DICEMBRE 2024

PROGETTO SICUREZZA

PERIODICO UFFICIALE OPERATORI DELLA POLIZIA DI STATO

“Quale modello di sicurezza tra intelligenza artificiale e nuove professionalità degli operatori per le sfide del futuro”

INFO

ANNO XXXVI N2/2024
Direttore Responsabile
Felice Romano

Vice Direttore
Alessandro Figus

Comitato di redazione
Silvano Filippi
Vincenzo Annunziata
Fabio Lauri
Pietro Francesco Caracciolo
Saturno Carbone
Innocente Carbone
Alessandro Pisaniello

Staff:
Andrea Pisaniello
Stefano Caponi

Proprietà testata:
SIULP
Registrazione
Tribunale di Roma
NR. 541988 e NR. 68/2016
Iscrizione al ROC n.1123

Direzione e redazione:
Via Vicenza 26, 00185
Roma
Tel. 06.4455213
Fax: 06.4469841
nazionale@siulp.it
www.siulp.it

Stampa a cura di:
Ciesse Stampa S.r.l.
Sede legale, amministrativa e produttiva
Via Cesare Dal Fabbro, 15 -00148 Roma
Codice Fiscale 15410541005
Partita IVA 15410541005
T.06 39729887

tutte le foto utilizzate nel numero sono foto di repertorio

Intelligenza artificiale, educazione digitale e tutela della privacy

La diffusione e il crescente impiego degli algoritmi dell'intelligenza artificiale in tutti i settori della società pongono interrogativi che riguardano l'impatto e i possibili effetti di un'evoluzione digitale che sta imponendo sensibili trasformazioni che interessano la produzione di beni e servizi, il mercato del lavoro, la scuola, la vita dei cittadini e il loro rapporto con la Pubblica Amministrazione e le condizioni di accesso a numerosi servizi essenziali.

La prima esigenza è legata alla necessità di garantire una efficace alfabetizzazione digitale della popolazione.

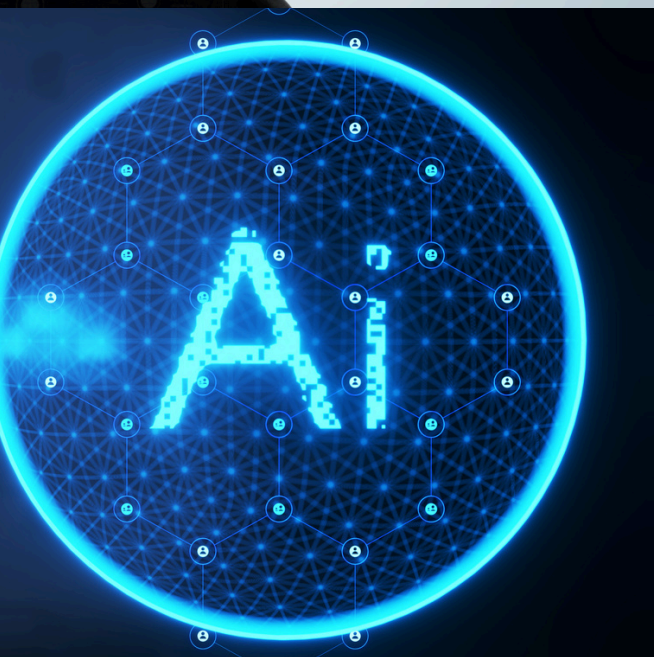
Per garantire una maggiore efficienza economica e sociale, servizi pubblici (sanità, trasporti, PA) efficaci e uno sviluppo sostenibile servono adeguate competenze e specialisti per la realizzazione delle infrastrutture digitali. Secondo le indicazioni della Commissione europea il raggiungimento di un'accettabile soglia delle competenze digitali comporta l'alfabetizzazione di base di almeno l'80 per cento della popolazione e la disponibilità di almeno 20 milioni di specialisti.

Un Rapporto della Commissione Europea che contiene un'analisi della situazione nei diversi paesi, evidenzia che "solo il 45,8% delle persone in Italia ha almeno competenze digitali di base e la quota di specialisti ICT nell'occupazione rimane limitata, mentre la domanda da parte delle imprese di queste competenze è in aumento".
In un mondo in cui la tecnologia è diventata parte integrante della vita quotidiana, è importante comprendere come funziona la tecnologia ed essere in grado di navigare in un ambiente digitale complesso, in modo consapevole e sicuro.

Si tratta del possesso di abilità e competenze che permettono di comunicare, creare contenuti e ricercare informazioni, con la consapevolezza dei rischi e con la capacità di distinguere ciò che è autorevole e affidabile da tutto il resto.
Con i progressi della digitalizzazione nel mondo del lavoro anche lo svolgimento di attività in ambiti tradizionalmente meno tecnologici richiede capacità basiche di gestione di software e strumenti digitali.

Scuole, università, uffici, negozi, servizi medici e legali utilizzano tecnologie digitali per il loro funzionamento, essere privi delle competenze necessarie può costituire un ostacolo significativo all'inclusione sociale e lavorativa.
Inoltre, l'alfabetizzazione digitale permette alle persone di essere attive e partecipi nella società. Avere accesso alla tecnologia e saperla usare efficacemente significa poter accedere a opportunità di educazione, lavoro, salute e partecipazione civica. In altre parole, la digitalizzazione non è solo una questione di sviluppo tecnologico, ma anche di sviluppo sociale e di governabilità della popolazione del terzo millennio, allo stesso modo, di come nel dopoguerra, lo era la capacità di leggere e far di conto.

Non meno importante è poi l'esigenza di educare le nuove generazioni al corretto utilizzo delle tecnologie evolute che, accanto alle abilità messe a disposizione di chi le utilizza, comportano la necessità di affrancare l'umanità da una dipendenza tecnologica priva di un adeguato bilanciamento e perciò stessa in grado condizionare lo stesso libero arbitrio.
Invero, se da un lato, una serie di applicazioni permettono, attraverso l'identità digitale, di gestire pratiche, ricevere notifiche, lavorare e accedere a informazioni utili direttamente dallo smartphone, dall'altro, se pensiamo ai programmi informatici capaci di interagire con le persone attraverso comandi vocali, è facile rendersi conto di come questi software siano capaci di sostituire figure come avvocati, consulenti del lavoro, promotori finanziari e persino psicologi introducendo i propri utenti in "stanze" ove persino le loro fragilità emotive vengono affidate a un robot che offre risposte preconfezionate e frutto di un addestramento etero finalizzato.



