatori di tecnologie, decisori politici e la comunità sono fondamentali per superare questi limiti tecnologici. Grazie a questa collaborazione, è possibile sviluppare, testare e perfezionare soluzioni innovative per migliorare l'efficienza, l'affidabilità e l'efficacia complessiva delle applicazioni di intelligenza artificiale nelle attività di polizia. Inoltre, investire in ricerca e sviluppo, concentrarsi sull'uso etico dell'intelligenza artificiale e promuovere un ambiente di apprendimento e adattamento continui tra il personale delle forze dell'ordine sono passaggi chiave per superare questi ostacoli.

Etico e sociale

problemi nell'intelligenza artificiale

per le forze dell'ordine

Come dimostrato nella sezione precedente, l'intelligenza artificiale sta diventando uno strumento sempre più essenziale per le attività di polizia in tutta l'Unione europea. Tuttavia, ciò solleva una moltitudine di sfide etiche e sociali che richiedono un'analisi meticolosa. Questo capitolo approfondisce aree critiche di preoccupazione: il potenziale di distorsione dei dati e le conseguenti implicazioni per l'equità; la sottile linea di demarcazione tra sorveglianza per la sicurezza e violazione della privacy individuale; l'urgente necessità di responsabilità e trasparenza nell'impiego dell'intelligenza artificiale, con particolare attenzione alla questione della "scatola nera". Inoltre, il capitolo discuterà la possibilità che l'intelligenza artificiale aggravi o mitighi le questioni relative ai diritti umani e la discriminazione nell'ambito delle forze dell'ordine.

Distorsione dei dati e correttezza

I dati sono il cuore di qualsiasi sistema di intelligenza artificiale e la loro qualità influenza direttamente i risultati prodotti dal sistema. Qualsiasi discordanza nei dati può portare involontariamente a risultati ingiusti o distorti. Un'attività di polizia equa e imparziale è un pilastro fondamentale delle società democratiche e, pertanto, riconoscere ed eliminare i pregiudizi è di particolare interesse per le forze dell'ordine.

> La distorsione nei dati può emergere da numerose fonti. Dati storici[45]
> I dati utilizzati per addestrare i sistemi di intelligenza artificiale possono incorporare pregiudizi sociali di lunga data, che riflettono pregiudizi e pratiche discriminatorie del passato. Ad esempio, se un determinato quartiere è stato storicamente sottoposto a controlli eccessivi da parte della polizia a causa di pregiudizi razziali o socio-economici, un sistema di intelligenza artificiale addestrato su questi dati potrebbe suggerire che l'area è più soggetta ad attività criminali. Tali risultati potrebbero creare un circolo vizioso.[46], portando le forze dell'ordine a continuare a controllare eccessivamente quell'area, riscontrando così un numero sproporzionato di crimini e rafforzando i pregiudizi presenti nei dati.

Oltre ai pregiudizi storici, c'è anche la sfida dei pregiudizi rappresentativi[47]Se i dati non rappresentano adeguatamente tutti i segmenti della popolazione, il sistema di intelligenza artificiale può effettuare previsioni errate. I gruppi sovrarappresentati possono essere colpiti in modo sproporzionato. Ad esempio, uno studio dell'Agenzia europea per i diritti dell'uomo (FRA)[48]hanno scoperto che gli algoritmi di rilevamento di discorsi offensivi, come quelli per l'identificazione di discorsi d'odio o molestie, presentavano tassi di errore più elevati per alcuni gruppi socioeconomici. Un fattore determinante è l'associazione di determinati termini con gruppi etnici (ad esempio, "musulmano", "gay", "ebreo"), che può indurre gli algoritmi a classificare erroneamente termini non offensivi.

frasi come offensive. Poiché questi termini sono utilizzati più frequentemente dai rispettivi gruppi etnici, vi è una maggiore probabilità che il loro contenuto venga erroneamente segnalato come offensivo e successivamente rimosso, a causa della loro sovrarappresentazione nei dati di addestramento. D'altro canto, i gruppi sottorappresentati nei dati potrebbero non beneficiare dello stesso livello di protezione da parte delle forze dell'ordine.

Vale la pena notare che non esiste un accordo universale sulle definizioni precise di equità. Esistono diverse interpretazioni. In alcuni casi, è giustificato utilizzare categorie protette come genere ed età; ad esempio, un sistema di intelligenza artificiale che deduce informazioni sui minori per garantire una protezione aggiuntiva deve essere addestrato con dati sensibili pertinenti. Pertanto, queste situazioni dovrebbero essere valutate individualmente e, in ultima analisi, spetta sempre agli esseri umani determinare come agire in base alle informazioni fornite dall'intelligenza artificiale.

Privacy e sorveglianza

Nelle forze dell'ordine, trovare il giusto equilibrio tra sicurezza pubblica e privacy individuale è sempre stata una sfida. Con la crescente integrazione dell'intelligenza artificiale nei metodi di polizia, questo equilibrio diventa ancora più delicato.

Storicamente, le forze dell'ordine in tutta l'UE operano all'interno di un solido quadro legislativo e regolamentare. L'introduzione di regolamenti come il Regolamento generale sulla protezione dei dati (GDPR) e la Direttiva sulle attività di contrasto (LED) sottolinea la posizione proattiva dell'UE nella tutela della protezione dei dati e dei diritti alla privacy individuali. Questi regolamenti costituiscono pilastri fondamentali che regolano l'intersezione tra tecnologia e diritti dei cittadini, rafforzati da solidi meccanismi di applicazione, una visione d'insieme umana e vie di ricorso. Non si tratta semplicemente di quadri giuridici, ma di misure complete volte a garantire il trattamento responsabile dei dati personali, promuovendo la trasparenza, la responsabilità e la fiducia nelle interazioni digitali.

Sebbene l'IA offra vantaggi significativi alle forze dell'ordine, come la capacità di elaborare enormi quantità di dati e di utilizzare dati biometrici per una rapida identificazione dei criminali e una valutazione delle minacce, comporta anche sfide complesse. Tecnologie avanzate come i sistemi di riconoscimento facciale possono migliorare notevolmente l'efficienza. Tuttavia, senza garanzie sufficienti, come la supervisione umana per valutarne i risultati, queste tecnologie rischiano di violare diritti fondamentali, come il diritto alla vita privata e il diritto alla protezione dei dati personali (artt. 7 e 8 della Carta dei diritti fondamentali dell'UE). Ciò potrebbe manifestarsi in una sorveglianza sproporzionata di individui innocenti o nel potenziale uso improprio di gruppi specifici, sollevando preoccupazioni in merito alla privacy e alla necessità di tale monitoraggio.

Mentre il mondo affronta le implicazioni dell'intelligenza artificiale e della sorveglianza, l'UE, rafforzata dalle sue severe normative, dall'etica istituzionale e da una storia di priorità per i suoi cittadini, è in una posizione unica per tracciare un percorso in cui i progressi tecnologici rafforzano la sicurezza senza

compromettere i diritti individuali. Questa coesistenza può fungere da modello globale, garantendo che la tecnologia rimanga uno strumento per il miglioramento della società.

Responsabilità e trasparenza

Responsabilità e trasparenza sono principi fondamentali nelle società democratiche, che garantiscono che le strutture di potere rimangano al servizio della comunità e funzionino con integrità. Poiché l'intelligenza artificiale sta diventando uno strumento di primo piano nelle forze dell'ordine, questi principi devono essere in prima linea per preservare la fiducia del pubblico e garantire la giustizia.

Nonostante i vantaggi offerti dalla tecnologia, una delle principali preoccupazioni è la possibilità che decisioni, previsioni o raccomandazioni formulate dall'IA rimangano inspiegate o ingiustificate. Quando l'output dell'IA viene utilizzato per supportare il processo decisionale nelle forze dell'ordine, che si tratti di identificazione biometrica o di valutazione delle minacce, è fondamentale che sia gli agenti di polizia sia coloro che sono interessati da queste decisioni ne comprendano le motivazioni. Senza questa chiarezza, il rischio di sfiducia, abusi e potenziali ingiustizie aumenta.

Nell'UE, la richiesta di responsabilità e trasparenza non è una novità. Tuttavia, la natura unica dell'IA, in cui gli algoritmi operano spesso con livelli di complessità che vanno oltre la comprensione umana, introduce nuove sfide.

> C'è un bisogno urgente di meccanismi che rendano interpretabili i processi decisionali dell'IA, soprattutto in ambienti ad alto rischio come la polizia e la giustizia penale, non solo in termini di come le prove rilevanti vengono raccolte, elaborate e presentate davanti a un tribunale, ma anche in senso più ampio per garantire che i cittadini possano comprendere, interagire e contestare l'uso dell'IA.

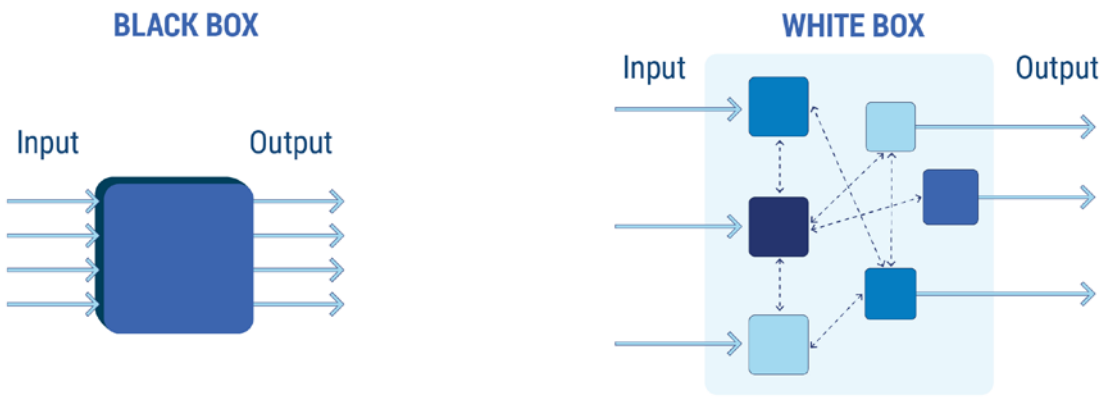
Garantire la responsabilità implica anche stabilire responsabilità chiare. Quando uno strumento di intelligenza artificiale viene utilizzato per generare raccomandazioni o fare previsioni, chi deve essere ritenuto responsabile in caso di errore o se ciò comporta un'ingiustizia? Sono gli sviluppatori del software, le forze dell'ordine che utilizzano lo strumento o l'autorità di regolamentazione generale?

corpo? La definizione di responsabilità è fondamentale per garantire che gli strumenti di intelligenza artificiale nelle forze dell'ordine rimangano efficaci e giusti.

Il problema della scatola nera

Nelle discussioni sulla trasparenza dell'IA, una preoccupazione centrale e urgente è l'enigmatica questione della "scatola nera". In sostanza, il dilemma della scatola nera sottolinea l'opacità intrinseca degli algoritmi di IA complessi, con particolare attenzione alla complessità dei modelli di deep learning.[49]Questi modelli di Machine Learning (ML) sono progettati per emulare l'elaborazione umana delle informazioni. Impiegando più livelli di neuroni artificiali connessi a una rete per estrarre funzionalità avanzate dai dati di input, portano l'etichetta "deep". Tuttavia, ciò che solleva interrogativi profondi è la loro capacità di prendere decisioni o fare previsioni prive di una spiegazione chiara e lineare per la loro logica. Proprio come una scatola nera opaca e sigillata, questi algoritmi producono risultati senza esporre il loro funzionamento interno per consentire una valutazione della logica applicata.

