



---

**TESTI APPROVATI**

---

**P9\_TA(2021)0405**

**L'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale**

**Risoluzione del Parlamento europeo del 6 ottobre 2021 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, in particolare l'articolo 16,
- vista la Carta dei diritti fondamentali dell'Unione europea (la "Carta"), in particolare gli articoli 6, 7, 8, 11, 12, 13, 20, 21, 24 e 47,
- 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), e il relativo protocollo di modifica (Convenzione 108+),
- vista la Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi della Commissione europea per l'efficienza della giustizia (CEPEJ) del Consiglio d'Europa,
- vista la comunicazione della Commissione, dell'8 aprile 2019, dal titolo "Creare fiducia nell'intelligenza artificiale antropocentrica" (COM(2019)0168),
- visti gli orientamenti etici per un'intelligenza artificiale affidabile, pubblicati l'8 aprile 2019 dal gruppo di esperti ad alto livello della Commissione sull'intelligenza artificiale,
- visto il Libro bianco della Commissione del 19 febbraio 2020 dal titolo "Intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia" (COM(2020)0065),
- vista la comunicazione della Commissione del 19 febbraio 2020 dal titolo "Una strategia europea per i dati" (COM(2020)0066),
- 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)<sup>1</sup>,

- 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<sup>2</sup>,
- 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<sup>3</sup>,
- 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)<sup>4</sup>,
- 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<sup>5</sup>,
- vista la sua risoluzione del 19 giugno 2020 sulle proteste contro il razzismo a seguito della morte di George Floyd<sup>6</sup>,
- vista la sua risoluzione del 14 marzo 2017 sulle implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto<sup>7</sup>,
- vista l'audizione presso la commissione per le libertà civili, la giustizia e gli affari interni (LIBE) del 20 febbraio 2020 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale,
- visto il resoconto di missione a seguito della missione effettuata dalla commissione LIBE negli Stati Uniti nel febbraio 2020,
- visto l'articolo 54 del suo regolamento,
- visti i pareri della commissione per il mercato interno e la protezione dei consumatori e

---

<sup>1</sup> GU L 119 del 4.5.2016, pag. 1.

<sup>2</sup> GU L 119 del 4.5.2016, pag. 89.

<sup>3</sup> GU L 295 del 21.11.2018, pag. 39.

<sup>4</sup> GU L 201 del 31.7.2002, pag. 37.

<sup>5</sup> GU L 135 del 24.5.2016, pag. 53.

<sup>6</sup> GU C 362 dell'8.9.2021, pag. 63.

<sup>7</sup> GU C 263 del 25.7.2018, pag. 82.

della commissione giuridica,

- vista la relazione della commissione per le libertà civili, la giustizia e gli affari interni (A9-0232/2021),
- A. considerando che le tecnologie digitali in generale e la diffusione del trattamento e analisi dei dati dovuta all'intelligenza artificiale (IA) in particolare portano con sé promesse e rischi straordinari; che lo sviluppo dell'IA ha compiuto un notevole balzo in avanti in anni recenti che la rende una delle tecnologie strategiche del XXI secolo, con il potenziale di generare notevoli benefici in termini di efficienza, precisione e comodità e di apportare in tal modo un cambiamento positivo all'economia e alla società europea, ma comporta anche rischi enormi per i diritti fondamentali e le democrazie basate sullo Stato di diritto; 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, le capacità umane e la sicurezza;
- B. considerando che, nonostante i continui progressi compiuti in termini di velocità di elaborazione e capacità di memoria dei computer, attualmente non esistono ancora programmi che possano assicurare una flessibilità analoga a quella dell'essere umano in relazione a domini più ampi o a compiti che richiedono la comprensione di un contesto o un'analisi critica; che talune applicazioni di IA hanno raggiunto livelli prestazionali analoghi a quelli di esperti umani e professionisti nell'esecuzione di taluni compiti specifici (per esempio le tecnologie applicate al contesto giuridico) e possono offrire risultati con una velocità e una scala notevolmente superiori;
- C. considerando che alcuni paesi, compresi diversi Stati membri, fanno un maggiore uso delle applicazioni di IA o dei sistemi integrati di IA per le attività di contrasto e nel settore giudiziario rispetto ad altri, in parte a causa della mancanza di regolamentazione e delle differenze normative che consentono o impediscono l'uso dell'IA per talune finalità; che l'uso sempre più frequente dell'IA nel diritto penale si basa, in particolare, sulla promessa che ridurrà determinati tipi di reati e favorirà l'adozione di decisioni più obiettive; che tale promessa non sempre viene mantenuta;
- D. considerando che i diritti e le libertà fondamentali sanciti nella Carta dovrebbero essere rispettati per l'intera durata del ciclo di vita dell'IA e delle tecnologie correlate, in particolare durante la loro progettazione, sviluppo, diffusione e impiego, e applicarsi alle attività di contrasto in ogni circostanza;
- E. considerando che la tecnologia dell'intelligenza artificiale dovrebbe essere sviluppata in modo da mettere le persone al centro, essere degna della fiducia dei cittadini ed essere sempre al servizio dell'essere umano; che i sistemi di IA dovrebbero essere progettati in modo che possano essere sempre spenti da un operatore umano;
- F. considerando che i sistemi di IA devono essere concepiti per la protezione e il vantaggio di tutti i membri della società (tenendo conto, nella loro progettazione, delle popolazioni vulnerabili ed emarginate), essere non discriminatori, sicuri e che le relative decisioni devono essere spiegabili e trasparenti e rispettare l'autonomia umana e i diritti fondamentali per poter essere considerati affidabili, come previsto dagli Orientamenti etici del gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale;
- G. considerando che l'Unione, insieme agli Stati membri, ha l'importante responsabilità di