Diventa, inoltre, sempre più difficile distinguere un falso dalla realtà considerando che la possibilità di sostituirsi a una persona usando il suo volto, la sua voce per realizzare un filmato e persino una diretta streaming mettendosi nei panni di chiunque può essere utilizzata da criminali, truffatori e in genere da persone interessate alla manipolazione delle opinioni o alla perpetrazione di condotte illecite come la truffa, la pedofilia, il revenge porn, oltre ai reati informatici previsti dall'articolo 615 bis del codice penale.

L'estrema facilità dell'approccio alle nuove tecnologie deve, dunque, essere accompagnata dalla consapevolezza dei possibili rischi che essa comporta allo scopo di favorirne un uso consapevole e a vantaggio della collettività.
Il primo delicato terreno è quello della tutela dei minori. Sull'età minima per accedere ai social media non si registra una unità di vedute. La garante per l'infanzia e l'adolescenza vorrebbe fissarla a 16 anni, mentre il garante della privacy sostiene la misura dei 14 anni. Ovviamente si tratta di pareri acquisiti dal legislatore attualmente alle prese con l'esame di un disegno di legge di iniziativa parlamentare (atto Senato n. 1136) intitolato "disposizioni per la tutela dei minori nella dimensione digitale".

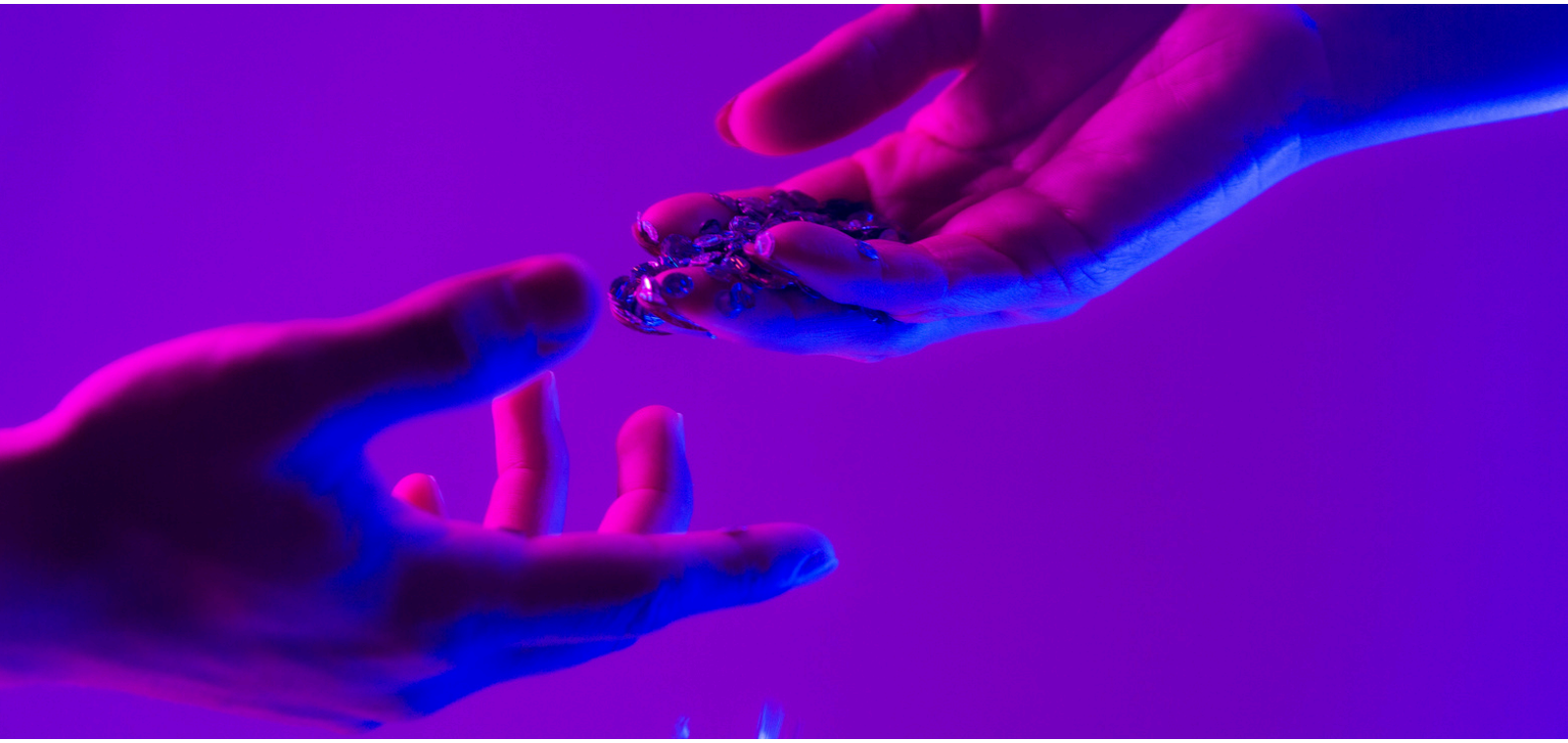
Un problema concerne l'uso dei dispositivi elettronici a scuola che una circolare emanata nel luglio scorso, ha espressamente vietato.
Un ulteriore problema concerne la privacy e l'individuazione del momento in cui i minori possono autonomamente dare il consenso al trattamento dei loro dati da parte dei gestori di piattaforme concludere da soli contratti con i citati fornitori.
In base alla normativa italiana la situazione attuale relativa ai due profili elencati registra l'abilitazione del minore maggiore di 14 anni (articolo 2-quinquies del codice della privacy che ha così abbassato la soglia di 16 anni prevista dal Gdpr, regolamento Ue n. 2016/679), a dare il consenso ai trattamenti connessi ai servizi della società dell'informazione e la capacità di agire contrattualmente al compimento del 18° anno di età, salvo espresse deroghe.