Nel settore delle forze dell'ordine, questa opacità rappresenta una sfida significativa. Quando un sistema basato sull'intelligenza artificiale solleva preoccupazioni circa la potenziale minaccia per un individuo o raccomanda l'invio di ulteriori agenti di pattuglia in un'area specifica, diventa fondamentale per gli agenti delle forze dell'ordine e per le persone interessate.



Risolvere il problema della scatola nera non è solo una sfida tecnica; è un profondo imperativo etico. Soluzioni innovative, come l'intelligenza artificiale spiegabile (XAI), sono alla base di questo approccio.[50], sono attivamente in fase di sviluppo per colmare questa lacuna e rendere questi algoritmi più trasparenti e comprensibili. Tuttavia, finché tali soluzioni non diventeranno universalmente accessibili e standardizzate, la questione della scatola nera rimarrà un punto focale indispensabile nella ricerca continua di un quadro di controllo basato sull'intelligenza artificiale che sia responsabile, equo e trasparente per tutte le parti interessate.

Va inoltre sottolineato che gli algoritmi di intelligenza artificiale possono essere poco trasparenti a causa del loro status di segreti commerciali. In questi casi, i titolari del trattamento dei dati evitano di condividere i dettagli del funzionamento interno degli algoritmi per proteggere i segreti commerciali ed evitare la manipolazione del sistema.

Tornando al panorama più ampio, diventa evidente che affinché l'intelligenza artificiale possa realmente apportare benefici alle forze dell'ordine nell'Unione europea e mantenere la fiducia del pubblico, è essenziale un impegno rigoroso verso la responsabilità e la trasparenza.[51]Per stabilire questo equilibrio sono indispensabili lo sviluppo di quadri che spieghino i processi decisionali dell'IA, insieme a standard normativi ben definiti e chiarezza nell'assegnazione delle responsabilità.

Diritti umani e discriminazione

Nell'Unione Europea, dove i diritti umani sono profondamente radicati nei nostri valori fondamentali, l'integrazione dell'IA nelle forze dell'ordine pone diverse sfide. La preoccupazione principale è il rafforzamento o l'amplificazione involontaria dei pregiudizi sociali da parte dell'IA, dovuta alla dipendenza da dati storici. Come discusso, tali pregiudizi possono portare a un'ingiustificata presa di mira di specifici gruppi sociali, con conseguente sproporzione delle attività di polizia.

Inoltre, le capacità predittive dell'intelligenza artificiale possono erroneamente classificare gli individui sulla base di modelli di dati generali. Tali generalizzazioni potrebbero rischiare di violare il principio fondamentale di "innocente fino a prova contraria", sollevando valide preoccupazioni circa il diritto a un giusto processo.

Per promuovere un'integrazione equilibrata dell'IA in questo paradigma critico, le forze dell'ordine hanno a disposizione una serie di opzioni. In primo luogo, l'importanza di condurre audit approfonditi non può essere sopravvalutata. Ogni sistema di IA, prima della sua implementazione attiva nelle forze dell'ordine, dovrebbe essere sottoposto a una valutazione approfondita. Sebbene la robustezza tecnica di questi sistemi sia essenziale, è altrettanto importante garantirne la conformità ai quadri normativi pertinenti, come le linee guida etiche per un'IA affidabile, introdotte dall'High-Level Expert Group on intelligenza artificiale[52]Individuando e affrontando eventuali pregiudizi intrinseci in questa fase, possiamo gettare le basi per implementazioni dell'IA eque e imparziali.

Altrettanto cruciale è la necessità di facilitare il coinvolgimento della comunità. Alcune comunità si trovano spesso escluse dal flusso principale dei progressi tecnologici, subendone spesso impatti negativi indesiderati. Promuovendo un dialogo continuo con queste comunità, le forze dell'ordine possono acquisire prospettive uniche, che vanno oltre le valutazioni puramente tecniche. Un coinvolgimento proattivo non solo migliora la fiducia, ma garantisce anche che i sistemi di intelligenza artificiale siano implementati in modo coerente con i più ampi ideali di equità, inclusività e giustizia.

Infine, la natura dinamica dell'IA richiede un monitoraggio e un'evoluzione continui. Le tecnologie evolvono, le norme sociali cambiano e sorgono nuove sfide. In un simile scenario, garantire che le applicazioni di IA nelle forze dell'ordine siano soggette a un monitoraggio continuo diventa fondamentale.

L'artificiale dell'UE

Legge sull'intelligence:

panoramica e contesto

essenziale. Questo controllo iterativo e questo feedback consentono aggiustamenti in tempo reale, garantendo che le iniziative basate sull'intelligenza artificiale nelle forze dell'ordine rispecchino e sostengano costantemente l'impegno dell'UE per la parità di diritti, la giustizia e la dignità umana.

Come evidenziato nella sezione precedente, la crescente integrazione dei sistemi di intelligenza artificiale in vari ambiti delle attività di polizia solleva preoccupazioni in merito alle loro implicazioni etiche, legali e sociali. La Commissione europea, riconoscendo il potenziale trasformativo dell'intelligenza artificiale in tutti i settori della società, ha proposto all'inizio del 2021 un nuovo strumento giuridico per regolamentare l'uso dell'intelligenza artificiale in modo orizzontale, bilanciando al contempo l'innovazione con la tutela dei diritti fondamentali e dei valori sociali.[53]La presente proposta legislativa è denominata "Legge UE sull'intelligenza artificiale" (Legge UE sull'IA). A seguito di una lunga consultazione, il Parlamento europeo e il Consiglio dell'UE hanno raggiunto un accordo e adottato la legge, pubblicata nella Gazzetta Ufficiale il 12 luglio 2025 (Regolamento (UE) 2024/168954). La legge entrerà pienamente in vigore gradualmente, entro due anni, con alcune eccezioni: le disposizioni generali e i divieti entreranno in vigore dopo 6 mesi, le norme di governance e gli obblighi per i modelli di IA di uso generale si applicheranno dopo 12 mesi. Infine, le norme per i sistemi di IA integrati nei prodotti regolamentati (articolo 6(1)) entreranno in vigore dopo tre anni.

Con la crescente adozione dei sistemi di IA, i quadri normativi stanno diventando sempre più importanti per definire chiaramente quali casi d'uso siano legalmente ammissibili. Nell'UE, questo quadro giuridico è stato ora stabilito tramite l'AIA (Atto UE sull'IA). Nello specificare come l'IA può essere utilizzata nell'UE, l'AIA mira a trovare un equilibrio tra la salvaguardia dei valori fondamentali dell'UE e la possibilità per le forze dell'ordine di sfruttare le opportunità offerte dall'IA.

Questa sezione approfondirà gli obiettivi, la portata e le disposizioni chiave dell'AIAct dell'UE, esplorandone le implicazioni per le forze dell'ordine.

Obiettivi, ambito di applicazione e disposizioni chiave

Le nuove normative saranno implementate uniformemente in tutti gli Stati membri, sulla base di una definizione lungimirante di IA, che ne garantirà un'applicazione coerente. Secondo la definizione, "un sistema di IA è un sistema basato su una macchina progettato per operare con diversi livelli di autonomia e che può mostrare adattabilità dopo l'implementazione e che, per obiettivi espliciti o impliciti, deduce, dagli input che riceve, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali" (art. 3 della legge UE sull'IA). La definizione è strettamente in linea con il lavoro delle organizzazioni internazionali che si occupano di intelligenza artificiale, in particolare l'OCSE.

L'ambito di applicazione della legge è molto ampio e comprende sistemi sviluppati con vari approcci (apprendimento automatico, approcci basati sulla logica e sulla conoscenza e approcci statistici o bayesiani) che possono

generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli "ambienti con cui interagiscono".

L'idea principale è quella di regolamentare l'IA in base al suo potenziale di causare danni alla società, seguendo un approccio "basato sul rischio": maggiore è il rischio, più severe sono le norme. La categoria "IA a rischio inaccettabile" vieta le applicazioni considerate una minaccia chiara e assoluta ai valori e ai diritti fondamentali europei, come il social scoring o la manipolazione del comportamento umano (ad esempio, giocattoli che utilizzano l'assistenza vocale per incoraggiare comportamenti pericolosi tra i minori). La categoria "IA ad alto rischio" include invece sistemi specifici che potrebbero mettere a repentaglio la sicurezza delle persone o violare i diritti fondamentali; questi sistemi non saranno vietati, ma saranno piuttosto soggetti a rigorosi requisiti obbligatori, come l'obbligo di sottoporsi a valutazioni di conformità.

I sistemi di intelligenza artificiale che rientrano nella categoria "rischio limitato" saranno vincolati solo da obblighi di base, in particolare in ambiti come la trasparenza. Ad esempio, nel caso di utilizzo di sistemi di intelligenza artificiale come i chatbot, è importante che gli utenti siano consapevoli di interagire con una macchina, consentendo loro di effettuare una scelta consapevole se procedere o meno. Tutte le altre applicazioni di intelligenza artificiale, definite "IA a rischio minimo", possono essere sviluppate e utilizzate all'interno dell'UE senza obblighi aggiuntivi rispetto alla legislazione vigente. Su base volontaria, le aziende possono tuttavia impegnarsi a sottoscrivere codici di condotta aggiuntivi per questi sistemi di intelligenza artificiale.

L'ambito di applicazione dell'atto UE sull'intelligenza artificiale è ampio e comprende sistemi sviluppati utilizzando varie tecniche, tra cui l'apprendimento automatico, metodi logici e basati sulla conoscenza, nonché metodi statistici o bayesiani.[7]Questi sistemi sono in grado di produrre output come contenuti, previsioni, raccomandazioni o decisioni che influenzano gli "ambienti con cui interagiscono"[55]Inoltre, la legge si applica e impone determinati obblighi a un'ampia gamma di attori, tra cui fornitori (ovvero sviluppatori), implementatori (ovvero utenti) e distributori di sistemi di intelligenza artificiale (art. 2(1) della legge UE sull'intelligenza artificiale).

Nelle sezioni seguenti, analizzeremo le principali disposizioni della legge dal punto di vista delle forze dell'ordine. Sebbene non si tratti di un'analisi esaustiva, comprendendole, potremo comprendere meglio come l'UE intenda trarre vantaggio dall'IA, garantendo al contempo che la tecnologia sia utilizzata in modo equo e trasparente per tutti.

USI VIETATI DELL'IA

Nel riconoscere le potenziali insidie e i danni associati a determinati sistemi di IA, la legge UE sull'IA delinea alcune pratiche di IA che sono severamente vietate (art. 5). Questi divieti mirano a impedire l'impiego dell'IA in modi che potrebbero causare potenziali danni, violare i diritti individuali o minare i principi fondamentali dell'UE. Le applicazioni che rientrano in questa categoria includono i sistemi di IA.

7 La statistica bayesiana è un metodo di analisi dei dati che sfrutta il teorema di Bayes per rivedere le conoscenze esistenti sui parametri del modello utilizzando le informazioni ottenute dai dati osservati.

che manipolano il comportamento umano[8], sistemi di punteggio sociale[9] e sistemi di intelligenza artificiale utilizzati per sfruttare le vulnerabilità delle persone (dovute alla loro età, disabilità, situazione sociale o economica).[10]

Inoltre, la legge introduce il divieto di sistemi biometrici remoti in tempo reale (RBI), quando questi sistemi vengono utilizzati in spazi pubblici. Tali sistemi sono in grado di acquisire e analizzare dati biometrici (come tratti del viso, pattern dell'iride, impronte digitali, pattern vocali, ecc.) in tempo reale e a distanza, senza la necessità di interazione diretta o contatto fisico con l'individuo da identificare. Sebbene questi sistemi offrano potenziali vantaggi per le applicazioni di polizia e sicurezza, la loro applicazione in spazi pubblici potrebbe essere considerata intrusiva, "evocare una sensazione di sorveglianza costante e dissuadere indirettamente dall'esercizio della libertà di riunione e di altri diritti fondamentali" (cfr. Considerando 18 della legge UE sull'intelligenza artificiale). Va notato che la legge prevede alcune eccezioni specifiche per le forze dell'ordine (art. 5(1)(h)). Tali eccezioni saranno discusse di seguito.

