PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4732 di Venerdì 03 luglio 2020

# Intelligenza artificiale e indagini criminali. Vi può essere conflitto?

***La commissione LIBE del parlamento europeo si è attivata per verificare se l'utilizzo di algoritmi di intelligenza artificiale, a fini di prevenzione e contrasto del crimine, possano andare in conflitto con esigenze di protezione dei dati personali.***

L' intelligenza artificiale (IA) è una delle tecnologie strategiche del 21° secolo, generando notevoli vantaggi in termini di efficienza, accuratezza e convenienza e contribuendo così positivamente all'economia europea. Tra le altre cose, le applicazioni IA hanno migliorato l'assistenza sanitaria, aumentato l'efficienza dell'agricoltura, contribuito alla mitigazione e all'adattamento IA cambiamenti climatici e migliorato l'efficienza della produzione.

L'intelligenza artificiale è una delle principali priorità dell'attuale Commissione. Il presidente della Commissione Ursula von der Leyen ha annunciato nei suoi orientamenti politici un approccio europeo coordinato sulle implicazioni umane ed etiche dell'intelligenza artificiale, nonché una riflessione sull'uso migliore dei big data per l'innovazione.

Il fulcro dell'IA è il fatto che si basa sulla raccolta, analisi e l'accumulo ricorrente di grandi quantità di dati, inclusi dati personali, da una varietà di fonti, che sono soggetti a elaborazione automatizzata da algoritmi informatici e tecniche avanzate di elaborazione dei dati. Queste tecniche utilizzano sia i dati archiviati, sia quelli in streaming, per generare determinate correlazioni, tendenze e modelli (analisi dei big data). I dati utilizzati per l'IA non provengono solo dalle persone stesse; Le applicazioni di intelligenza artificiale utilizzano principalmente dati provenienti dall'industria, dalle imprese e dal settore pubblico, elaborati per scopi diversi.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0551] ?#>

Anche se i dati utilizzati dalle applicazioni IA possono talvolta essere dati non personali, molto spesso l'attività di IA comporta l'elaborazione di dati personali, poiché spesso l'attività di IA porta a decisioni automatizzate che hanno un effetto diretto sugli individui. Queste caratteristiche dell'intelligenza artificiale ci richiedono pertanto di prestare particolare attenzione in questo settore al rispetto dei principi di base della protezione dei dati e della privacy.

L' intelligenza artificiale offre grandi opportunità anche nel settore dell'applicazione della legge e della giustizia penale, in particolare nel miglioramento dei metodi di lavoro delle forze dell'ordine e delle autorità giudiziarie e nella lotta contro alcuni tipi di reati in modo più efficiente, in particolare nel campo della criminalità finanziaria, del denaro riciclaggio e finanziamento del terrorismo e alcuni tipi di criminalità informatica. In questo settore, le applicazioni IA includono tecnologie di riconoscimento facciale, riconoscimento automatico della targa, identificazione degli oratori, identificazione del parlato, tecnologie di lettura delle labbra, sorveglianza uditiva (ad es. algoritmi di rilevazione degli spari), ricerca e analisi autonome di banche dati identificate, previsioni (attività di polizia predittiva e analisi degli hotspot criminali), strumenti di rilevazione del comportamento, strumenti autonomi per identificare frodi finanziarie e finanziamento del terrorismo, social media,

monitoraggio (scraping e raccolta dati per il mining delle connessioni), sistemi di sorveglianza automatizzati che incorporano diverse funzionalità di rilevamento (come rilevamento del battito cardiaco e telecamere termiche). In ambito giudiziario, gli strumenti di intelligenza artificiale possono essere utilizzati nel calcolo delle probabilità di recidiva e nella determinazione della libertà vigilata o della decisione sulla condanna.

Nonostante i benefici apportati dall' intelligenza artificiale, il fatto è che contemporaneamente l'IA comporta una serie di rischi potenziali, come processi decisionali opachi, diversi tipi di discriminazione, intrusione nella nostra vita privata, sfide alla protezione dei dati personali, dignità umana e la libertà di espressione e informazione. Questi potenziali rischi sono aggravati nel settore delle forze dell'ordine e della giustizia penale, poiché possono influire sulla presunzione di innocenza, sui diritti fondamentali alla libertà e alla sicurezza dell'individuo e su un ricorso effettivo e un processo equo.

La relazione LIBE intende affrontare le questioni sollevate dall'uso dell'intelligenza artificiale nel diritto penale e dal suo uso da parte della polizia e delle autorità giudiziarie in materia penale. Pur riconoscendo le potenziali opportunità e vantaggi che l'IA può comportare, evidenzia anche i rischi e gli effetti significativi che può comportare.

La relazione sottolinea la necessità di rispettare pienamente i diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, dalla normativa dell'Unione in materia di privacy e protezione dei dati, vale a dire la direttiva (UE) 2016/680 (direttiva polizia) e la necessità di applicare diversi principi fondamentali nel ciclo di vita dell'IA, come trasparenza dell'algoritmo, tracciabilità, svolgimento di valutazioni d'impatto obbligatorie sui diritti fondamentali, prima dell'implementazione o della diffusione di qualsiasi sistema di IA e audit obbligatori. Tutti questi requisiti non sono solo necessari per garantire la liceità dei sistemi di intelligenza artificiale, ma anche per ottenere la fiducia delle persone sul loro uso da parte delle forze dell'ordine e delle autorità giudiziarie penali.

Infine, il relatore chiede una moratoria per la diffusione di sistemi di riconoscimento facciale a fini di contrasto. Lo stato attuale di queste tecnologie, gli impatti significativi sui diritti fondamentali, richiedono un dibattito sociale approfondito e aperto al fine di considerare le diverse domande poste e la giustificazione per il loro spiegamento.

**Adalberto Biasiotti**

Questo articolo è pubblicato sotto una Licenza Creative Commons.

---

**www.puntosicuro.it**