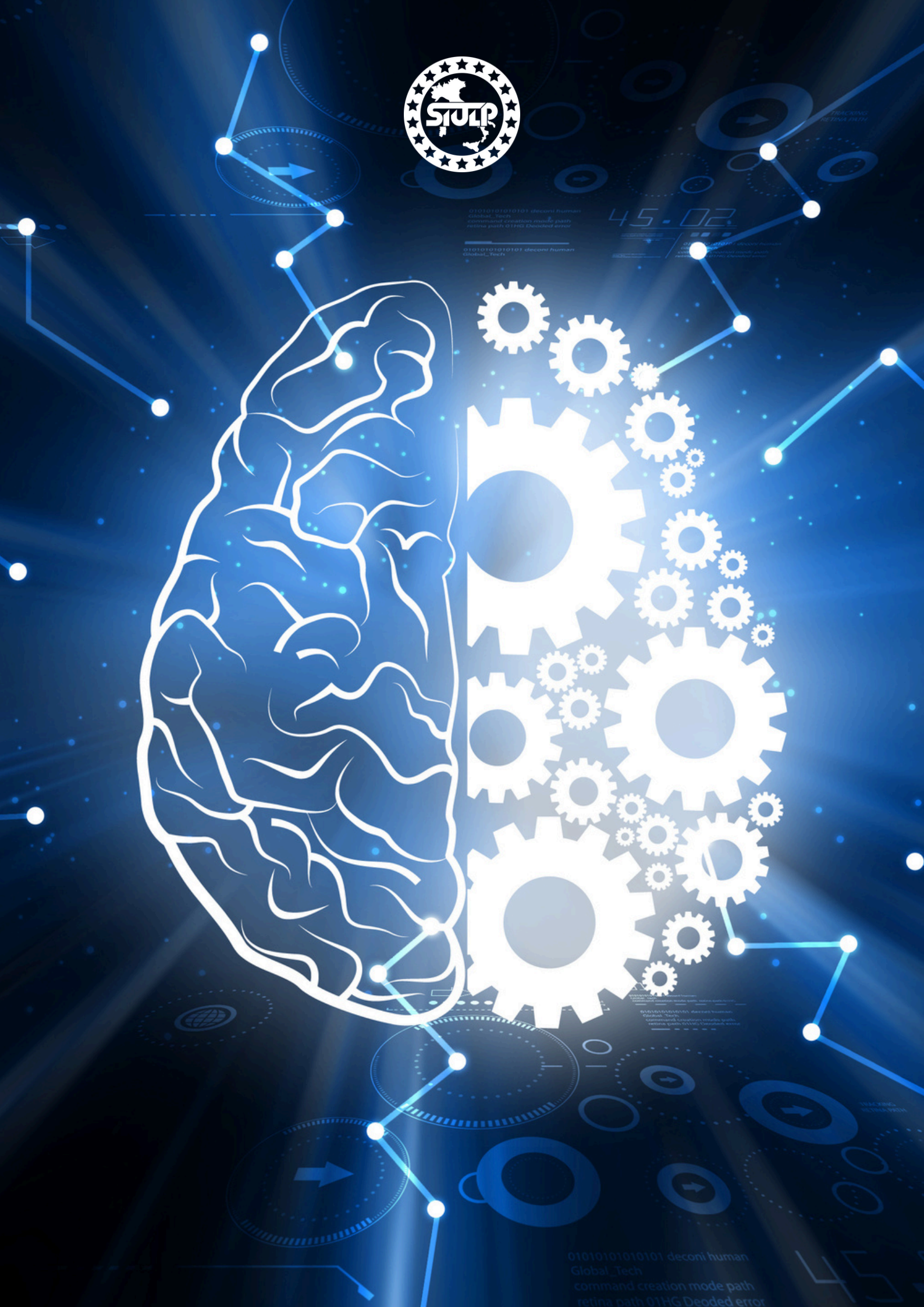
Occorre precisare, tuttavia, che nonostante la soglia minima del 14° anno, l'accesso dei minori ai siti, social media e ai servizi della rete è praticamente senza controlli e ciò anche perché non esistono strumenti che assicurino una verifica dell'età. I filtri sono attualmente costituiti da autodichiarazioni concernenti il possesso della maggiore età funzionali per lo più alla protezione di chi gestisce il sito e non di chi accede allo stesso. Il minore può tranquillamente mettere la spunta e navigare de plano.

La sfida principale, in un mondo sempre più digitale, è quella di individuare un giusto equilibrio tra l'uso efficiente delle nuove tecnologie e il rispetto della privacy degli individui.
La quantità di dati personali digitalmente trattata è enorme: informazioni anagrafiche, performance lavorative e personali, dati sensibili relativi a questioni mediche o disciplinari. Il GDPR impone obblighi rigorosi in termini di trasparenza, sicurezza e responsabilizzazione nella gestione dei dati personali e pesanti sanzioni economiche e reputazionali per l'uso improprio di sistemi di IA senza adeguati controlli sulla protezione dei dati personali.

L'uso di tecnologie come l'IA e i Big Data permette di analizzare comportamenti con effetti predittivi. Per tali ragioni, l'implementazione di tecnologie e sistemi di intelligenza artificiale solleva una serie di preoccupazioni etiche e legali, in particolare quando i dati raccolti vengono spesso utilizzati senza un esplicito consenso o senza un'adeguata protezione contro gli abusi.
Il GDPR stabilisce che l'uso di dati personali, soprattutto quelli sensibili, richiede una base giuridica chiara, come il consenso informato o la necessità per l'esecuzione di un contratto, con l'obbligo di dare una informazione trasparente sulla raccolta e utilizzazione dei dati e garantire idonee misure a presidio della loro sicurezza contro rischio di accessi non autorizzati.

Il rispetto della privacy e la protezione dei dati personali sono diventati temi centrali in tutto il mondo. Mentre l'uso di tecnologie avanzate come l'intelligenza artificiale e i big data offrono opportunità straordinarie per migliorare l'offerta educativa e l'efficienza amministrativa, è fondamentale che venga garantita la sicurezza e la privacy attraverso una maggiore formazione, investimenti nella sicurezza informatica e la formazione di professionalità esperte del settore.
Non si tratta, quindi, solo di comminare o evitare sanzioni, ma di costruire un ambiente più sicuro e trasparente per una corretta governance dei dati ed un rassicurante e proficuo uso delle nuove tecnologie.





Intelligenza Artificiale e Sicurezza Pubblica: Il Futuro del Controllo del Territorio

Negli ultimi anni, l'intelligenza artificiale (IA) ha rivoluzionato il modo in cui le forze dell'ordine gestiscono la sicurezza pubblica, offrendo strumenti avanzati per il controllo del territorio e la prevenzione del crimine. Dalla videosorveglianza intelligente al predictive policing, le applicazioni dell'IA stanno trasformando il settore con impatti significativi su efficienza e strategia operativa.

Riconoscimento facciale e analisi video in tempo reale

Uno degli sviluppi più rilevanti è l'uso del riconoscimento facciale e dell'analisi video basata su IA. Sistemi avanzati come Clearview AI e NEC NeoFace sono in grado di analizzare migliaia di volti in tempo reale, identificando individui sospetti e correlando le informazioni con database di criminali ricercati. L'adozione di queste tecnologie è in crescita in diversi paesi, come Cina e Stati Uniti, dove le autorità stanno testando la loro efficacia nel ridurre i tempi di identificazione e localizzazione dei soggetti di interesse.

Tuttavia, il loro utilizzo solleva questioni etiche e legali, in particolare per quanto riguarda la privacy e il rischio di errori di identificazione. Il General Data Protection Regulation (GDPR) dell'Unione Europea impone limitazioni sull'uso di queste tecnologie, vietando in alcuni casi il riconoscimento facciale nei luoghi pubblici. Organizzazioni per i diritti civili, come la Electronic Frontier Foundation (EFF), sottolineano il rischio di sorveglianza di massa e discriminazione algoritmica, spingendo per una regolamentazione più stringente a livello internazionale.