Inoltre, la legge vieta l'uso di sistemi di intelligenza artificiale che consentono la categorizzazione biometrica delle persone fisiche sulla base di determinati attributi strettamente definiti. Questi sistemi elaborano dati biometrici per dedurre o dedurre la loro razza, le opinioni politiche, l'appartenenza sindacale, le convinzioni religiose o filosofiche o l'orientamento sessuale. Tali sistemi saranno quindi vietati, a meno che non vengano utilizzati per identificare le vittime. Il filtraggio dei set di dati basato sui dati biometrici nell'ambito delle attività di contrasto sarà comunque possibile (art. 5(1)(g)).

Una delle aggiunte più critiche è stata il divieto di sistemi di polizia predittiva individuale. Come già discusso, tali sistemi, progettati per prevedere potenziali attività criminali sulla base di eventi, luoghi o persone, hanno sollevato preoccupazioni. Si teme che questi sistemi possano inavvertitamente rafforzare pregiudizi, portando a sorveglianza o interventi ingiustificati. In risposta a ciò, la legge UE sull'intelligenza artificiale introduce un divieto parziale di polizia predittiva individuale. Il divieto riguarda i sistemi che valutano o prevedono il rischio che una persona fisica commetta un reato, basandosi esclusivamente sulla profilazione della persona fisica o sulla valutazione dei suoi tratti e caratteristiche della personalità. L'uso di sistemi di intelligenza artificiale che supportano la valutazione umana del coinvolgimento in un reato effettivamente commesso è consentito, poiché ciò non è considerato una previsione, ma una valutazione basata su fatti oggettivi e verificabili direttamente collegati a un'attività criminale reale (art. 5(1)(d))

Sebbene i sistemi di identificazione biometrica remota post-evento non siano del tutto vietati, la loro classificazione ad alto rischio impone un processo di valutazione della conformità da parte di terzi (considerando 125 della legge). Inoltre, la legge impone obblighi aggiuntivi per gli utenti dei sistemi RBI post-evento (art. 26(10)). In particolare, nel quadro

8 Applicazioni di intelligenza artificiale che potrebbero potenzialmente alterare il processo decisionale di una persona sfruttandone le vulnerabilità o causando danni.

9 Sistemi che valutano e classificano l'affidabilità degli individui in base ai dati sociali comportamento o caratteristiche di personalità note e previste.

10 Qualsiasi applicazione di intelligenza artificiale progettata per utilizzare tecniche subliminali che una persona potrebbe non riconoscere consapevolmente ma che potrebbero avere un impatto sul suo comportamento.

di un'indagine per la ricerca mirata di una persona condannata o sospettata di aver commesso un reato, l'utilizzatore di un sistema di IA per l'identificazione biometrica post-remota deve richiedere un'autorizzazione prima dell'uso, o senza indebito ritardo e non oltre 48 ore. L'autorizzazione dovrebbe essere rilasciata da un'autorità giudiziaria o amministrativa, la cui decisione è vincolante e soggetta a controllo giurisdizionale. Tale autorizzazione non è necessaria se il sistema viene utilizzato per l'identificazione iniziale di un potenziale sospettato sulla base di fatti oggettivi e verificabili direttamente collegati al reato. Inoltre, la legge UE sull'IA vieta esplicitamente l'uso non mirato dell'identificazione biometrica post-remota nelle attività di contrasto.

La legge UE sull'intelligenza artificiale adotta una posizione ferma nel prevenire la creazione o l'espansione di database di riconoscimento facciale attraverso l'estrazione non mirata di immagini facciali da Internet o da filmati di videosorveglianza (art. 5(1)(e)). L'estrazione non mirata (ad esempio, l'estrazione di dati da un sito web) consiste nella raccolta di immagini facciali senza uno scopo specifico e predefinito. Va oltre l'uso necessario e proporzionato della tecnologia di riconoscimento facciale, accumulando potenzialmente vasti set di dati senza obiettivi chiari. Questo divieto è concepito per affrontare le preoccupazioni relative alla sorveglianza di massa e alle potenziali violazioni dei diritti fondamentali, in particolare del diritto alla privacy.

ECCEZIONI DELLE FORZE DELL'ORDINE ALLE PRATICHE VIETATE

Considerate le specificità delle attività di contrasto, i colegislatori hanno concordato alcune eccezioni alle pratiche di IA vietate, come discusso in precedenza. Fatte salve le opportune garanzie, queste eccezioni intendono riflettere la necessità di dotare le forze dell'ordine di tutti gli strumenti disponibili per essere efficaci contro le moderne forme di criminalità, nel rispetto al contempo della riservatezza dei dati operativi sensibili relativi alle loro attività. Ad esempio, ai sensi dell'articolo 46, paragrafo 2, della legge UE sull'IA, le autorità di contrasto o di protezione civile possono mettere in servizio con urgenza uno specifico sistema di IA ad alto rischio per motivi di sicurezza pubblica o in caso di una minaccia specifica, sostanziale e imminente alla vita o all'incolumità fisica delle persone. Ciò può essere fatto senza autorizzazione preventiva, a condizione che una richiesta di autorizzazione venga presentata durante o immediatamente dopo l'utilizzo del sistema. Se l'autorizzazione viene successivamente respinta, l'utilizzo del sistema deve essere interrotto immediatamente e tutti i risultati e gli output derivanti dal suo utilizzo devono essere eliminati.

Inoltre, ai sensi dell'art. 5(1)(h), l'uso di sistemi di identificazione biometrica remota in tempo reale negli spazi pubblici è possibile solo per finalità di contrasto esaustivamente definite. Tali finalità includono la ricerca mirata delle vittime, la prevenzione di attacchi terroristici e minacce alla vita, e la localizzazione di criminali sospettati di essere coinvolti in reati gravi e di criminalità organizzata.

Le circostanze in cui alle forze dell'ordine è consentito utilizzare sistemi RBI in tempo reale sono soggette a condizioni specifiche (art. 5(2)(a)):

- Individui specificamente presi di mira:L'uso è limitato alla conferma dell'identità di individui specificamente presi di mira. Ciò implica che l'RBI in tempo reale non dovrebbe essere utilizzato per scopi di sorveglianza indiscriminata o di identificazione generica.
- Ambito limitato:L'uso dell'RBI in tempo reale deve essere strettamente necessario e mirato. Ciò include limitazioni relative agli individui da identificare, alla posizione, all'ambito temporale e alla base di un set di dati chiuso di filmati video acquisiti legalmente.
- Valutazione d'impatto sui diritti fondamentali (FRIA):Le autorità preposte all'applicazione della legge sono tenute a completare una valutazione d'impatto sui diritti fondamentali prima di utilizzare questi sistemi. Tale valutazione valuterebbe il potenziale impatto sui diritti e sulle libertà degli individui.
- Requisiti di autorizzazione:L'uso di tali sistemi in spazi accessibili al pubblico per finalità di contrasto deve essere espressamente e specificamente autorizzato da un'autorità giudiziaria o da un'autorità amministrativa indipendente. Sebbene la legge UE sull'intelligenza artificiale preveda eccezioni a questa regola,[11], idealmente questa autorizzazione dovrebbe essere ottenuta prima dell'utilizzo del sistema (o entro 24 ore).
- Leggi nazionali:Le eccezioni per l'uso dell'RBI in tempo reale da parte delle forze dell'ordine saranno possibili solo se esiste una legislazione nazionale che lo preveda esplicitamente, come delineato nella legge UE sull'intelligenza artificiale. Pertanto, gli Stati membri hanno la flessibilità di decidere se le eccezioni saranno applicabili nel loro Paese, se introdurre condizioni più severe o persino un divieto orizzontale di tali sistemi.
- Notifica all'autorità di vigilanza del mercato:L'autorità di vigilanza del mercato competente e l'autorità nazionale per la protezione dei dati devono essere informate di ogni utilizzo del "sistema di identificazione biometrica in tempo reale".

Le eccezioni previste dalla legge sull'intelligenza artificiale dell'UE sono benvenute dal punto di vista delle forze dell'ordine. Questi sistemi consentono interventi mirati ed efficaci, evitando al contempo misure di fermo e perquisizione sproporzionate basate su razza, etnia o caratteristiche fisiche distintive. Questo cambiamento strategico verso un uso più mirato della tecnologia non solo migliora la capacità delle forze dell'ordine di garantire la sicurezza pubblica, ma riduce anche significativamente la probabilità di pratiche discriminatorie che storicamente hanno compromesso gli sforzi di polizia.

Tuttavia, sebbene queste eccezioni siano viste come uno sviluppo positivo, introducono anche un livello di complessità nel contesto più ampio dell'adozione e dell'applicazione degli strumenti di intelligenza artificiale nell'ambito della legge.

11 Sono ammesse eccezioni in situazioni urgenti in cui non sia possibile ottenere un'autorizzazione preventiva, ma anche in questi casi l'uso deve essere limitato al minimo indispensabile. In caso di rifiuto dell'autorizzazione, l'uso dei sistemi di identificazione biometrica in tempo reale ad essa collegati dovrebbe essere interrotto con effetto immediato e tutti i dati relativi a tale utilizzo dovrebbero essere eliminati e cancellati.

Applicazione. Sebbene la legge sia concepita per garantire che le tecnologie pertinenti siano utilizzate in modo da tutelare i diritti fondamentali e promuovere la fiducia tra i cittadini, ciò potrebbe anche rallentare il processo di adozione, poiché le forze dell'ordine devono districarsi tra i requisiti normativi aggiuntivi, assicurandosi che i loro strumenti di intelligenza artificiale siano conformi ai nuovi standard.

Questo attento equilibrio tra l'utilizzo dell'IA per migliorare le capacità di contrasto e il rispetto degli standard etici, legali e normativi stabiliti dalla legge UE sull'IA influenzerà probabilmente il modo in cui le tecnologie di IA vengono sostenute e implementate dalle forze dell'ordine in tutta l'UE. Il successo di questo sforzo dipende dalla ricerca di una via di mezzo che consenta l'uso innovativo dell'IA a fini di polizia, tutelando al contempo da un uso improprio della tecnologia che potrebbe violare i diritti e le libertà individuali.

SISTEMI DI IA AD ALTO RISCHIO

La legge UE sull'intelligenza artificiale identifica alcune applicazioni di intelligenza artificiale nell'ambito delle forze dell'ordine come "ad alto rischio" a causa del loro significativo potenziale di impatto sui diritti, le libertà e la sicurezza individuali. Classificando questi sistemi come ad alto rischio, il nuovo quadro normativo impone una serie di requisiti rigorosi per garantirne un utilizzo etico e responsabile.

Tra le applicazioni considerate ad alto rischio figurano i sistemi biometrici utilizzati per l'identificazione univoca di individui, come il riconoscimento delle emozioni, e i poligrafi, volti a valutare l'affidabilità o lo stato emotivo di una persona. Altre applicazioni ad alto rischio includono alcuni sistemi di categorizzazione, nonché sistemi progettati per valutare il rischio di vittimizzazione o reato analizzando la probabilità che gli individui diventino vittime o autori di reati, tra cui la tratta di esseri umani, la violenza domestica o la criminalità informatica. Inoltre, le tecnologie di intelligenza artificiale impiegate per esaminare l'affidabilità delle prove durante le indagini penali o per scopi di profilazione nelle fasi di indagine e perseguimento penale sono soggette a queste rigorose normative.