garantire che le decisioni relative al ciclo di vita e all'impiego delle applicazioni di IA nel settore giudiziario e delle attività di contrasto siano prese in modo trasparente, tutelino appieno i diritti fondamentali e, in particolare, non perpetuino le discriminazioni, le distorsioni o i pregiudizi laddove esistano; che le pertinenti decisioni politiche dovrebbero rispettare i principi di necessità e proporzionalità al fine di garantire la costituzionalità e un sistema di giustizia equo e umano;

- H. considerando che le applicazioni di IA possono offrire 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, finanziamento del terrorismo, abusi sessuali e sfruttamento sessuale nei confronti di minori online nonché alcuni tipi di reati informatici, contribuendo in tal modo alla sicurezza e incolumità dei cittadini europei, pur comportando, al contempo, rischi significativi per i diritti fondamentali dei cittadini; che l'applicazione generalizzata dell'IA al fine della sorveglianza di massa sarebbe sproporzionata;
- I. considerando che lo sviluppo e il funzionamento dei sistemi di IA per le autorità di polizia e le autorità giudiziarie richiede il contributo di molteplici persone, organizzazioni, componenti meccanici, algoritmi software e utenti umani in ambienti spesso complessi e problematici; che le applicazioni di IA per le attività di contrasto e in ambito giudiziario sono in diverse fasi di sviluppo, passando dalla concettualizzazione alla realizzazione o valutazione di prototipi fino all'impiego post-approvazione; che in futuro vi potranno essere nuove possibilità di impiego in virtù della maturazione delle tecnologie a seguito della continua ricerca scientifica in tutto il mondo;
- J. 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; che le norme regolamentari in questo ambito dovrebbero sempre sostenere la responsabilità umana e che il loro primo e principale scopo deve innanzi tutto essere la prevenzione di qualunque effetto negativo;
- K. considerando che in ultima analisi è responsabilità degli Stati membri garantire il pieno rispetto dei diritti fondamentali quando i sistemi di IA vengono utilizzati nel settore delle attività di contrasto e nel settore giudiziario;
- L. considerando che la relazione tra la protezione dei diritti fondamentali e un'attività di contrasto efficace deve sempre essere un elemento essenziale nelle discussioni sull'opportunità e le modalità di utilizzo dei sistemi di IA nell'ambito delle attività di contrasto, in cui le decisioni potrebbero avere conseguenze durature sulla vita e la libertà degli individui; che ciò riveste particolare importanza in quanto l'IA può potenzialmente diventare parte integrante del nostro ecosistema di giustizia penale fornendo analisi investigative e assistenza;
- M. considerando che l'IA è utilizzata dalle autorità di contrasto in applicazioni quali le tecnologie di riconoscimento facciale, ad esempio per la ricerca in database di sospetti e l'identificazione delle vittime della tratta di esseri umani o di sfruttamento sessuale e abusi nei confronti di minori, 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 avanzati di autopsia virtuale per contribuire a determinare la causa di morte, 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) 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, unitamente ad altre applicazioni potenziali o future della tecnologia dell'IA nelle attività di contrasto, possono presentare gradi molto diversi di affidabilità e precisione e di impatto sulla protezione dei diritti fondamentali e sulle dinamiche dei sistemi di giustizia penale; che molti di questi strumenti sono utilizzati in paesi non UE ma sarebbero illegali ai sensi dell'acquis dell'Unione in materia di protezione dei dati e della relativa giurisprudenza; che la diffusione di routine degli algoritmi, anche con un tasso limitato di falsi positivi, può generare falsi allarmi in numero decisamente superiore agli allarmi corretti;