Inoltre, numerosi casi di falsi positivi hanno sollevato preoccupazioni su possibili errori giudiziari derivanti dall'uso di sistemi di riconoscimento facciale. Alcuni studi hanno evidenziato come questi algoritmi possano avere difficoltà nell'identificazione di individui appartenenti a minoranze etniche, aumentando il rischio di ingiuste detenzioni o errori investigativi. Per questo motivo, in alcune città statunitensi come San Francisco e Boston, è stato vietato l'uso del riconoscimento facciale nelle operazioni delle forze dell'ordine.

Predictive Policing: il crimine si può prevedere?

L'analisi predittiva è un altro strumento chiave. Basandosi su modelli di machine learning, piattaforme come PredPol analizzano dati storici sui crimini per identificare aree ad alto rischio e suggerire pattugliamenti mirati. Questi sistemi utilizzano dati geospaziali, informazioni demografiche e tendenze criminali per individuare le zone dove è più probabile che avvengano crimini, consentendo una distribuzione più efficace delle risorse delle forze dell'ordine.

Uno studio condotto dall'Università della California ha dimostrato che, se ben calibrato, il predictive policing può ridurre la criminalità fino al 20% in alcune aree urbane. Tuttavia, questi modelli non sono esenti da critiche. Ricercatori della Carnegie Mellon University hanno evidenziato il rischio di bias nei dati, con il pericolo che la polizia concentri le proprie risorse in quartieri già sovrapattugliati, perpetuando cicli di disuguaglianza e tensioni sociali. Un ulteriore problema è rappresentato dalla possibile sovrastima di alcune tipologie di reati minori rispetto a crimini più gravi, con il rischio di una gestione inefficiente delle risorse.

Alcuni stati stanno sperimentando una combinazione di predictive policing e analisi sociologica per mitigare questi problemi. Ad esempio, nei Paesi Bassi, un programma pilota integra dati predittivi con strategie di coinvolgimento della comunità per evitare discriminazioni e migliorare la collaborazione tra cittadini e forze dell'ordine.

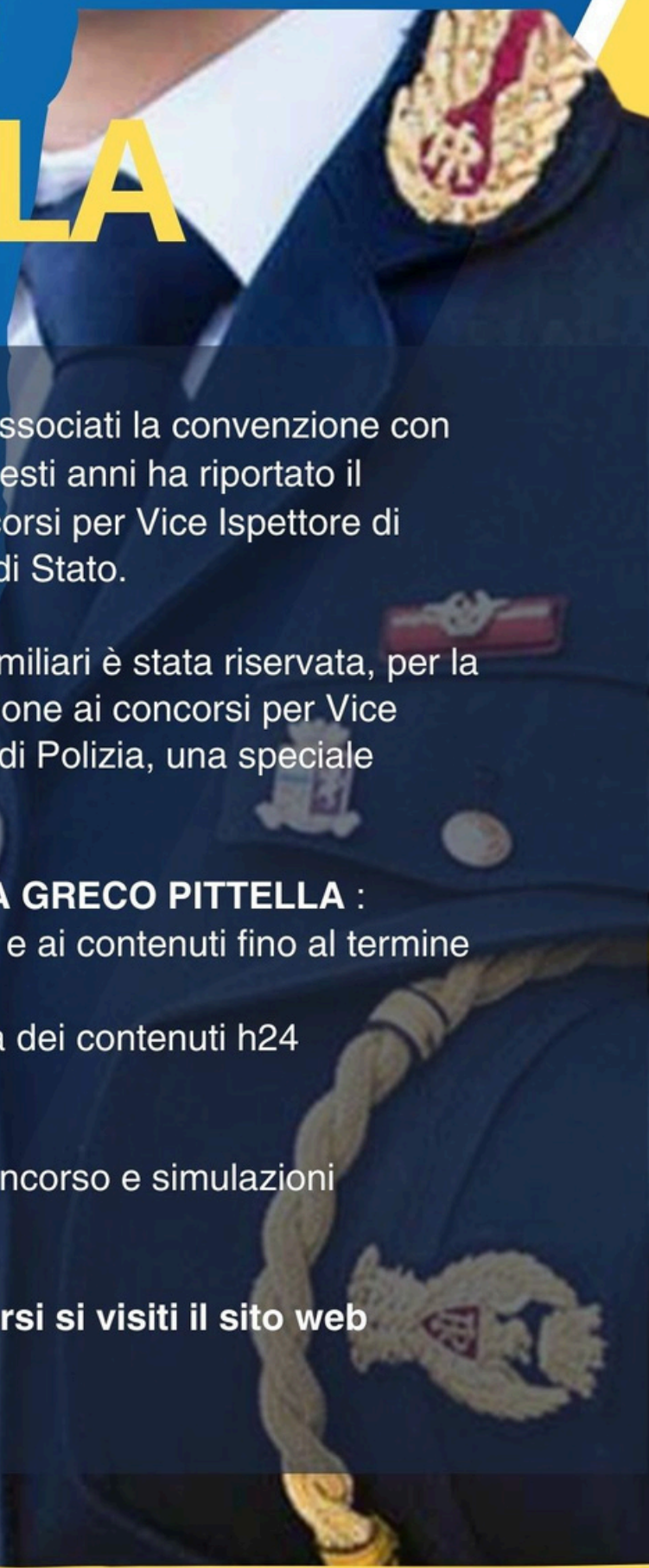
Sfide etiche e legali

L'impiego di IA nella sicurezza pubblica richiede un quadro normativo chiaro. L'Unione Europea ha recentemente proposto il Regulation on Artificial Intelligence Act, che mira a regolamentare l'uso di queste tecnologie, garantendo che non violino i diritti fondamentali. Organizzazioni internazionali, come l'ONU, hanno avviato dibattiti sull'etica dell'IA applicata alla sicurezza pubblica, sottolineando l'importanza della trasparenza degli algoritmi e della protezione dei dati personali.

Oltre alle regolamentazioni esistenti, vi è la necessità di standard più rigorosi per la verifica della correttezza e imparzialità degli algoritmi utilizzati dalle forze dell'ordine. Alcuni esperti propongono l'adozione di un audit indipendente per i sistemi di IA impiegati nella sicurezza pubblica, garantendo che siano equi e non discriminatori. Inoltre, la questione della responsabilità legale rimane aperta: chi è responsabile in caso di errore dell'IA? Le attuali normative non offrono ancora risposte chiare a queste domande cruciali.