In particolare, nonostante la loro iniziale classificazione come ad alto rischio, il testo finale dell'EU AI Act ha escluso le tecnologie per il rilevamento dei deepfake e l'analisi dei crimini, riflettendo un approccio sfumato nel bilanciare i vantaggi di queste tecnologie con le preoccupazioni relative alla privacy, all'etica e ai rischi di abuso.

Alla luce della classificazione di alcuni sistemi come ad alto rischio, utenti, fornitori, sviluppatori e venditori di tali sistemi di intelligenza artificiale dovrebbero seguire alcune regole rigorose. Ogni applicazione, ad esempio, deve essere sottoposta a un approfondito processo di valutazione e mitigazione del rischio per comprendere e contrastare potenziali pericoli (valutazione di conformità). Deve essere inoltre eseguita un'approfondita valutazione d'impatto sui diritti fondamentali (FRIA). I dati fondamentali che guidano questi sistemi di intelligenza artificiale devono essere della massima qualità, non solo per ridurre i rischi, ma anche per aggirare eventuali esiti discriminatori e distorsioni algoritmiche.

IL MECCANISMO DI FILTRO PER LA VALUTAZIONE DEI SISTEMI AD ALTO RISCHIO

La legge UE sull'intelligenza artificiale introduce un sistema di filtri per affrontare le preoccupazioni relative al fatto che la classificazione di "alto rischio" per alcune applicazioni di intelligenza artificiale possa essere eccessivamente ampia (art. 6(3)). Questo sistema consente ai fornitori di sistemi di intelligenza artificiale che potrebbero rientrare nella categoria ad alto rischio, ma che non presentano un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, di condurre autovalutazioni. Il meccanismo di filtro si concentra sui sistemi di intelligenza artificiale progettati per funzionalità specifiche e meno rischiose, comprese quelle per compiti procedurali ristretti, revisione o miglioramento di compiti completati da esseri umani, identificazione di modelli decisionali e svolgimento di compiti preliminari nella preparazione di valutazioni critiche.[12].

Per le forze dell'ordine che impiegano l'intelligenza artificiale, questo meccanismo di filtro potrebbe apportare significativi vantaggi operativi, riducendo gli oneri normativi per i sistemi di intelligenza artificiale considerati a basso rischio. Ad esempio, strumenti di intelligenza artificiale che assistono nell'organizzazione delle prove o nella gestione dei dati, a condizione che non valutino direttamente l'affidabilità delle prove o profilino gli individui. Un altro esempio potrebbero essere i sistemi di intelligenza artificiale che ottimizzano la logistica della raccolta delle prove o i sistemi utilizzati per organizzare e incrociare registri pubblici e fascicoli, e che supportano le fasi iniziali di un'indagine, che potrebbero anch'essi rientrare in questo meccanismo di filtro.

Tuttavia, il funzionamento di questo sistema di filtraggio potrebbe porre sfide pratiche, tra cui potenziali difficoltà nel determinare l'ammissibilità alle esenzioni e nel garantire che l'uso dell'IA rimanga entro i limiti di legge. Ciò potrebbe comportare incertezze riguardo alla portata delle esenzioni e alla necessità di linee guida ed esempi chiari da parte della Commissione europea per garantire che le forze dell'ordine possano trarne pieno beneficio, senza compromettere gli standard legali o le considerazioni etiche.

Implicazioni per le forze dell'ordine

L'introduzione della legge UE sull'intelligenza artificiale pone diverse sfide e implicazioni per l'uso dell'intelligenza artificiale da parte delle forze dell'ordine in tutta l'UE, in particolare per quanto riguarda l'implementazione e l'utilizzo di strumenti basati sull'intelligenza artificiale che includono l'intelligenza artificiale. In primo luogo, la posizione esplicita della legge sul divieto di determinate pratiche di intelligenza artificiale implica l'immediata necessità di interrompere l'implementazione di queste tecnologie. Le forze di polizia, che potrebbero già utilizzare determinati sistemi di intelligenza artificiale, dovranno ora affrontare il difficile compito di rivalutare questi strumenti. Se una qualsiasi di queste tecnologie operative dovesse rientrare nella categoria vietata dalla legge, dovrebbe essere disattivata, con potenziali difficoltà nel mantenimento della continuità operativa. Ciò solleva la domanda: come?

12 La Commissione Europea ha il compito di elaborare linee guida per l'applicazione di questi filtri, con l'obiettivo di chiarire e semplificare il processo di conformità per i fornitori di sistemi di IA. È opportuno sottolineare che i sistemi di IA utilizzati per la profilazione delle persone fisiche dovrebbero sempre essere considerati applicazioni ad alto rischio.

la transizione sarà gestita per i sistemi legacy in base alle nuove normative?

Inoltre, il processo di valutazione della conformità per i sistemi considerati ad alto rischio dalla legge UE sull'intelligenza artificiale sarà senza dubbio complesso e dispendioso in termini di tempo. Le autorità competenti saranno tenute a valutare in modo completo questi sistemi alla luce delle disposizioni stabilite dal nuovo regolamento.
In molti casi, ciò potrebbe comportare modifiche sostanziali ai sistemi esistenti per garantire l'allineamento ai nuovi standard. Di conseguenza, ciò non solo suggerisce potenziali modifiche al software, ma evidenzia anche la necessità di allocare risorse aggiuntive, sia in termini finanziari che di personale.

Inoltre, l'influenza della legge non si limita ai soli sistemi di intelligenza artificiale di nuova implementazione. Considerata la natura dinamica dell'intelligenza artificiale, la sua continua evoluzione e i suoi aggiornamenti, anche i sistemi già operativi saranno soggetti a queste normative. La natura in continua evoluzione dell'intelligenza artificiale implica che le forze dell'ordine saranno sottoposte a un ciclo perpetuo di revisione e modifica, garantendo che i loro sistemi, anche se precedentemente conformi, rimangano in linea con le normative, soprattutto se gli aggiornamenti ne alterano le funzioni o i rischi associati.

Uno scenario particolarmente impegnativo emerge per le LEA che hanno preso l'iniziativa di sviluppare internamente strumenti di IA. Queste agenzie si troveranno ad affrontare la duplice responsabilità di garantire la conformità sia come utenti che come sviluppatori. Ciò implica essenzialmente un investimento sostanziale per garantire che ogni fase del processo, dallo sviluppo, alla raccolta dei dati, alla formazione e all'implementazione, sia rigorosamente conforme ai requisiti dell'Atto UE sull'IA.

Ulteriori garanzie nel contesto della RBI per le forze dell'ordine.

Data la natura sensibile delle implementazioni RBI e le implicazioni sulla privacy e su altri diritti fondamentali, la legge UE sull'intelligenza artificiale prevede ulteriori garanzie per l'uso di tali sistemi. Ai sensi del regolamento, le forze dell'ordine che utilizzano tali sistemi devono garantire che nessuna decisione che produca un effetto giuridico negativo su una persona possa essere presa esclusivamente sulla base dei risultati di questi sistemi di identificazione biometrica post-remota (cfr. art. 26 (10) della legge UE sull'intelligenza artificiale). Pertanto, il nuovo regolamento impone un ulteriore livello di verifica e conferma.

Per raggiungere questo obiettivo è necessaria una combinazione di garanzie tecnologiche, procedurali e legali, come la convalida umana, l'implementazione di sistemi biometrici multimodali, la definizione di soglie di confidenza appropriate e la formazione degli operatori umani sulle capacità e i limiti della tecnologia di identificazione biometrica.

Inoltre, la legge UE sull'intelligenza artificiale considera una migliore visione d'insieme umana come un requisito per tali sistemi, in modo che nessuna azione o decisione possa essere intrapresa a meno che l'output del sistema RBI non sia stato verificato e confermato separatamente da almeno due persone fisiche, dotate delle competenze, della formazione e dell'autorità necessarie (art. 14 (5)).

Il requisito di una verifica separata da parte di almeno due persone fisiche non si applica ai sistemi di IA ad alto rischio utilizzati a fini di contrasto, migrazione, controllo delle frontiere o asilo, nei casi in cui il diritto dell'Unione o nazionale ritenga sproporzionata l'applicazione di tale requisito. Il mandato del cosiddetto principio dei quattro occhi riflette il processo di revisione paritaria che caratterizza in modo prominente le scienze forensi.

Tuttavia, aderire a questo principio per misure investigative piuttosto basilari, come l'identificazione di un criminale, presenta potenziali sfide per le forze dell'ordine, come l'efficienza operativa, la disponibilità di risorse, la soggettività nella verifica, la competenza e la tempestività della formazione in scenari critici e altro ancora.

In qualità di agenzia modello dell'UE per l'applicazione della legge, Europol sta guidando gli sforzi volti a dimostrare la conformità alle disposizioni della legge UE sull'intelligenza artificiale. In tale direzione, Europol, insieme a partner selezionati,[13] ha co-sviluppato CC4AI, uno strumento di verifica della conformità all'AI Act. CC4AI è una guida passo passo progettata per supportare le forze dell'ordine nella valutazione se le applicazioni di intelligenza artificiale esistenti o future utilizzate nelle attività di polizia soddisfano i criteri stabiliti dal nuovo quadro normativo.

Con l'iniziativa CC4AI, Europol intende contribuire a garantire un'adozione e un'attuazione armoniose dell'IA dell'UE

Garantire l'osservanza dei requisiti delle forze dell'ordine nell'UE, prevenendo così incongruenze che potrebbero potenzialmente ostacolare la futura collaborazione tra forze di polizia. L'accesso a CC4AI sarà offerto gratuitamente alle agenzie per la sicurezza interna.

Sebbene il nuovo regolamento offra un quadro completo volto a massimizzare i vantaggi dell'IA senza compromettere gli standard etici e la sicurezza pubblica, introduce anche una serie complessa di sfide per le autorità competenti. Per muoversi con successo in questo terreno normativo sarà necessaria una profonda comprensione dell'IA.

13 Agenzie GAI dell'UE (CEPOL, Eurojust, EUAA e EU FRA) dell'EU Innovation Hub per la sicurezza interna e del Centro di eccellenza per la ricerca sul terrorismo, la resilienza, l'intelligence e la criminalità organizzata (CENTRIC)

aspetti tecnologici, uniti a una maggiore consapevolezza delle sue dimensioni legali nell'ambito delle forze dell'ordine.

Innovazione e sandbox normativi

Al centro della legge UE sull'intelligenza artificiale e del suo approccio innovativo c'è l'istituzione di "aree di regolamentazione" coordinate per l'intelligenza artificiale (artt. 57-60). Questi ambienti controllati sono progettati per consentire agli sviluppatori di testare e perfezionare prodotti e servizi di intelligenza artificiale innovativi in un ambiente sicuro. L'enfasi della legge sulle aree di regolamentazione è di grande importanza per le forze dell'ordine. Come ampiamente discusso, le innovazioni dell'intelligenza artificiale, che vanno dall'identificazione biometrica all'analisi avanzata dei dati, offrono vantaggi sostanziali alle forze dell'ordine. Le aree di regolamentazione offrono un'opportunità unica per queste agenzie di esplorare queste tecnologie, comprenderne le implicazioni e identificare eventuali problemi prima dell'implementazione in contesti reali di applicazione della legge.

Inoltre, la legge incoraggia un approccio armonizzato tra gli Stati membri, con l'obiettivo di eliminare le disparità normative. Ciò garantisce che le autorità di polizia di tutta l'UE possano beneficiare uniformemente di Progressi nell'intelligenza artificiale, che promuovono un uso coerente ed efficace della tecnologia nelle operazioni di contrasto.