- N. considerando che gli strumenti e le applicazioni di IA sono altresì utilizzati dal potere giudiziario in diversi paesi in tutto il mondo, per esempio a sostegno delle decisioni sulla custodia cautelare, nell'irrogazione delle pene, nel calcolo delle probabilità di recidiva e nelle decisioni di sospensione condizionale, nella risoluzione delle controversie online, nella gestione della giurisprudenza e nella garanzia di un accesso facilitato al diritto; che ciò ha causato distorsioni e ridotto le opportunità per le persone di colore e le persone appartenenti ad altre minoranze; che, al momento, nell'UE, salvo qualche Stato membro, il loro utilizzo è limitato prevalentemente all'ambito civile;
- O. considerando che l'utilizzo dell'IA nelle attività di contrasto comporta una serie di rischi potenzialmente elevati, e in alcuni casi inaccettabili, per la protezione dei diritti fondamentali degli individui, quali processi decisionali opachi, vari tipi di discriminazione ed errori intrinseci nell'algoritmo di base che possono essere aggravati da meccanismi di feedback, nonché rischi per la protezione della vita privata e dei dati personali, per la protezione della libertà di espressione e informazione, la presunzione di innocenza, il diritto a un ricorso efficace e a un processo equo nonché rischi per la libertà e la sicurezza degli individui;
- P. considerando che i sistemi di IA utilizzati dalle autorità di contrasto e giudiziarie sono anch'essi vulnerabili agli attacchi ai sistemi informatici basati sull'IA o all'avvelenamento dei dati, dove una serie di dati errati è inserita volutamente per generare risultati falsati; 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;
- Q. considerando che la diffusione dell'IA nel settore delle attività di contrasto e nel settore giudiziario non dovrebbe essere considerata una mera questione di realizzabilità tecnica ma piuttosto una decisione politica riguardante la progettazione e gli obiettivi dei sistemi di attività di contrasto e di giustizia penale; che il moderno diritto penale si basa sull'idea che le autorità reagiscono a un reato dopo che è stato commesso, senza supporre che le persone siano pericolose e debbano essere sorvegliate costantemente per prevenire possibili illeciti; che le tecniche di sorveglianza basate sull'IA mettono in dubbio profondamente tale approccio e impongono ai legislatori in tutto il mondo di valutare con attenzione le conseguenze derivanti dalla diffusione delle tecnologie che riducono il ruolo dell'essere umano nelle attività di contrasto e di giudizio;
- 1. ribadisce che, poiché il trattamento di grandi quantità di dati personali 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; rammenta, pertanto, che l'UE ha già definito norme sulla protezione dei dati per l'attività di contrasto, che costituiscono la base per qualunque futura regolamentazione dell'IA per l'impiego nelle attività di contrasto e nel settore giudiziario; ricorda che il trattamento dei dati personali dovrebbe essere lecito e corretto, le finalità del trattamento dovrebbero essere specificate, esplicite e legittime, il trattamento dovrebbe essere adeguato, pertinente e non eccessivo rispetto alle finalità perseguite, i dati dovrebbero essere accurati e aggiornati e i dati imprecisi dovrebbero, salvo restrizioni, essere corretti o cancellati e non dovrebbero essere conservati più a lungo del necessario, dovrebbero essere stabiliti limiti temporali chiari e appropriati per la cancellazione o per la revisione periodica della necessità di conservazione di tali dati e dovrebbero essere trattati in modo sicuro; sottolinea che dovrebbe essere impedita la possibile identificazione degli individui da parte di un'applicazione IA sulla base di dati precedentemente anonimizzati;