Un altro aspetto da considerare è l'equilibrio tra sicurezza e diritti civili. Se da un lato l'IA offre strumenti innovativi per il contrasto alla criminalità, dall'altro il suo utilizzo massivo potrebbe portare a una società sempre più monitorata e meno libera. Il dibattito su questi temi è ancora aperto, e sarà essenziale che le decisioni in merito vengano prese con un approccio basato sulla trasparenza, sul rispetto della privacy e sulla protezione dei diritti umani.

SCUOLA GRECO PITTELLA



Il **SIULP** ha rinnovato per i propri associati la convenzione con la **Scuola Greco Pittella** che in questi anni ha riportato il maggior numero di vincitori ai concorsi per Vice Ispettore di Polizia e Commissari della Polizia di Stato.

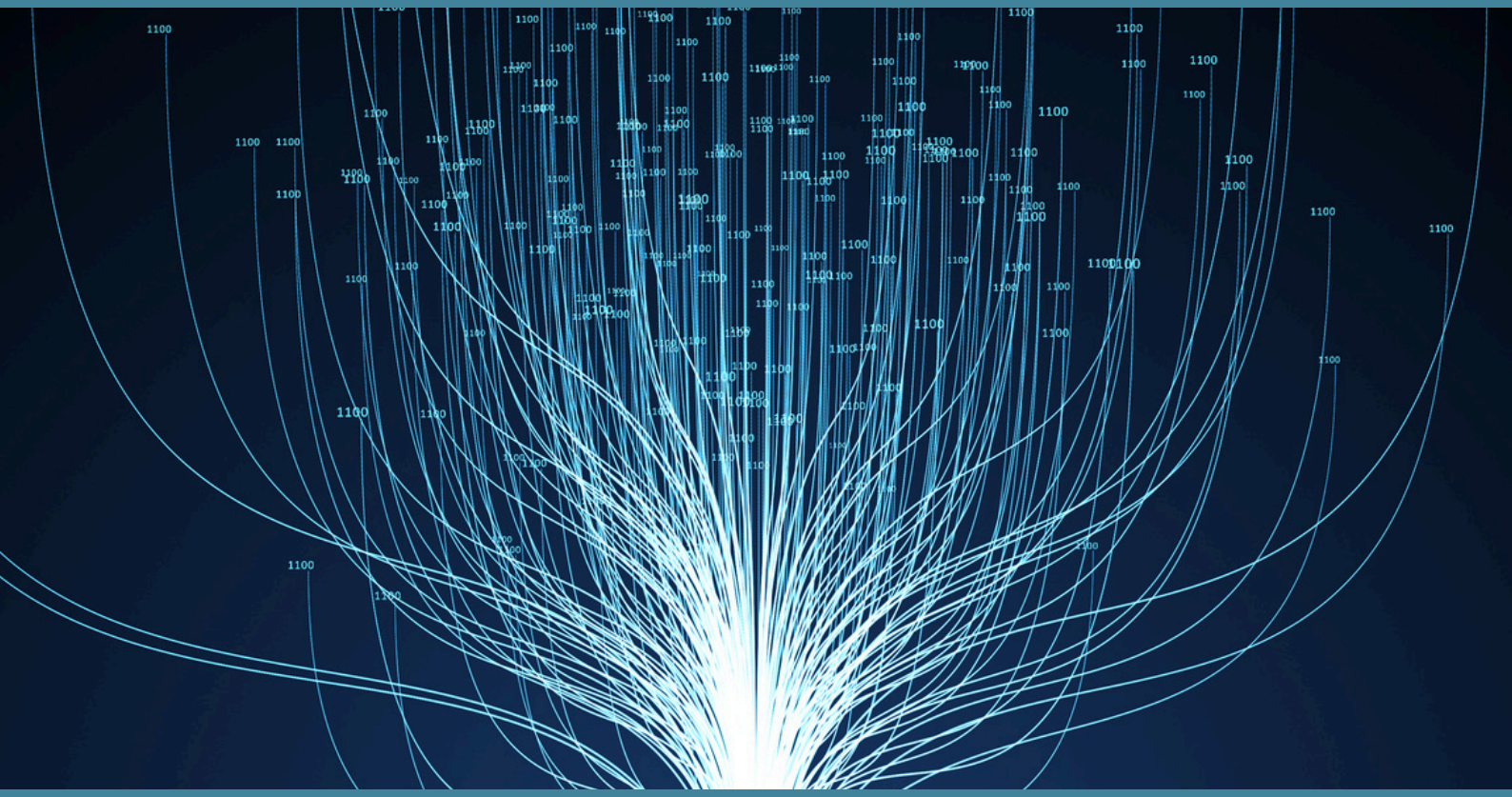
Per gli iscritti al Siulp e per i loro familiari è stata riservata, per la partecipazione ai corsi di preparazione ai concorsi per Vice Ispettore di Polizia e Commissario di Polizia, una speciale tariffa.

Preparati con i corsi della **SCUOLA GRECO PITTELLA** :

- accesso illimitato alla piattaforma e ai contenuti fino al termine delle prove concorsuali
- lezioni fruibili online e disponibilità dei contenuti h24
- docenti qualificati
- numero limitato di studenti
- lezioni sulle materie oggetto di concorso e simulazioni realistiche di prova scritta