Un altro aspetto critico affrontato nell'EU AI Act è l'intersezione tra le attività sandbox e le severe normative UE sulla protezione dei dati, tra cui il Regolamento generale sulla protezione dei dati (GDPR) e la Direttiva sulle forze dell'ordine (LED).
La legge riconosce l'importanza di bilanciare la necessità di sperimentazione con l'aderenza ai principi di protezione dei dati, sottolineando la necessità di trasparenza nell'implementazione e nell'uso dell'intelligenza artificiale all'interno di sandbox, soprattutto in settori sensibili come le forze dell'ordine, dove la fiducia del pubblico è fondamentale.

Le disposizioni contenute nella legge UE sull'intelligenza artificiale relative alle sandbox normative rappresentano un approccio lungimirante, che consente alle forze dell'ordine di sfruttare il potenziale delle tecnologie di intelligenza artificiale. Affrontando le principali preoccupazioni in materia di responsabilità, armonizzazione normativa e protezione dei dati, la legge garantisce che l'innovazione possa avvenire in modo responsabile, trasparente e in linea con i valori e i diritti fondamentali tutelati dall'Unione europea. Già nel 2022, i legislatori dell'UE avevano previsto l'utilizzo di sandbox per consentire a Europol di trattare i dati personali ai fini dei suoi progetti di ricerca e innovazione per addestrare, testare e convalidare algoritmi, in un ambiente di elaborazione dati separato, isolato e protetto (art. 33a del regolamento Europol).[14].

14 REGOLAMENTO (UE) 2022/991 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO dell'8 giugno 2022 che modifica il regolamento (UE) 2016/794 per quanto riguarda la cooperazione di Europol con i privati, il trattamento dei dati personali da parte di Europol a sostegno delle indagini penali e il ruolo di Europol nella ricerca e nell'innovazione (Fonte: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32022R0991#d1e2572-1-1)

Bilanciamento del benefici e restrizioni

Come evidenziato in tutto il rapporto, la fusione tra intelligenza artificiale e attività di polizia promette maggiore efficienza, capacità nuove o migliorate e ottimizzazione delle risorse. Tuttavia, solleva anche questioni critiche, come potenziali pregiudizi, potenziali violazioni dei diritti e delle libertà fondamentali e questioni di responsabilità.

Questa sezione esamina le principali preoccupazioni e le strategie corrispondenti, sottolineando l'importanza di garantire l'equità, salvaguardare i diritti individuali, sostenere rigorosi standard di responsabilità e promuovere un ambiente che promuova sia l'innovazione sia il rigoroso rispetto delle normative.

Affrontare le preoccupazioni relative a pregiudizi e discriminazioni

Sebbene le questioni fondamentali relative alla distorsione dei dati e all'equità nell'IA per le forze dell'ordine siano state elaborate nella sezione 3.1, affrontare queste preoccupazioni va oltre i meri aspetti tecnici dei dati. Le implicazioni della distorsione e dell'ingiustizia nei sistemi di IA hanno un profondo impatto sulle strutture sociali, sulle dinamiche di fiducia e sul più ampio ideale di governance democratica.

> Nelle forze dell'ordine, dove le conseguenze delle decisioni possono cambiare la vita e l'obiettivo è contribuire all'equità e alla giustizia, gli strumenti di intelligenza artificiale devono essere più che semplicemente tecnicamente validi: dovrebbero incarnare i principi di giustizia, equità e imparzialità.

La sfida si estende quindi dalla garanzia dell'equità a livello di dati alla garanzia dell'equa applicazione e interpretazione dei risultati dell'IA in scenari reali. Aderendo a questi principi, le forze dell'ordine possono garantire che le prove elaborate dall'IA soddisfino i rigorosi standard richiesti per l'accettazione in tribunale, preservando così l'integrità del processo giudiziario.

Per affrontare questa sfida dalle molteplici sfaccettature, è necessario un approccio multidisciplinare. Sebbene un sistema di intelligenza artificiale possa essere addestrato su dati imparziali e utilizzare un algoritmo imparziale, il modo in cui i suoi risultati vengono interpretati e applicati dalle forze dell'ordine potrebbe introdurre distorsioni. Garantire che gli agenti comprendano i risultati dell'intelligenza artificiale e seguano linee guida chiare su come agire in base ad essi può prevenire applicazioni errate. Ad esempio, il risultato di un sistema di riconoscimento facciale è semplicemente un'indicazione che due persone presentano somiglianze in una certa misura. Senza decisioni umane e la conferma di questi risultati con informazioni aggiuntive (come impronte digitali o dati biografici), questo risultato non dovrebbe essere utilizzato come probabile causa di arresto.

Inoltre, è necessario istituire meccanismi di supervisione umana e trasparenza. Coinvolgere le comunità nella valutazione degli strumenti di polizia basati sull'intelligenza artificiale può essere un modo efficace per generare fiducia e garantire che i sistemi siano in linea con i valori sociali. I cicli ricorsivi con le comunità possono anche contribuire a perfezionare questi strumenti per garantire che siano maggiormente in linea con le esigenze della comunità. Inoltre, è fondamentale una formazione continua del personale delle forze dell'ordine sulle dimensioni etiche dell'intelligenza artificiale. Gli agenti dovrebbero essere preparati non solo a utilizzare questi strumenti.

strumenti, ma anche comprenderne le implicazioni sulla società, assicurandosi che la tecnologia venga utilizzata in modo responsabile.

In conclusione, sebbene gli aspetti tecnici di parzialità ed equità siano innegabilmente critici, la sfida più ampia consiste nell'integrare l'intelligenza artificiale nell'etica delle forze dell'ordine in modo da sostenere i valori di giustizia, equità e fiducia nella comunità.

Tutela della privacy e protezione dei dati

Con l'affermarsi dei sistemi di intelligenza artificiale nelle forze dell'ordine, aumentano contemporaneamente le preoccupazioni relative alla privacy e alla protezione dei dati. L'uso di analisi basate sull'intelligenza artificiale, di sistemi di polizia predittiva e di sistemi di identificazione biometrica sottolinea l'urgente necessità di proteggere i dati personali e il diritto alla privacy degli individui.

Per affrontare queste sfide è fondamentale stabilire un solido quadro di protezione dei dati e di governance dell'IA. La raccolta dei dati dovrebbe essere regolata dai principi di liceità, correttezza e trasparenza, garantendo che vengano trattati solo i dati necessari e pertinenti. Inoltre, la durata di conservazione dei dati, in particolare per quanto riguarda le informazioni personali, deve essere strettamente limitata a quanto necessario per le finalità per le quali i dati vengono trattati. L'accesso ai dati archiviati dovrebbe essere limitato alle persone o entità autorizzate, in conformità con le leggi applicabili, per impedire l'accesso non autorizzato.

Inoltre, la crittografia e altre misure tecniche e organizzative appropriate devono essere implementate come procedure standard per garantire la sicurezza e la riservatezza dei dati archiviati, proteggendoli così da violazioni e accessi non autorizzati. Per i sistemi di intelligenza artificiale che richiedono l'immissione continua di dati, è fondamentale rispettare il principio di minimizzazione dei dati, raccogliendo solo i dati strettamente necessari. Ciò è in linea con i requisiti delineati nel Regolamento generale sulla protezione dei dati (GDPR) e nella Direttiva sulle forze dell'ordine (LED), che sottolineano l'importanza di limitare il trattamento dei dati personali a quanto essenziale per le finalità previste.

Altrettanto importante è garantire il diritto all'informazione di ogni individuo. I cittadini dovrebbero essere informati sulla natura dei dati raccolti, sulle loro finalità e sulla portata del loro utilizzo. Inoltre, gli individui dovrebbero avere il diritto di accedere, rettificare o persino cancellare i propri dati in determinate circostanze, in conformità con le leggi applicabili in materia di protezione dei dati.

Garantire un'adeguata supervisione umana è essenziale. Sebbene i sistemi di intelligenza artificiale siano in grado di elaborare e analizzare enormi quantità di dati, l'intervento umano è necessario per garantire che l'interpretazione dei dati sia in linea con gli standard legali ed etici. L'esecuzione di audit regolari dei sistemi di intelligenza artificiale può fornire un'ulteriore garanzia di conformità alle normative vigenti in materia di privacy e protezione dei dati.

Anche il coinvolgimento del pubblico e la promozione di una cultura della trasparenza possono contribuire a creare fiducia. Un dialogo aperto sulla portata e i limiti dell'intelligenza artificiale nelle forze dell'ordine, sulle sue implicazioni per la privacy e sulle misure adottate per salvaguardare i dati promuoverà la fiducia e la collaborazione nella comunità.

In sintesi, mentre l'intelligenza artificiale rimodella le moderne attività di polizia, la tutela della privacy e la protezione dei dati sono di fondamentale importanza. Si tratta di trovare un equilibrio tra lo sfruttamento del potenziale delle intuizioni basate sull'intelligenza artificiale e la garanzia che i principi fondamentali della privacy e delle libertà individuali rimangano intatti.

Prospettive future e raccomandazioni

Potenziale di progresso tecnologico

Nel panorama in rapida evoluzione dell'intelligenza artificiale, l'orizzonte per i progressi tecnologici rimane vasto. L'intersezione tra intelligenza artificiale e forze dell'ordine è particolarmente favorevole all'innovazione, promettendo di rimodellare i paradigmi tradizionali di polizia e sicurezza.

- Calcolo quantistico:Con l'avvicinarsi dello sviluppo del calcolo quantistico, la possibilità di gestire calcoli complessi di specifici problemi matematici a velocità senza precedenti potrebbe introdurre nuovi metodi di analisi forense e decifrazione digitale. Il machine learning quantistico può migliorare la velocità di calcolo e le prestazioni dei modelli di intelligenza artificiale a livelli senza precedenti. Un recente rapporto[56]pubblicato dall'Osservatorio dell'Europol fa luce su come l'informatica quantistica e le tecnologie quantistiche avranno un impatto sulle forze dell'ordine e su cosa si dovrebbe fare per prepararsi.

- Connettività 6G:Si prevede che il 6G diventerà una delle prime reti native basate sull'intelligenza artificiale, integrando l'intelligenza artificiale direttamente nell'infrastruttura di rete. Questa integrazione consentirà alla rete di autoapprendere e autogestirsi, migliorando la propria autonomia e riducendo i costi operativi.[57]Ciò consentirà probabilmente velocità di trasferimento dati ancora più elevate, facilitando l'uso di strumenti di comunicazione sicuri in tempo reale per le forze dell'ordine, garantendo agli agenti sul campo l'accesso immediato a informazioni cruciali e migliorando l'efficienza e la sicurezza sul campo. Di conseguenza, l'aumento dei volumi di dati richiederà probabilmente una nuova gamma di strumenti e metodi di intelligenza artificiale per analizzarli.

- Droni automatizzati e robotica:Il futuro potrebbe prevedere un utilizzo più diffuso di droni e robot basati sull'intelligenza artificiale per operazioni di ricerca e soccorso, o addirittura per la sicurezza di grandi eventi, fornendo informazioni aeree o assistenza a terra senza mettere a rischio vite umane.

- Chip AI:L'ulteriore sviluppo e l'integrazione dei chip di intelligenza artificiale accelereranno significativamente il progresso e le capacità delle tecnologie di intelligenza artificiale in futuro. I chip di intelligenza artificiale specializzati sono progettati per elaborare in modo efficiente le attività di intelligenza artificiale e apprendimento automatico, offrendo velocità di calcolo più elevate e consumi energetici ridotti rispetto ai processori generici. Ulteriori progressi in questo settore consentiranno un'intelligenza artificiale più complessa e sofisticata.

modelli da addestrare e implementare, migliorando le prestazioni delle applicazioni di intelligenza artificiale nelle forze dell'ordine.

