Parlamento europeo
2019-2024

Commissione per le libertà civili, la giustizia e gli affari interni

2020/2016(INI)

8.6.2020

PROGETTO DI RELAZIONE

sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale
(2020/2016(INI))

Commissione per le libertà civili, la giustizia e gli affari interni

Relatore: Tudor Ciuhodaru

PR_INI

INDICE

Pagina

PROPOSTA DI RISOLUZIONE DEL PARLAMENTO EUROPEO

sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale
(2020/2016(INI))

Il Parlamento europeo,

– visti il trattato sull'Unione europea, in particolare gli articoli 2 e 6 e il trattato sul funzionamento dell'Unione europea,

– vista la Carta dei diritti fondamentali dell'Unione europea,

– vista la Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali,

– vista la Convenzione del Consiglio d'Europa per la tutela delle persone fisiche con riguardo al trattamento automatizzato di dati personali (ETS 108),

– vista la comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni dal titolo "Creare fiducia nell'intelligenza artificiale antropocentrica" dell'8 aprile 2019[1],

– visto il libro bianco della Commissione dal titolo "Intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia" del 19 febbraio 2020[2],

– vista la comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni dal titolo "Una strategia europea per i dati" del 19 febbraio 2020[3],

– visto il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)[4],

– vista la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio[5],

[1] COM(2019)0168.
[2] COM(2020)0065.
[3] COM(2020)0066.
[4] GU L 119 del 4.5.2016, pag. 1.
[5] GU L 119 del 4.5.2016, pag. 89.

– visto il regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE[6],

– vista la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)[7],

– visto il regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI[8],

– visto l'articolo 54 del suo regolamento,

– visti i pareri della commissione per il mercato interno e la protezione dei consumatori e della commissione giuridica,

– vista la relazione della commissione per le libertà civili, la giustizia e gli affari interni (A9-0000/2020),

A. considerando che le tecnologie digitali in generale e l'intelligenza artificiale (IA) in particolare portano con sé una promessa straordinaria; che l'IA è una delle tecnologie strategiche del XXI secolo e genera notevoli benefici in termini di efficienza, precisione e comodità, apportando in tal modo un cambiamento positivo all'economia europea; che l'IA non dovrebbe essere vista come fine a stessa, ma come uno strumento al servizio delle persone, con lo scopo ultimo di accrescere il benessere degli esseri umani;

B. considerando che lo sviluppo dell'IA deve rispettare i valori su cui si fonda l'Unione, in particolare la dignità umana, la democrazia, l'uguaglianza, lo Stato di diritto e i diritti umani e fondamentali;

C. considerando che sistemi di IA affidabili devono essere responsabili, concepiti per tutti (tenendo conto, nella loro progettazione, delle popolazioni vulnerabili ed emarginate), non discriminatori, sicuri e trasparenti e rispettare l'autonomia umana e i diritti fondamentali;

D. considerando che l'Unione, insieme agli Stati membri, ha l'importante responsabilità di garantire che le scelte politiche relative allo sviluppo, alla diffusione e all'utilizzo delle applicazioni di IA nel settore giudiziario e delle attività di contrasto siano fatte in modo trasparente, rispettino i principi di necessità e proporzionalità e garantiscano che le politiche e le misure adottate salvaguardino appieno i diritti fondamentali all'interno

[6] GU L 295 del 21.11.2018, pag. 39.
[7] GU L 201 del 31.7.2002, pag. 37.
[8] GU L 135 del 24.5.2016, pag. 53.

dell'Unione;

E. considerando che le applicazioni di IA offrono grandi opportunità nel settore delle attività di contrasto, in particolare migliorando i metodi di lavoro delle autorità di contrasto e delle autorità giudiziarie e lottando in modo efficace contro alcuni tipi di reati, in particolare reati finanziari, riciclaggio di denaro e finanziamento del terrorismo, nonché alcuni tipi di reati informatici;

F. considerando che è necessario un modello chiaro per attribuire la responsabilità per i potenziali effetti nocivi dei sistemi di IA nel settore del diritto penale;