Per maggiori informazioni sui corsi si visiti il sito web

www.scuolagrecopittella.it



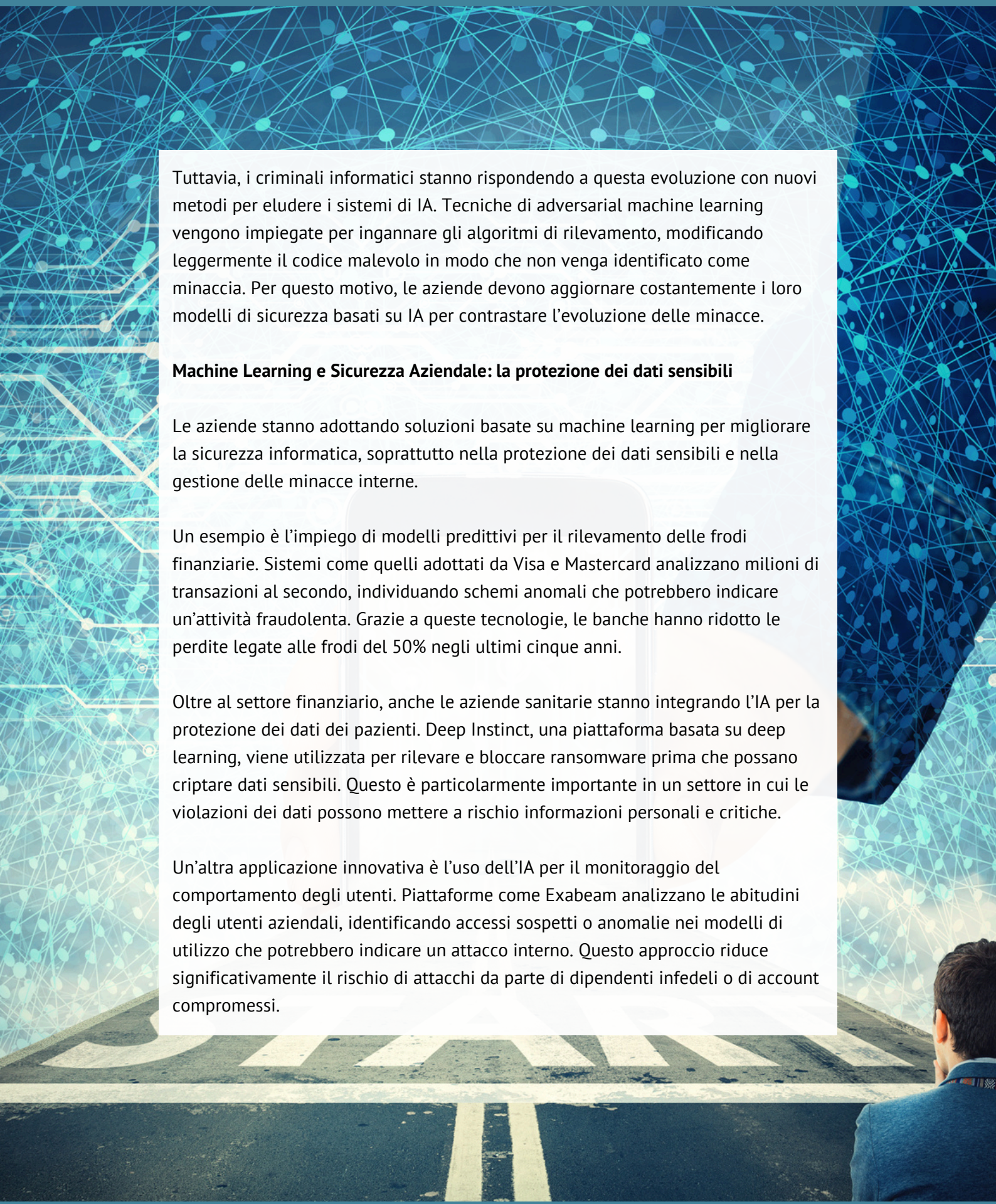
AI e Cybersecurity: La Nuova Frontiera della Protezione Digitale

L'intelligenza artificiale (IA) ha rivoluzionato il settore della cybersecurity, fornendo strumenti avanzati per la protezione dei sistemi informatici, ma introducendo al contempo nuove sfide. Se da un lato le aziende e le istituzioni possono contare su sistemi di difesa più sofisticati, dall'altro gli attori malevoli stanno sviluppando attacchi sempre più avanzati basati sulle stesse tecnologie.

AI e Threat Detection: identificare gli attacchi in tempo reale

L'IA viene oggi utilizzata per individuare minacce informatiche in tempo reale, riducendo i tempi di reazione rispetto ai metodi tradizionali. I sistemi di Intrusion Detection and Prevention Systems (IDPS) basati su IA analizzano continuamente il traffico di rete, identificando comportamenti anomali che potrebbero indicare un attacco in corso.

Tecnologie come Darktrace, che utilizza algoritmi di apprendimento automatico per monitorare il traffico di rete, sono in grado di rilevare attività sospette e prevenire attacchi avanzati, tra cui attacchi zero-day e Advanced Persistent Threats (APT). Secondo un report di IBM X-Force Threat Intelligence Index, le organizzazioni che adottano sistemi di threat detection basati su IA riescono a ridurre i tempi di risposta agli attacchi fino al 96% rispetto a sistemi tradizionali.



Tuttavia, i criminali informatici stanno rispondendo a questa evoluzione con nuovi metodi per eludere i sistemi di IA. Tecniche di adversarial machine learning vengono impiegate per ingannare gli algoritmi di rilevamento, modificando leggermente il codice malevolo in modo che non venga identificato come minaccia. Per questo motivo, le aziende devono aggiornare costantemente i loro modelli di sicurezza basati su IA per contrastare l'evoluzione delle minacce.

Machine Learning e Sicurezza Aziendale: la protezione dei dati sensibili

Le aziende stanno adottando soluzioni basate su machine learning per migliorare la sicurezza informatica, soprattutto nella protezione dei dati sensibili e nella gestione delle minacce interne.

Un esempio è l'impiego di modelli predittivi per il rilevamento delle frodi finanziarie. Sistemi come quelli adottati da Visa e Mastercard analizzano milioni di transazioni al secondo, individuando schemi anomali che potrebbero indicare un'attività fraudolenta. Grazie a queste tecnologie, le banche hanno ridotto le perdite legate alle frodi del 50% negli ultimi cinque anni.

Oltre al settore finanziario, anche le aziende sanitarie stanno integrando l'IA per la protezione dei dati dei pazienti. Deep Instinct, una piattaforma basata su deep learning, viene utilizzata per rilevare e bloccare ransomware prima che possano criptare dati sensibili. Questo è particolarmente importante in un settore in cui le violazioni dei dati possono mettere a rischio informazioni personali e critiche.

Un'altra applicazione innovativa è l'uso dell'IA per il monitoraggio del comportamento degli utenti. Piattaforme come Exabeam analizzano le abitudini degli utenti aziendali, identificando accessi sospetti o anomalie nei modelli di utilizzo che potrebbero indicare un attacco interno. Questo approccio riduce significativamente il rischio di attacchi da parte di dipendenti infedeli o di account compromessi.

Deepfake e Frodi Digitali: la nuova frontiera del crimine informatico

L'uso dei deepfake rappresenta una delle minacce più pericolose e in crescita nel panorama della cybersecurity. Grazie ai progressi nelle reti neurali generative (GANs), i criminali informatici possono creare video e audio falsificati estremamente realistici, utilizzati per frodi aziendali, disinformazione politica e attacchi di social engineering.

Un caso emblematico è quello delle truffe basate su synthetic voice phishing, in cui l'IA viene utilizzata per imitare la voce di dirigenti aziendali e convincere i dipendenti a trasferire ingenti somme di denaro. Nel 2019, una società britannica ha subito una frode da 243.000 dollari dopo che un dipendente è stato ingannato da una chiamata deepfake che imitava la voce del CEO.

Oltre agli attacchi finanziari, i deepfake vengono impiegati anche per la disinformazione politica. Secondo un report del Cybersecurity and Infrastructure Security Agency (CISA), le campagne elettorali e le operazioni di manipolazione dell'opinione pubblica stanno sempre più sfruttando video e immagini deepfake per diffondere notizie false. Questo fenomeno rappresenta una sfida per le piattaforme di social media, che stanno sviluppando strumenti di IA per rilevare contenuti manipolati.