- Edge computing:Avvicinando l'elaborazione e l'archiviazione dei dati al luogo in cui sono necessari, l'edge computing ha il potenziale per rivoluzionare il futuro dell'IA. L'edge computing può abilitare capacità di elaborazione dell'IA più rapide, efficienti e in tempo reale, riducendo la dipendenza dai servizi cloud e dai data center. Ciò può contribuire a ridurre al minimo la latenza, l'utilizzo della larghezza di banda e il rischio di violazioni della privacy dei dati. Per le applicazioni di IA, ciò significa la capacità di elaborare e analizzare i dati sul dispositivo in tempo reale, un aspetto cruciale per le applicazioni che richiedono un processo decisionale immediato, come veicoli autonomi, dispositivi IoT e tecnologie per le smart city. Ciò potrebbe avere un impatto significativo sulle forze dell'ordine, consentendo un'integrazione più fluida dell'IA a vari livelli operativi. L'edge computing potrebbe facilitare casi d'uso che spaziano dal riconoscimento facciale e dai centri di comando mobili ai dispositivi indossabili intelligenti, ai sensori migliorati e all'implementazione avanzata di sistemi senza pilota, come i droni.

> Con l'emergere di questi progressi tecnologici, è fondamentale che le forze dell'ordine restino al passo con i tempi, si adattino e integrino questi strumenti in modo responsabile. Sebbene il potenziale sia significativo, garantire che queste tecnologie siano impiegate in modo etico e in linea con i principi di giustizia ed equità sarà fondamentale. L'equilibrio tra lo sfruttamento della tecnologia e la tutela dei diritti determinerà la traiettoria del ruolo dell'IA nel futuro delle attività di polizia.

Costruire la fiducia e l'accettazione del pubblico

La fiducia e l'accettazione da parte del pubblico sono fondamentali per un'integrazione efficace delle tecnologie di intelligenza artificiale nelle forze dell'ordine. Senza la fiducia collettiva del pubblico, anche i progressi più innovativi rischiano di incontrare resistenza, ostacolandone potenzialmente l'efficace utilizzo. Investire nel coinvolgimento della comunità, nella formazione e nei meccanismi di feedback può aumentare significativamente la fiducia e la cooperazione del pubblico nelle tecnologie di intelligenza artificiale, portando infine a una comunità più informata e solidale. Ad esempio:

- Coinvolgimento della comunità:Interagire regolarmente con la comunità può fornire spunti preziosi sulle loro preoccupazioni e aspettative e promuovere la comprensione reciproca. Organizzare forum pubblici, workshop o dibattiti aperti può aiutare a demistificare l'IA, affrontare idee sbagliate e identificare in modo collaborativo le aree di miglioramento. Questo dialogo è inoltre essenziale per gestire efficacemente i compromessi tra privacy e sicurezza, soprattutto nel contesto delle applicazioni di IA ad alto rischio nelle forze dell'ordine.
- Istruzione e consapevolezza:Investire in campagne di sensibilizzazione pubblica sui vantaggi e i limiti dell'IA può ridurre la paura e lo scetticismo nella società. Quando le persone sono informate sugli impatti positivi, come la riduzione della criminalità,

velocità o tempi di risposta più rapidi, è più probabile che adottino questa tecnologia.

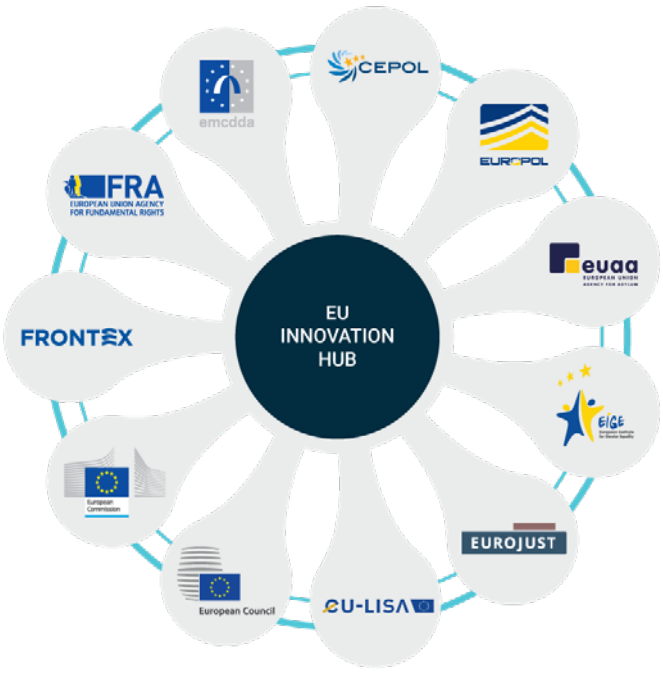
- Meccanismi di feedback:L'istituzione di canali in cui il pubblico possa esprimere le proprie preoccupazioni, fornire feedback o persino segnalare potenziali abusi dell'intelligenza artificiale potrebbe infondere un senso di partecipazione e di comproprietà nell'evoluzione della tecnologia.

Costruire la fiducia del pubblico è un processo continuo, che richiede sforzi costanti e un dialogo aperto. Mentre l'intelligenza artificiale continua a plasmare il futuro delle forze dell'ordine, dare priorità alla fiducia e all'accettazione del pubblico non solo convaliderà il progresso tecnologico, ma garantirà anche che la società progredisca in modo coeso, con la tecnologia che funge da facilitatore piuttosto che da divisore.

Rafforzare la collaborazione e la condivisione delle conoscenze all'interno delle LEA

In questo ecosistema dinamico, la collaborazione e la condivisione delle conoscenze sono di fondamentale importanza. Promuovendo un ambiente di intelligenza collettiva e dialogo aperto, le forze dell'ordine possono garantire che il potenziale dell'IA venga riconosciuto in modo coerente con il bene collettivo. Ciò include:

- Collaborazioni interagenzia:Le agenzie di diverse regioni e paesi possono collaborare per mettere in comune risorse, condividere conoscenze e sviluppare congiuntamente strumenti di intelligenza artificiale su misura per diversi scenari. Tali iniziative collaborative possono semplificare gli sforzi, ridurre le ridondanze e portare a soluzioni più universalmente adattabili. Un'iniziativa di questo tipo è il già citato EU Innovation Hub for Internal Security, una rete collaborativa di laboratori di innovazione che lavora per fornire gli ultimi aggiornamenti sull'innovazione e soluzioni efficaci.



soluzioni per supportare il lavoro degli attori della sicurezza interna nell'UE e nei suoi Stati membri, tra cui gli operatori della giustizia, della sicurezza delle frontiere, dell'immigrazione e dell'asilo e delle forze dell'ordine.

- Partnership con il mondo accademico e l'industria:Grazie alle alleanze con università e aziende tecnologiche, le forze dell'ordine possono attingere a ricerche, metodologie e strumenti all'avanguardia. Questo spirito collaborativo può accelerare lo sviluppo e il perfezionamento dei sistemi di intelligenza artificiale, garantendo che rimangano all'avanguardia dell'innovazione.

- Intelligenza artificiale open source:Promuovere progetti di intelligenza artificiale open source può facilitare l'accesso a strumenti avanzati, consentendo anche alle forze dell'ordine più piccole di sfruttare la potenza dell'intelligenza artificiale. Tali iniziative possono anche promuovere un approccio allo sviluppo basato sulla comunità, migliorando la qualità e l'applicabilità degli strumenti.

- Alfabetizzazione AI:Migliorare la conoscenza dell'IA tra il personale delle forze dell'ordine, in linea con la legge europea sull'IA, è fondamentale per promuovere un approccio informato ed etico all'integrazione dell'IA nelle attività di polizia. Il personale delle forze dell'ordine dovrebbe acquisire consapevolezza delle dimensioni operative, etiche e legali delle tecnologie di IA, assicurandosi di poter implementare efficacemente gli strumenti di IA, affrontando al contempo le problematiche relative a pregiudizi, privacy e responsabilità. Allo stesso modo, è fondamentale coinvolgere il pubblico in dibattiti trasparenti sul ruolo dell'IA nelle forze dell'ordine, chiarendone i vantaggi, i limiti e la supervisione normativa, come previsto dal nuovo regolamento. Promuovendo una profonda comprensione delle capacità dell'IA e dei quadri giuridici che ne disciplinano l'utilizzo, questo sforzo mira a creare fiducia, migliorare la collaborazione tra le forze dell'ordine e le comunità e garantire che l'implementazione dell'IA sia in linea con i valori sociali e i diritti fondamentali.

- Depositi di conoscenza centralizzati:La creazione di database o piattaforme centralizzate in cui le agenzie possano condividere casi di studio, articoli di ricerca, kit di strumenti e buone pratiche può rappresentare una risorsa inestimabile. Tali archivi possono garantire che la conoscenza non venga solo creata, ma anche resa accessibile a coloro che ne hanno bisogno. Un esempio significativo è la Piattaforma per Esperti (EPE) di Europol.[15]e il Tool Repository (ETR) di Europol[16] Quest'ultimo è stato creato dall'Europol Innovation Lab come piattaforma partecipativa per le forze dell'ordine di tutta Europa, per condividere strumenti innovativi basati su tecnologie all'avanguardia. Il primo è un ambiente sicuro per specialisti in diversi settori delle forze dell'ordine, tra cui l'intelligenza artificiale, che consente loro di condividere, all'interno delle rispettive comunità, conoscenze, buone pratiche e dati non personali sui reati. Attualmente, conta oltre 18.000 membri.

15 Per saperne di più sull'EPE, clicca qui: https://www.europol.europa.eu/operations-services-andinnovation/services-support/information-exchange/europol-platform-for-experts

16 ETR è una piattaforma online sicura ed esclusiva per le forze dell'ordine, che consente la condivisione di software non commerciale e gratuito, sviluppato da forze dell'ordine e da organizzazioni di ricerca e tecnologia. ETR è stata progettata per evitare la duplicazione degli sforzi tra le forze dell'ordine. Consente a tutte le forze di polizia in Europa di beneficiare di strumenti innovativi e di diventare più efficienti nel loro lavoro, migliorando così la protezione dei cittadini dell'UE. Gli strumenti di intelligenza artificiale disponibili tramite ETR hanno già supportato diverse operazioni in tutta Europa, che hanno portato all'arresto di criminali organizzati e al salvataggio di vittime della tratta di esseri umani.

provenienti da oltre 100 paesi che interagiscono e collaborano tra loro in comunità virtuali.

F Coinvolgimento della società civile:Collaborare con la società civile e le organizzazioni comunitarie può fornire prospettive uniche sulle implicazioni etiche e sociali dell'intelligenza artificiale nelle attività di polizia.

Conclusione

L'integrazione dell'IA nelle forze dell'ordine, in particolare all'interno dell'Unione Europea, rappresenta un cambiamento di paradigma con profonde implicazioni sia per l'efficienza operativa che per le considerazioni etiche. Questo rapporto ha valutato le molteplici applicazioni dell'IA nelle attività di polizia, che spaziano dall'analisi dei dati e dalla polizia predittiva all'informatica forense, alla visione artificiale e alla biometria. Il rapporto ha evidenziato il potenziale trasformativo che queste tecnologie possiedono per migliorare la sicurezza pubblica e l'efficacia operativa.

Tuttavia, questa evoluzione tecnologica non è priva di sfide. Le dimensioni etiche e sociali, tra cui le preoccupazioni relative a distorsioni dei dati, privacy, responsabilità e diritti umani, sono cruciali. La posizione proattiva dell'Unione Europea attraverso l'elaborazione dell'Artificial Intelligence Act sottolinea l'impegno a bilanciare l'innovazione con considerazioni etiche, con l'obiettivo di promuovere un ambiente in cui i benefici dell'IA nelle forze dell'ordine possano essere sfruttati in modo responsabile.