G. considerando che le applicazioni di IA utilizzate dalle autorità di contrasto includono applicazioni quali le tecnologie di riconoscimento facciale, riconoscimento automatizzato delle targhe, identificazione di chi parla, identificazione vocale, tecnologie di lettura labiale, analisi di segnali acustici (algoritmi di rilevamento di colpi di arma da fuoco), ricerca autonoma e analisi di database identificati, previsioni (polizia predittiva e analisi della scena del crimine), strumenti di rilevamento dei comportamenti, strumenti autonomi per identificare le frodi finanziarie e il finanziamento del terrorismo, monitoraggio dei social media (estrazione e raccolta di dati per l'estrazione di connessioni), numeri IMSI (International Mobile Subscriber Identity) e sistemi di sorveglianza automatica che integrano diverse capacità di rilevamento (come il rilevamento cardiaco e le videocamere termiche); che le applicazioni di cui sopra presentano gradi molto diversi di affidabilità e precisione;

H. considerando che gli strumenti e le applicazioni di IA sono altresì utilizzati dal potere giudiziario in tutto il mondo, per esempio nell'irrogazione delle pene, nel calcolo delle probabilità di recidiva e nelle decisioni di sospensione condizionale;

I. considerando che l'utilizzo dell'IA nelle attività di contrasto comporta una serie di rischi potenziali, quali processi decisionali opachi, vari tipi di discriminazione e rischi per la protezione della vita privata e dei dati personali, per la protezione della libertà di espressione e informazione e per la presunzione di innocenza;

J. considerando che i sistemi di IA utilizzati dalle autorità di contrasto sono anch'essi vulnerabili agli attacchi basati sull'IA; che in tali situazioni i danni che ne derivano sono potenzialmente ancora più significativi e possono tradursi in livelli esponenzialmente maggiori di danni tanto per gli individui quanto per i gruppi;

1. ribadisce che, poiché il trattamento di grandi quantità di dati costituisce la base dell'IA, il diritto alla tutela della vita privata e il diritto alla protezione dei dati personali si applicano a tutti i settori dell'IA, e che il quadro giuridico dell'Unione in materia di protezione dei dati e della vita privata deve essere pienamente rispettato;

2. ribadisce che tutte le soluzioni di IA per le attività di contrasto e il settore giudiziario devono inoltre rispettare appieno i principi di non discriminazione, libertà di movimento, presunzione di innocenza e diritto di difesa, libertà di espressione e informazione, libertà di riunione e associazione, uguaglianza dinanzi alla legge, e diritto a un ricorso effettivo e a un processo equo;

3. ritiene, a tale proposito, che qualsiasi strumento di IA sviluppato o utilizzato dalle autorità

di contrasto o giudiziarie dovrebbe come minimo essere sicuro e adatto allo scopo previsto, rispettare i principi di equità, responsabilità, trasparenza e spiegabilità, e la sua diffusione dovrebbe essere soggetta a una rigorosa verifica della necessità e della proporzionalità;

4. sottolinea l'importanza di evitare la sorveglianza di massa tramite le tecnologie di IA e di vietare le applicazioni che risulterebbero in tale sorveglianza;

5. sottolinea che l'uso di strumenti di apprendimento automatico e di applicazioni basate sull'intelligenza artificiale potrebbe comportare distorsioni e discriminazioni; osserva che le distorsioni possono essere intrinseche agli insiemi di dati di base, specie se si utilizzano dati storici, inseriti dagli sviluppatori degli algoritmi o generati quando i sistemi sono attuati in contesti reali;

6. sottolinea che molte tecnologie di identificazione basate su algoritmi commettono un numero sproporzionato di errori di identificazione sulle persone non bianche, i bambini, gli anziani e le donne;

7. sottolinea l'asimmetria di potere tra coloro che sviluppano e diffondono le tecnologie di IA e coloro che interagiscono con esse e vi sono soggetti;

8. sottolinea che gli aspetti legati alla sicurezza e alla protezione dei sistemi di IA utilizzati nelle attività di contrasto devono essere valutati con attenzione ed essere abbastanza solidi e resilienti per prevenire le conseguenze potenzialmente catastrofiche di attacchi dolosi contro i sistemi di IA;

9. ritiene sia necessario istituire un regime chiaro ed equo per attribuire la responsabilità giuridica delle potenziali conseguenze negative prodotte da tali tecnologie digitali avanzate;

10. sottolinea che, nei contesti giudiziari e di contrasto, la decisione finale deve sempre essere presa da un essere umano, il quale possa essere ritenuto responsabile per le decisioni adottate, e deve includere la possibilità di ricorrere a un rimedio;