Per contrastare questa minaccia, aziende come Microsoft e Facebook hanno avviato iniziative per identificare e bloccare i deepfake prima che vengano diffusi. Il progetto Deepfake Detection Challenge, ad esempio, mira a creare algoritmi in grado di riconoscere contenuti manipolati con un'accuratezza superiore al 95%.

L'intelligenza artificiale sta ridefinendo il panorama della cybersecurity, offrendo strumenti innovativi per la protezione delle reti, la rilevazione delle minacce e la gestione della sicurezza aziendale. Tuttavia, l'evoluzione parallela delle tecniche di attacco basate su IA impone un aggiornamento continuo delle strategie di difesa.
Le aziende e le istituzioni devono investire nella formazione dei loro dipendenti, nell'implementazione di sistemi di threat detection sempre più avanzati e nella collaborazione con enti specializzati nella ricerca sulla cybersecurity. Solo attraverso un approccio proattivo e basato sull'innovazione sarà possibile contrastare le minacce emergenti e garantire la protezione dei dati e delle infrastrutture digitali in un'epoca sempre più connessa e vulnerabile.

BJJ4POLICE

L'INNOVATIVO CORSO DI BRAZILIAN JIU JITSU PER GLI OPERATORI DELLA POLIZIA DI STATO

L’Intelligenza Artificiale nelle Operazioni Antiterrorismo: Nuove Strategie di Intervento

Negli ultimi anni, l’intelligenza artificiale (IA) ha assunto un ruolo centrale nelle strategie globali di contrasto al terrorismo. L’IA offre strumenti innovativi per l’analisi delle comunicazioni sospette, il monitoraggio del web e il rilevamento di minacce, permettendo alle forze di sicurezza di agire in modo più rapido ed efficace. Tuttavia, il suo utilizzo solleva questioni relative alla privacy e alla governance internazionale della sicurezza digitale.

Analisi automatizzata delle minacce: come l’IA aiuta le forze di sicurezza

Uno degli utilizzi più avanzati dell’IA nell’antiterrorismo riguarda l’analisi automatizzata delle comunicazioni online e il monitoraggio delle attività sospette nel dark web. Piattaforme basate su machine learning, come Palantir e IBM Watson, vengono impiegate da agenzie di intelligence per analizzare enormi quantità di dati e identificare schemi sospetti nelle comunicazioni digitali.

L'IA consente di individuare rapidamente parole chiave, frasi e modelli di comportamento associati a gruppi terroristici. Ad esempio, la tecnologia sviluppata dal programma Inspire dell'FBI è stata utilizzata per tracciare le comunicazioni di cellule terroristiche e prevedere possibili attacchi. Inoltre, il Progetto TITAN dell'Europol sfrutta il deep learning per identificare minacce terroristiche in tempo reale, aggregando informazioni da fonti aperte, social media e dati riservati.

Tuttavia, l'uso dell'IA per il monitoraggio di comunicazioni solleva questioni legali ed etiche. La sorveglianza di massa e la possibilità di raccogliere dati di utenti non sospettati di attività illecite creano tensioni con il diritto alla privacy sancito da regolamenti internazionali, come il GDPR europeo e il Cloud Act statunitense.

Droni e robot per la sicurezza: impiego di tecnologie autonome

Un altro ambito in cui l'IA sta rivoluzionando l'antiterrorismo è l'impiego di droni e robot autonomi per missioni di intelligence e neutralizzazione di minacce.

Le forze armate e le agenzie di sicurezza utilizzano droni equipaggiati con IA per sorveglianza aerea, ricognizione tattica e operazioni di contrasto a gruppi terroristici in aree difficilmente accessibili. Sistemi come il Reaper MQ-9 e il Skyborg dell'US Air Force sono in grado di operare autonomamente, analizzando in tempo reale la situazione sul campo e trasmettendo dati critici ai centri operativi.

Oltre ai droni, anche i robot terrestri vengono utilizzati in scenari di alto rischio. Dispositivi come il PackBot di iRobot, impiegato dall'esercito statunitense, sono progettati per operazioni di neutralizzazione di ordigni esplosivi (EOD) e per il supporto tattico nelle operazioni urbane.

L'autonomia di queste tecnologie solleva interrogativi sulla necessità di un controllo umano nelle decisioni letali. Il dibattito sull'uso di sistemi d'arma autonomi letali (LAWS) è aperto, con organismi come l'ONU che chiedono regolamentazioni chiare per evitare abusi e garantire il rispetto del diritto internazionale umanitario.

Collaborazione internazionale: IA e lotta globale al terrorismo

La lotta contro il terrorismo richiede una cooperazione internazionale sempre più avanzata, con lo scambio di informazioni tra governi e agenzie di intelligence. L'IA sta facilitando questa cooperazione, migliorando la condivisione dei dati e ottimizzando il coordinamento operativo.

A livello europeo, progetti come il CT INFLOW dell'Europol utilizzano l'intelligenza artificiale per analizzare flussi finanziari sospetti legati a organizzazioni terroristiche. Algoritmi avanzati monitorano transazioni bancarie, criptovalute e crowdfunding illegale, aiutando le forze di sicurezza a individuare finanziamenti illeciti destinati ad attività terroristiche.

L'intelligenza artificiale rappresenta uno strumento fondamentale nelle moderne strategie di antiterrorismo, offrendo capacità avanzate di analisi, sorveglianza e intervento. Tuttavia, il suo impiego solleva questioni etiche e richiede una regolamentazione chiara per evitare violazioni della privacy e garantire un uso responsabile delle tecnologie.

Per affrontare queste sfide, è essenziale che i governi e le istituzioni internazionali promuovano politiche di trasparenza, supervisione umana e cooperazione globale. L'IA può essere un alleato prezioso nella lotta contro il terrorismo, ma solo se utilizzata in modo etico e conforme ai diritti umani.

SERVIZIO DI CONSULENZA FISCALE E SERVIZIO DI ASSISTENZA PENSIONISTICO

SIULP.OKCAF.IT

SERVIZI GRATUITI OFFERTI AGLI ISCRITTI SIULP

L’AI e la Sicurezza nei Sistemi di Smart Cities: Protezione e Sorveglianza Urbana

Le smart cities stanno adottando soluzioni di intelligenza artificiale (IA) per migliorare la sicurezza urbana, ottimizzare i servizi pubblici e proteggere le infrastrutture critiche. Tuttavia, l’integrazione diffusa dell’IA solleva interrogativi su privacy, sorveglianza e governance etica.