Il rapporto ha sottolineato l'importanza di contrastare pregiudizi e discriminazioni, tutelare la privacy e la protezione dei dati e garantire la responsabilità e il rispetto delle normative. Ha delineato strategie come la promozione di sandbox normativi, che consentano l'esplorazione e lo sviluppo sicuri delle tecnologie di intelligenza artificiale all'interno di un quadro strutturato che rispetti i valori e i diritti fondamentali dell'UE.

> Guardando al futuro, l'evoluzione dell'intelligenza artificiale nelle forze dell'ordine è destinata a significativi progressi tecnologici, tra cui l'informatica quantistica e la connettività 6G, che promettono di migliorare ulteriormente le capacità delle forze dell'ordine. Tuttavia, il successo dell'integrazione di queste tecnologie dipende dalla creazione di fiducia e accettazione da parte del pubblico, dall'enfasi sulla trasparenza e dal rafforzamento della collaborazione e della condivisione delle conoscenze all'interno della comunità delle forze dell'ordine.

In conclusione, il rapporto ha auspicato un approccio equilibrato all'IA nelle forze dell'ordine, in cui i vantaggi dei progressi tecnologici siano sfruttati per migliorare la sicurezza pubblica e l'efficienza operativa, affrontando al contempo le sfide etiche, legali e sociali. Il quadro normativo dell'UE, incluso l'Artificial Intelligence Act, fornisce una solida base per questo impegno, garantendo che l'integrazione dell'IA nelle forze dell'ordine sia in linea con i valori fondamentali e i diritti fondamentali dell'UE. Il futuro delle attività di polizia basate sull'IA risiede, pertanto, nell'armoniosa integrazione tra innovazione e regolamentazione, guidata dai principi di equità, responsabilità e trasparenza.

RESPONSABILITÀ: La responsabilità e la spiegabilità delle azioni e delle decisioni prese dai sistemi di Intelligenza Artificiale. Nel contesto delle attività di polizia basate sull'IA, ciò implica garantire che l'uso dell'IA nelle forze dell'ordine rispetti gli standard etici e le normative legali.

GOVERNANCE DELL'IA: Il quadro e l'insieme di regole e regolamenti che guidano lo sviluppo, l'implementazione e l'utilizzo dei sistemi di intelligenza artificiale. Include considerazioni etiche, meccanismi di responsabilità e conformità agli standard legali.

UFFICIO IA: La funzione della Commissione europea è quella di contribuire all'implementazione, al monitoraggio e alla supervisione dei sistemi di intelligenza artificiale, dei modelli di intelligenza artificiale di uso generale e della governance dell'intelligenza artificiale.

SISTEMA DI IA: Un sistema di intelligenza artificiale è un sistema basato su macchine progettato per funzionare con diversi livelli di autonomia e che può mostrare adattabilità dopo l'implementazione e che, per obiettivi espliciti o impliciti, deduce, dall'input che riceve, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali (art. 3 della legge UE sull'intelligenza artificiale).

ALGORITMO: Un insieme di istruzioni sequenziali applicate a input specifici per raggiungere un obiettivo predefinito, che spazia dall'output di una funzione matematica di base a compiti più complessi.

INTELLIGENZA ARTIFICIALE (IA): Sviluppo di sistemi informatici in grado di svolgere compiti che tipicamente richiedono l'intelligenza umana. Questi compiti includono apprendimento, ragionamento, risoluzione di problemi, percezione e comprensione del linguaggio.

PREGIUDIZIO: Preferenze o pregiudizi sistematici e ingiusti nei dati o negli algoritmi che possono portare a risultati discriminatori. I pregiudizi possono derivare dai dati utilizzati per addestrare i modelli di intelligenza artificiale o dalla progettazione degli algoritmi stessi.

DATI BIOMETRICI: Dati personali risultanti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali l'immagine facciale o i dati dattiloscopici (art. 3 della legge UE sull'intelligenza artificiale).

CHATBOT: Software progettato per imitare la conversazione con gli esseri umani.

CLASSIFICAZIONE: Un tipo di attività di apprendimento automatico in cui l'algoritmo assegna categorie o etichette predefinite ai dati di input.

CLOUD COMPUTING: Fornitura di servizi informatici, quali archiviazione, potenza di calcolo e applicazioni software, tramite Internet.

VALUTAZIONE DELLA CONFORMITÀ: Il processo di dimostrazione del rispetto dei requisiti stabiliti dalla legge UE sull'intelligenza artificiale in relazione a un sistema di intelligenza artificiale ad alto rischio.

VISIONE COMPUTERIZZATA: Un campo dell'intelligenza artificiale che consente alle macchine di interpretare e prendere decisioni sulla base di dati visivi. La visione artificiale viene utilizzata per l'analisi di immagini e video.

DEEPFAKE: Immagini, contenuti audio o video generati o manipolati dall'IA che assomigliano a persone, oggetti, luoghi o altre entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri a una persona (art. 3 della legge UE sull'IA).

APPRENDIMENTO PROFONDO: Il deep learning è un sottoinsieme dell'apprendimento automatico e dell'intelligenza artificiale che imita l'acquisizione della conoscenza umana per consentire ai modelli di eseguire attività complesse come il riconoscimento di pattern in vari tipi di dati. Crittografia Il processo di conversione delle informazioni in un codice per impedire l'accesso non autorizzato, particolarmente importante per la protezione dei dati nelle applicazioni di intelligenza artificiale.

SPIEGABILITÀ: Capacità di comprendere e interpretare le decisioni e le azioni dei sistemi di intelligenza artificiale, in particolare nei modelli complessi come le reti neurali.

EQUITÀ: Garantire che i sistemi di intelligenza artificiale trattino tutti gli individui e i gruppi in modo equo, senza introdurre pregiudizi o discriminazioni.

MODELLO DI FONDAZIONE: Un modello pre-addestrato che funge da punto di partenza per varie attività a valle nell'apprendimento automatico.

IA PER SCOPI GENERALI (GPAI): Un sistema di intelligenza artificiale basato su un modello di intelligenza artificiale di uso generale, in grado di soddisfare una varietà di scopi, sia per l'uso diretto che per l'integrazione in altri sistemi di intelligenza artificiale (art. 3 dell'AIA).

IA GENERATIVA: Sistemi di intelligenza artificiale in grado di generare nuovi contenuti, come immagini, testo o musica, spesso utilizzando modelli di intelligenza artificiale generici.

IA AD ALTO RISCHIO:applicazioni di intelligenza artificiale con un potenziale impatto significativo sui diritti e sulla sicurezza degli individui, che richiedono un controllo normativo più rigoroso.

MODELLO LINGUISTICO AMPIO: Un tipo di modello di intelligenza artificiale, come GPT-4, che viene addestrato su grandi quantità di dati di testo ed è in grado di generare un linguaggio simile a quello umano.

APPRENDIMENTO AUTOMATICO: Un sottoinsieme dell'intelligenza artificiale che si concentra sullo sviluppo di algoritmi che consentono ai computer di apprendere e fare previsioni o decisioni basate sui dati.

AUTORITÀ DI VIGILANZA DEL MERCATO: Un organismo di regolamentazione responsabile del monitoraggio e della garanzia del rispetto delle normative di mercato, comprese quelle relative alle applicazioni di intelligenza artificiale.

ELABORAZIONE DEL LINGUAGGIO NATURALE: Un sottoinsieme dell'intelligenza artificiale che si concentra sul modo in cui i computer e i linguaggi umani interagiscono, consentendo alle macchine di comprendere, decifrare e generare il linguaggio umano.

RETI NEURALI: Un insieme di algoritmi, vagamente modellati sul cervello umano, progettati per riconoscere schemi. Le reti neurali sono una componente chiave del deep learning.

PROFILAZIONE: Il processo di analisi e classificazione degli individui in base alle loro caratteristiche, comportamenti o preferenze.

CALCOLO QUANTISTICO:L'informatica quantistica è una tecnologia in rapida ascesa che sfrutta le leggi della meccanica quantistica per risolvere problemi troppo complessi per i computer classici.

SANDBOX REGOLAMENTARE: Un quadro concreto e controllato, istituito da un'autorità competente, che offre ai fornitori o ai potenziali fornitori di sistemi di IA la possibilità di sviluppare, addestrare, convalidare e testare, ove opportuno in condizioni reali, un sistema di IA innovativo, secondo un piano sandbox, per un periodo di tempo limitato sotto la supervisione normativa (art. 3 della legge UE sull'IA).

IDENTIFICAZIONE BIOMETRICA REMOTA (RBI):sistema Un sistema di intelligenza artificiale allo scopo di identificare persone fisiche, senza il loro coinvolgimento attivo, in genere a distanza, mediante il confronto dei dati biometrici di una persona con i dati biometrici contenuti in una banca dati di riferimento (art. 3 della legge UE sull'intelligenza artificiale).

ROBOTICA: Campo interdisciplinare che unisce informatica e ingegneria per sviluppare, costruire e far funzionare robot.

PUNTEGGIO SOCIALE:L'uso dell'intelligenza artificiale e dell'analisi dei dati per valutare e assegnare punteggi agli individui in base al loro comportamento, alle loro attività o alle loro interazioni sociali.

TRASPARENZA:L'apertura e la chiarezza nel funzionamento e nel processo decisionale dei sistemi di intelligenza artificiale, garantendo che gli utenti e le parti interessate possano comprendere il comportamento del sistema.

Note finali

1 Europol, 2021, Valutazione della minaccia rappresentata dalla criminalità organizzata e seria (SOCTA) 2021, accessibile all'indirizzo https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021

2 Comunicato stampa del Parlamento europeo, giugno 2023, Gli eurodeputati pronti a negoziare le prime regole per un'intelligenza artificiale sicura e trasparente, accessibile all'indirizzo https://www.europarl.europa.eu/news/en/pressroom/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai

3 Parlamento europeo, 2023, Studio a supporto della concettualizzazione tecnica, giuridica e finanziaria di uno spazio europeo dei dati di sicurezza per l'innovazione, accessibile all'indirizzo https://home-affairs.ec.europa.eu/system/files/2023-02/Data%20spaces%20study_0.pdf

4 YJ Tan, S. Ramachandran, MA Jabar, et al., 2022, Rilevamento delle frodi finanziarie basato sull'apprendimento automatico: una revisione sistematica della letteratura, Applied Sciences, vol. 12, n. 19, pp. 9637, accessibile all'indirizzo https://doi.org/10.3390/app12199637

5 K. Gülen, 2023, L'universo parallelo dell'informatica: come si svolgono simultaneamente più attività?, Dataconomy, accessibile all'indirizzo https://dataconomy.com/2023/04/18/what-is-parallel-processing/

6 Comunicato stampa di Europol, 2020, Lo smantellamento di una rete crittografata provoca onde d'urto nei gruppi della criminalità organizzata in tutta Europa, accessibile all'indirizzo https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwavesthrough-organised-crime-groups-across-europe

7 Comunicato stampa di Europol, 2023, Lo smantellamento delle comunicazioni criminali crittografate di EncroChat porta a oltre 6.500 arresti e quasi 900 milioni di euro sequestrati, accessibile all'indirizzo https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochat-communications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized

8 A. Babuta, 2017, Big Data e polizia: una valutazione dei requisiti, delle aspettative e delle priorità delle forze dell'ordine, RUSI, accessibile all'indirizzo https://static.rusi.org/201709_rusi_big_data_and_policing_babuta_web.pdf

9 Ivi.

10 Ivi.

11 W. Hardyns, A. Rummens, 2018, La polizia predittiva come nuovo strumento per le forze dell'ordine? Sviluppi e sfide recenti, Eur J Crim Policy Res 24 (2018), pp. 201–218, accessibile all'indirizzo https://doi.org/10.1007/s10610-017-9361-2

12 P. Walter et al., 2013, Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations, RAND, accessibile all'indirizzo https://www.rand.org/pubs/research_reports/RR233.html