11. chiede la spiegabilità e la trasparenza degli algoritmi al fine di garantire che lo sviluppo, la diffusione e l'utilizzo di sistemi di IA per il settore giudiziario e delle attività di contrasto rispettino i diritti fondamentali e godano della fiducia dei cittadini, nonché al fine di garantire che i risultati generati dagli algoritmi di IA possano essere resi intelligibili per gli utenti e coloro che sono soggetti a tali sistemi, e che vi sia trasparenza riguardo ai dati di base e alle modalità con cui il sistema è giunto a una certa conclusione;

12. chiede una tracciabilità dei sistemi di IA che definisca le capacità e i limiti dei sistemi e tenga traccia dell'origine degli attributi che definiscono una decisione;

13. chiede che sia eseguita una valutazione di impatto obbligatoria sui diritti fondamentali prima dell'attuazione o della diffusione di qualsiasi sistema di IA destinato alle attività di contrasto o al settore giudiziario, al fine di valutare i potenziali rischi per i diritti fondamentali;

14. chiede un audit obbligatorio periodico di tutti i sistemi di IA utilizzati dalle autorità di

contrasto e dal potere giudiziario per testare e valutare i sistemi di algoritmi una volta che questi siano operativi, al fine di individuare, indagare, diagnosticare e rettificare eventuali effetti indesiderati e negativi;

15. chiede una moratoria sulla diffusione dei sistemi di riconoscimento facciale per le attività di contrasto, finché le norme tecniche non possano essere considerate pienamente conformi con i diritti fondamentali, i risultati ottenuti siano non discriminatori, e vi sia fiducia da parte del pubblico nella necessità e nella proporzionalità della diffusione di tali tecnologie;

16. chiede agli Stati membri una maggiore trasparenza generale e una comprensione globale dell'utilizzo delle applicazioni di IA nell'Unione, suddivisa per autorità di contrasto e autorità giudiziaria degli Stati membri, per tipo di strumento utilizzato, per tipo di reato cui si applicano e per società che fornisce gli strumenti;

17. incarica il suo Presidente di trasmettere la presente risoluzione al Consiglio e alla Commissione.

MOTIVAZIONE

L'intelligenza artificiale (IA) figura tra le tecnologie strategiche del XXI secolo, poiché genera notevoli benefici in termini di efficienza, precisione e comodità, apportando in tal modo un contributo positivo all'economia europea. Le applicazioni di IA hanno, tra le altre cose, migliorato le cure sanitarie, accresciuto l'efficienza dell'agricoltura, contribuito alla mitigazione e all'adattamento ai cambiamenti climatici nonché migliorato l'efficienza della produzione.

L'IA figura tra le principali priorità dell'attuale Commissione. La Presidente della Commissione Ursula von der Leyen ha annunciato nei suoi orientamenti politici un approccio europeo coordinato alle implicazioni umane ed etiche dell'IA e una riflessione volta a migliorare l'uso dei big data per favorire l'innovazione. L'adozione di un approccio a livello dell'UE alla questione dell'IA si è accompagnata ad una riflessione su come garantire la fiducia nelle tecnologie di IA e su come assicurarsi che l'IA non pregiudichi i diritti fondamentali dell'UE.

Tuttavia, l'IA è stata affrontata dal Parlamento europeo diversi anni prima che la Commissione decidesse di farne una delle sue principali priorità. Diverse risoluzioni in materia di big data, robotica e intelligenza artificiale, approvate dal Parlamento dal 2016, dimostrano l'importanza attribuita a questo argomento da parte del Parlamento. Le risoluzioni hanno esaminato le diverse implicazioni sollevate dall'IA e il modo in cui essa incide sul benessere, l"istruzione, la tecnologia, i diritti giuridici e fondamentali nonché l'industria in generale. Tali risoluzioni hanno sottolineato la necessità di adottare un approccio "antropocentrico" basato sul rispetto dei diritti fondamentali, segnatamente la Carta dell'UE e il quadro dell'UE di protezione dei dati.