Videosorveglianza avanzata e analisi del comportamento sospetto

Uno degli impieghi più diffusi dell’IA nelle smart cities è la videosorveglianza avanzata. Le città stanno implementando telecamere intelligenti dotate di computer vision per il riconoscimento facciale, l’analisi dei movimenti e la rilevazione di comportamenti sospetti. Sistemi come quelli utilizzati a Londra e Pechino consentono alle autorità di identificare rapidamente individui ricercati, rilevare attività anomale e prevenire potenziali minacce.

Piattaforme come BriefCam e Avigilon sfruttano l’IA per analizzare automaticamente flussi video in tempo reale, riducendo il carico di lavoro degli operatori di sicurezza. Tali sistemi permettono di individuare assembramenti improvvisi, oggetti abbandonati e movimenti non conformi ai normali schemi urbani.

Tuttavia, l'impiego di questi strumenti non è privo di controversie. Organizzazioni per i diritti civili, come l'Electronic Frontier Foundation (EFF), mettono in guardia sul rischio di sorveglianza di massa e sulla possibilità che tali sistemi vengano utilizzati per fini di controllo sociale anziché per la sola sicurezza pubblica. In alcuni paesi, come gli Stati Uniti, città come San Francisco e Portland hanno vietato l'uso del riconoscimento facciale da parte delle forze dell'ordine per motivi di privacy.

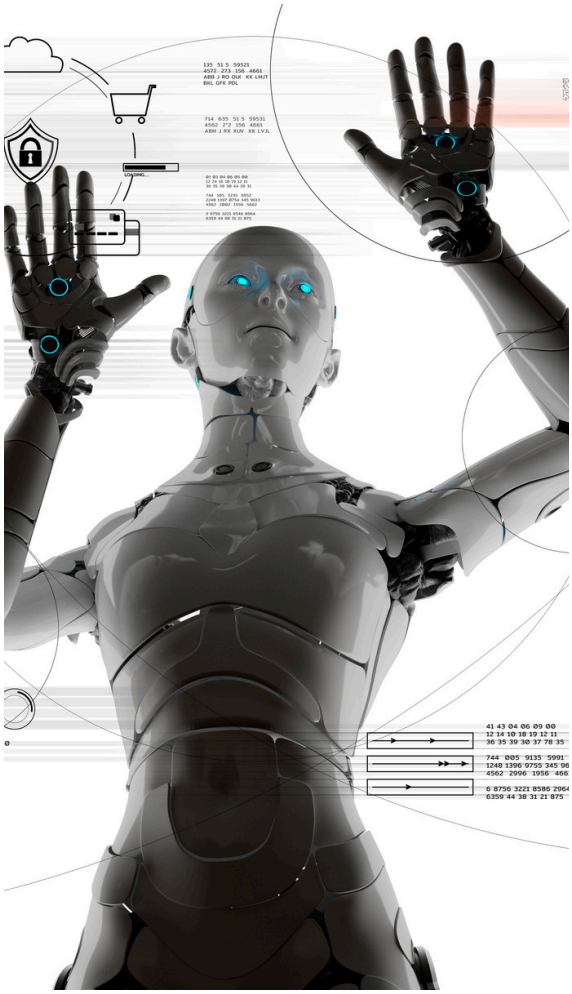
Cybersecurity per infrastrutture critiche

Le smart cities dipendono da reti digitali avanzate per la gestione dei servizi essenziali, tra cui illuminazione pubblica, trasporti, sanità e distribuzione dell'energia. La loro interconnessione le rende particolarmente vulnerabili ad attacchi informatici. Proteggere queste infrastrutture è quindi una priorità assoluta.

L'IA viene impiegata per rafforzare la sicurezza informatica delle città intelligenti, analizzando in tempo reale il traffico di rete e identificando anomalie che potrebbero indicare un attacco. Strumenti come Darktrace, basati su algoritmi di apprendimento automatico, consentono di rilevare e mitigare minacce cibernetiche prima che possano compromettere sistemi critici.

Un esempio concreto di vulnerabilità delle smart cities è l'attacco hacker subito dalla città di Atlanta nel 2018, quando un attacco ransomware ha paralizzato numerosi servizi municipali, inclusi il pagamento delle multe e l'accesso ai dati giudiziari. Episodi simili evidenziano l'importanza di dotare le città di sistemi di protezione avanzati, che combinino crittografia, autenticazione multi-fattore e intelligenza artificiale per la rilevazione delle minacce.

In Europa, il programma EU Cybersecurity Act ha introdotto normative più stringenti per garantire che le infrastrutture urbane siano adeguatamente protette. Tuttavia, la continua evoluzione delle minacce informatiche richiede un aggiornamento costante delle strategie difensive, specialmente con l'aumento dell'Internet of Things (IoT), che connette milioni di dispositivi alle reti cittadine.



L'importanza di una governance etica

L'integrazione dell'IA nelle smart cities solleva questioni fondamentali di governance e diritti civili. Se da un lato l'automazione migliora l'efficienza urbana, dall'altro vi è il rischio di creare una società in cui la sorveglianza sia onnipresente e le libertà individuali siano limitate.

Per questo motivo, diverse organizzazioni e governi stanno lavorando per stabilire principi etici per l'uso dell'IA. L'Unione Europea, ad esempio, ha sviluppato il Regolamento sull'Intelligenza Artificiale, che mira a garantire trasparenza, equità e responsabilità nell'uso delle tecnologie di sorveglianza.

Un approccio equilibrato alla governance dell'IA dovrebbe includere:
Trasparenza: Le città devono informare i cittadini sull'uso dei sistemi di IA, specificando finalità e limiti della raccolta dati.
Supervisione umana: Nonostante l'automazione, le decisioni critiche che riguardano la sicurezza pubblica devono essere supervisionate da esseri umani.

Protezione della privacy: L'adozione di sistemi di anonimizzazione dei dati e limiti alla conservazione delle informazioni personali è essenziale per evitare abusi.

L'intelligenza artificiale sta rivoluzionando il concetto di sicurezza urbana, offrendo soluzioni innovative per il monitoraggio, la prevenzione del crimine e la protezione delle infrastrutture critiche. Tuttavia, il suo utilizzo deve essere attentamente regolamentato per evitare derive autoritarie e garantire il rispetto dei diritti fondamentali.

Per il futuro, sarà cruciale trovare un equilibrio tra innovazione e tutela della libertà individuale, garantendo che le smart cities rimangano spazi sicuri ma anche rispettosi della privacy e della democrazia.

SE PENSI IN GRANDE
PENSI SIULP

SEGRETERIA NAZIONALE
Via Vicenza, 26 - 00185 Roma
Tel. +39 06 4455213
e-mail: nazionale@siulp.it