13 W.Hardynn e A. Rummens, 2017, La polizia predittiva come nuovo strumento per le forze dell'ordine? Sviluppi e sfide recenti, Eur J Crim Policy Res 24 (2018), pp. 201-2018, accessibile all'indirizzo https://doi.org/10.1007/s10610-017-9361-2

14 EUPCN, 2022, Intelligenza artificiale e polizia predittiva: rischi e sfide, accessibile all'indirizzo https://eucpn.org/sites/default/files/document/files/PP%20%282%29.pdf

15 Polizia olandese, 2021, Crime Anticipation System, accessibile all'indirizzo https://www.politie.nl/wet-open-overheid/woo-verzoeken/landelijke-eenheid/woo-verzoeken-per-jaar/2021/crime-anticipation-system.html

16 S. Oosterloo e G. van Schie, 2022, La politica e i pregiudizi del "sistema di anticipazione del crimine" della polizia olandese, accessibile all'indirizzo https://ceur-ws.org/Vol-2103/paper_6.pdf

17 Europol, 2021, Valutazione della minaccia della criminalità organizzata su Internet (IOCTA) 2021, accessibile all'indirizzo https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021

18 Europol, 2022, Rapporto sulla situazione e le tendenze del terrorismo nell'UE (TE-SAT) 2022, accessibile all'indirizzo https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2022-te-sat

19 Medium, 2023, Utilizzo di OSINT per migliorare la tua strategia di intelligence competitiva, accessibile su https://goldenowl.medium.com/using-osint-to-improve-your-competitive-intelligence-strategy-eeb6114f9c71

20 Cambridge Consultants, 2019, Uso dell'intelligenza artificiale nella moderazione dei contenuti online, accessibile all'indirizzo https://www.ofcom.org.uk/__data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf

21 Commissione Europea, 2023, L'impatto del Digital Services Act sulle piattaforme digitali

moduli, accessibili all'indirizzo https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms

22 Meta, 2023, Nuove funzionalità e misure aggiuntive di trasparenza con l'entrata in vigore del Digital Services Act, accessibile all'indirizzo https://about.fb.com/news/2023/08/new-features-and-additional-transparency-measures-as-the-digital-services-act-comes-into-effect/

23 DeepLearning.AI, 2023, Elaborazione del linguaggio naturale, accessibile all'indirizzo https://www.deeplearning.ai/resources/natural-language-processing/

24 P. Sarzaeim et al., 2023, Una revisione sistematica dell'utilizzo dell'apprendimento automatico e dell'elaborazione del linguaggio naturale nella polizia intelligente, Computers 2023; 12(12):255, accessibile all'indirizzo https://doi.org/10.3390/computers12120255

25 A. Dixon e D. Birks, 2021, Migliorare le attività di polizia con l'elaborazione del linguaggio naturale, negli Atti del 1° workshop sulla PNL per un impatto positivo, pp. 115–124, accessibile all'indirizzo https://aclanthology.org/2021.nlp4posimpact-1.13.pdf

26 Ivi.

27 R. Abhijit, 2020, Understanding Automatic Text Summarization-1: Extractive Methods, Towards Data Science, accessibile all'indirizzo https://towardsdatascience.com/understanding-automatic-text-summarization-1-extractive-methods-8eb512b21ecc

28 Progetto Roxanne, tecnologie NLP contro la criminalità online, accessibile su https://www.roxanne-euproject.org/news/blog/nlp-technologies-against-online-crime

29 JM James et al., 2022, Digital Forensics AI: valutazione, standardizzazione e ottimizzazione delle indagini forensi digitali, SpringerLink, accessibile all'indirizzo https://link.springer.com/article/10.1007/s13218-022-00763-9

30 H. Ravichandran, 2023, Come l'intelligenza artificiale sta rivoluzionando e trasformando il panorama della sicurezza informatica, Forbes, accessibile all'indirizzo https://www.forbes.com/sites/forbestechcouncil/2023/03/15/how-ai-is-disrupting-and-transforming-the-cybersecurity-landscape/?sh=5aab864c4683

31 JS Hollywood et al., 2018, Utilizzo dell'analisi video e della fusione dei sensori nelle forze dell'ordine, RAND, accessibile all'indirizzo https://www.rand.org/pubs/research_reports/RR2619.html

32 Ivi.

33 A. Jain, K. Nandakumar e A. Ross, 2016, 50 anni di ricerca biometrica: risultati, sfide e opportunità, Pattern Recognition Letters, 79, doi: 10.1016/j.patrec.2015.12.013.

34 P. Grother et al., 2024, Valutazione della tecnologia di riconoscimento facciale (FRTE). Parte 2: Identificazione, NIST, disponibile all'indirizzo https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf

35 P. Grother et al., 2019, Face Recognition Vendor Test (FRVT) Parte 3: Effetti demografici, NIST, accessibile all'indirizzo https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf

36 JL Mnookin, 2003, Impronte digitali: non uno standard d'oro, Numeri, XX (1) Autunno, 2003, accessibile su https://issues.org/mnookin-fingerprints-evidence/

37 Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA), 2020, La trasformazione digitale della sicurezza interna nell'UE, l'intelligenza artificiale e il ruolo di eu-LISA, accessibile all'indirizzo https://www.eulisa.europa.eu/Newsroom/News/Pages/The-digital-transformation-of-internal-security-in-the-EU-AI-and-the-role-of-eu-LISA.aspx

38 Y. Rawat, et al., 2023, Il ruolo dell'intelligenza artificiale nella biometria, 2a conferenza internazionale su Edge Computing e applicazioni, pp. 622-626, doi: 10.1109/ICE-CAA58104.2023.10212224.

39 A. Mitchell, 2013, Distinguere l'amico dal nemico: diritto e politica nell'era della biometria sui campi di battaglia, Canadian Yearbook of international Law/Annuaire canadien de droit international, 50, pp. 289-330, doi: 10.1017/S0069005800010869.

40 J. Thorpe, 2023, L'FBI tra i principali utilizzatori dell'innovativa tecnologia di riconoscimento dell'iride per le forze dell'ordine, International Security Journal, accessibile all'indirizzo https://internationalsecurityjournal.com/fbi-iris-recognition-law-enforcement/

41 J. Lunter, 2023, Dati sintetici: una vera via per eliminare i pregiudizi nella biometria, Biometric Technology Today 2023(1), accessibile all'indirizzo https://www.magonlinelibrary.com/doi/

completo/10.12968/S0969-4765%2823%2970001-5

42 A. Gomez-Alanis, JA Gonzalez-Lopez e AM Peinado, 2022, GANBA: Generative Adversarial Network for Biometric Anti-Spoofing, Applied Sciences, 12(3):1454, accessibile all'indirizzo https://doi.org/10.3390/app12031454

43 Z.Zhang et al.,2023, Una rete di stima della profondità basata su GAN migliorata per l'anti-spoofing facciale, ICCAI '23: Atti della 9a conferenza internazionale del 2023 su informatica e intelligenza artificiale, marzo 2023, pp. 323–328, accessibile all'indirizzo https://doi.org/10.1145/3594315.3594661

44 Europol, 2023, ChatGPT - l'impatto dei modelli linguistici di grandi dimensioni sulle forze dell'ordine, un rapporto flash di Tech Watch dell'Europol Innovation Lab, accessibile all'indirizzo https://www.europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-languagemodels-law-enforcement

45 P. Tomczak, 2018, Machine Learning e il valore dei dati storici, accessibile all'indirizzo https://kx.com/blog/machine-learning-and-the-value-of-historical-data/

46 C. Veal, M. Raper e P. Waters, 2023, I pericoli dei cicli di feedback nell'apprendimento automatico: polizia predittiva, Gilbert +Tobin, accessibile all'indirizzo https://www.lexology.com/library/detail.aspx?g=c8fff116-2112-48dd-841c-f9d1688d722b

47 N. Shahbazi, Y. Lin, A. Asudeh e HV Jagadish, 2023, Distorsione di rappresentazione nei dati: un'indagine sulle tecniche di identificazione e risoluzione, ACM Computing Surveys (55)13, accessibile all'indirizzo https://doi.org/10.1145/3588433

48 Agenzia dell'UE per i diritti fondamentali, 2022, Bias negli algoritmi - Intelligenza artificiale e discriminazione, doi:10.2811/25847

49 J. Burrell, 2016, Come "pensa" la macchina: comprendere l'opacità negli algoritmi di apprendimento automatico, Big Data & Society, 3(1), accessibile all'indirizzo https://doi.org/10.1177/2053951715622512

50 S. Ali et al., 2023, Intelligenza artificiale spiegabile (XAI): cosa sappiamo e cosa resta per raggiungere un'intelligenza artificiale affidabile, Information Fusion (99)2023, accessibile all'indirizzo https://doi.org/10.1016/j.inffus.2023.101805

51 B. Akhgar, et al., 2022, Principi di responsabilità per l'intelligenza artificiale (AP4AI) nel dominio della sicurezza interna AP4AI Framework Blueprint, accessibile all'indirizzo https://www.ap4ai.eu/sites/default/files/2022-03/AP4AI_Framework_Blueprint_22Feb2022.pdf

52 Commissione europea, 2019, Linee guida etiche per un'intelligenza artificiale affidabile, accessibili all'indirizzo https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

53 Commissione europea, 2021, Proposta di regolamento che stabilisce norme armonizzate sull'intelligenza artificiale, accessibile all'indirizzo https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence

54 Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce norme armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Legge sull'intelligenza artificiale)

55 L. Edwards, 2022, The EU AI Act: a summary of its meaning and scope, Ada Lovelace Institute, accessibile all'indirizzo https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf

56 Europol, 2023, La seconda rivoluzione quantistica: l'impatto del calcolo quantistico e delle tecnologie quantistiche sulle forze dell'ordine, accessibile all'indirizzo https://www.europol.europa.eu/ publication-events/main-reports/second-quantum-revolution-impact-of-quantum-computing-and-quantum-technologies-law-enforcement#downloads

57 MIT Technology Review, 2023, Le reti 6G basate sull'intelligenza artificiale rimodelleranno le interazioni digitali, accessibile all'indirizzo https://www.technologyreview.com/2023/10/26/1082028/ai-powered-6g-networks-will-reshape-digital-interactions/

Informazioni sull'Europol Innovation Lab

La tecnologia ha un impatto significativo sulla natura della criminalità. I criminali integrano rapidamente le nuove tecnologie nel loro modus operandi o costruiscono modelli di business completamente nuovi attorno a esse. Allo stesso tempo, le tecnologie emergenti creano opportunità per le forze dell'ordine di contrastare queste nuove minacce criminali. Grazie all'innovazione tecnologica, le autorità di contrasto possono ora accedere a un numero maggiore di strumenti idonei a combattere la criminalità. Nell'esplorazione di questi nuovi strumenti, il rispetto dei diritti fondamentali deve rimanere una considerazione fondamentale.

Nell'ottobre 2019, i ministri del Consiglio Giustizia e Affari interni hanno chiesto la creazione di un laboratorio di innovazione all'interno di Europol, che avrebbe sviluppato una capacità centralizzata di previsione strategica sulle tecnologie dirompenti per informare le strategie di polizia dell'UE.

I metodi di previsione strategica e di scenario offrono un modo per comprendere e prepararsi al potenziale impatto delle nuove tecnologie sulle forze dell'ordine. La funzione di Osservatorio dell'Europol Innovation Lab monitora gli sviluppi tecnologici rilevanti per le forze dell'ordine e segnala rischi, minacce e opportunità di queste tecnologie emergenti. Ad oggi, l'Europol Innovation Lab ha organizzato tre attività di previsione strategica con le forze dell'ordine degli Stati membri dell'UE e altri esperti.

www.europol.europa.eu