Poiché l"IA è un "insieme di tecnologie che combina dati, algoritmi e potenza di calcolo", "i progressi compiuti nell'ambito del calcolo e la crescente disponibilità di dati sono pertanto fattori determinanti per l'attuale crescita dell'IA"[1]. La questione centrale è data dal fatto che l'IA si basa sulla raccolta, l'analisi e l'accumulo ricorrente di ingenti quantità di dati, compresi i dati personali, provenienti da una serie di fonti diverse, che sono oggetto di trattamenti automatizzati mediante algoritmi informatici e tecniche avanzate di trattamento dei dati. Tali tecniche utilizzano sia dati memorizzati sia in streaming, al fine di individuare determinate correlazioni, tendenze e modelli (analisi dei Big Data). I dati utilizzati per l'IA provengono non solo dagli stessi individui, ma le applicazioni di IA utilizzano principalmente dati provenienti dall'industria, dalle imprese e dal settore pubblico, che sono trattati per tutta una serie di scopi diversi. Sebbene i dati utilizzati dalle applicazioni di IA possano a volte essere dati non personali, molto spesso le attività di IA comportano il trattamento di dati personali, dato che tali attività conducono spesso a decisioni automatizzate che hanno un effetto diretto sugli individui. Alla luce di tali caratteristiche dell'IA, dobbiamo prestare particolare attenzione in tale settore al rispetto dei principi fondamentali della protezione dei dati e della vita privata.

L'IA offre grandi opportunità anche nel settore delle attività di contrasto e della giustizia penale, in particolare migliorando i metodi di lavoro delle autorità di contrasto e delle autorità giudiziarie e lottando in modo maggiormente efficace contro alcuni tipi di reati, in particolare nel settore dei reati finanziari, del riciclaggio di denaro e del finanziamento del terrorismo, nonché alcuni tipi di reati informatici. In tale settore, le applicazioni di IA includono per

[1] COM(2020) 65 final.

esempio le tecnologie di riconoscimento facciale, il riconoscimento automatizzato delle targhe, l'identificazione vocale, tecnologie di lettura labiale, analisi di segnali acustici (algoritmi di rilevamento di colpi di arma da fuoco), ricerca autonoma e analisi di database identificati, previsioni (polizia predittiva e analisi della scena del crimine), strumenti di rilevamento dei comportamenti, strumenti autonomi per identificare le frodi finanziarie e il finanziamento del terrorismo, monitoraggio dei social media (estrazione e raccolta di dati per l'estrazione di connessioni), numeri IMSI e sistemi di sorveglianza automatica che integrano diverse capacità di rilevamento (come il rilevamento cardiaco e le videocamere termiche). In ambito giudiziario, gli strumenti di IA possono essere utilizzati nel calcolo delle probabilità di recidiva e nelle decisioni di sospensione condizionale o di condanna.

Nonostante i benefici che essa apporta, l'IA comporta nel contempo una serie di rischi potenziali, quali processi decisionali opachi, vari tipi di discriminazione, intrusione nella vita privata, rischi per la protezione dei dati personali, per la dignità umana e la libertà di espressione e informazione. Tali rischi potenziali sono ancora più gravi nel settore delle attività di contrasto e della giustizia penale, in quanto possono incidere sulla presunzione di innocenza, sui diritti fondamentali per la libertà e la sicurezza dell'individuo e su un ricorso effettivo e un processo equo.

La presente relazione intende affrontare le questioni sollevate dall'uso dell'IA nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in materia penale. Pur prendendo atto delle opportunità e dei vantaggi potenziali offerti dall'IA, essa sottolinea anche i rischi e le implicazioni significative che essa può comportare.

La relazione sottolinea la necessità di rispettare appieno i diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, la legislazione dell'Unione in materia di tutela della vita privata e protezione dei dati, in particolare la direttiva (UE) 2016/680 ("direttiva polizia") e la necessità di rispettare diversi principi fondamentali nel ciclo di vita dell'IA, tra cui la spiegabilità e la trasparenza degli algoritmi, la tracciabilità, l'esecuzione di valutazioni di impatto obbligatorie sui diritti fondamentali prima dell'attuazione o della diffusione di qualsiasi sistema di IA e audit obbligatori. Tutti questi requisiti sono necessari non solo per garantire la legittimità dei sistemi di IA, ma anche per ottenere la fiducia delle persone per quanto riguarda l'utilizzo di tali sistemi da parte delle autorità di contrasto e delle autorità giudiziarie.

Infine il relatore chiede una moratoria sulla diffusione dei sistemi di riconoscimento facciale a fini di contrasto. L'attuale stato di avanzamento di tali tecnologie e il loro impatto significativo sui diritti fondamentali richiedono un dibattito sociale aperto e approfondito, al fine di esaminare le diverse problematiche sollevate e la giustificazione di una loro diffusione.