2. ribadisce che tutte le soluzioni di IA per le attività di contrasto e il settore giudiziario devono inoltre rispettare appieno i principi di dignità umana, non discriminazione, libertà di movimento, presunzione di innocenza e diritto di difesa, compreso il diritto di non rispondere, libertà di espressione e informazione, libertà di riunione e associazione, uguaglianza dinanzi alla legge, principio dell'eguaglianza delle armi e diritto a un ricorso effettivo e a un processo equo, conformemente alla Carta e alla Convenzione europea dei diritti dell'uomo; sottolinea che l'utilizzo dell'IA deve essere proibito se incompatibile con i diritti fondamentali;
3. riconosce che la velocità con cui sono sviluppate le applicazioni di IA nel mondo non consente di redigere elenchi esaustivi delle applicazioni e richiede, pertanto, un modello di gestione chiaro e coerente che garantisca sia il rispetto dei diritti fondamentali degli individui che la chiarezza giuridica per gli sviluppatori, in considerazione della costante evoluzione tecnologica; ritiene, tuttavia, che, considerati il ruolo e le responsabilità delle autorità di polizia e giudiziarie e dell'impatto delle decisioni prese dalle stesse ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, l'impiego delle applicazioni di IA deve essere classificato come ad alto rischio nei casi in cui esso possa influire in maniera significativa sulla vita delle persone;
4. ritiene, a tale proposito, che qualsiasi strumento di IA sviluppato o utilizzato dalle autorità di contrasto o giudiziarie dovrebbe come minimo essere sicuro, solido e adatto allo scopo previsto, rispettare i principi di equità, minimizzazione dei dati, responsabilità, trasparenza, non discriminazione e spiegabilità, e il suo sviluppo, la sua diffusione e il suo utilizzo dovrebbero essere soggetti a una valutazione dei rischi e a una rigorosa verifica della necessità e della proporzionalità, e le relative salvaguardie dovrebbero essere proporzionate ai rischi individuati; sottolinea che la fiducia tra i cittadini nell'utilizzo dell'IA sviluppata, diffusa e utilizzata nell'Unione dipende dal pieno rispetto di tali criteri;
5. riconosce il contributo positivo di determinati tipi di applicazioni di IA al lavoro delle autorità di contrasto e giudiziarie in tutta l'Unione; sottolinea, ad esempio, il miglioramento nella gestione della giurisprudenza ottenuto con gli strumenti che garantiscono ulteriori opzioni di ricerca; ritiene che vi sia una serie di altri utilizzi

potenziali per l'IA da parte delle autorità di contrasto e giudiziarie che potrebbe essere esaminata, tenendo in considerazione i cinque principi della Carta etica sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambienti connessi, adottata dalla CEPEJ e prestando particolare attenzione agli "utilizzi da esaminare con le più estreme riserve" identificati dalla CEPEJ;

6. sottolinea che qualsiasi tecnologia può essere utilizzata per altre finalità e chiede, pertanto, un controllo democratico rigoroso e una supervisione indipendente per qualunque tecnologia basata sull'IA utilizzata da parte delle autorità di contrasto e giudiziarie, in particolare quella che può essere destinata alla sorveglianza o alla profilazione di massa; prende atto, pertanto, con grande preoccupazione del potenziale di determinate tecnologie di IA impiegate nel settore delle attività di contrasto per la sorveglianza di massa; sottolinea l'esigenza giuridica di prevenire la sorveglianza di massa tramite le tecnologie di IA, che per definizione non corrisponde ai principi di necessità e proporzionalità, e di vietare l'uso delle applicazioni che potrebbero risultare in tale sorveglianza;
7. sottolinea che l'approccio adottato da alcuni paesi terzi per quanto riguarda lo sviluppo, la diffusione e l'utilizzo delle tecnologie di sorveglianza di massa interferisce in modo sproporzionato con i diritti fondamentali e non può pertanto essere seguito dall'UE; sottolinea, pertanto, che anche le salvaguardie contro l'uso improprio delle tecnologie di IA da parte delle autorità di contrasto e giudiziarie devono essere disciplinate in modo uniforme in tutta l'Unione;
8. sottolinea che l'uso di applicazioni basate sull'intelligenza artificiale come l'apprendimento automatico, compresi gli algoritmi sui quali sono basate tali applicazioni, 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; ricorda che il risultato fornito dalle applicazioni di IA è necessariamente influenzato dalla qualità dei dati utilizzati e che tali distorsioni intrinseche sono destinate ad aumentare gradualmente e quindi a perpetuare e amplificare le discriminazioni esistenti, in particolare nei confronti delle persone che appartengono a determinate minoranze etniche o comunità razziali;
9. sottolinea che molte tecnologie di identificazione basate su algoritmi attualmente in uso commettono un numero sproporzionato di errori di identificazione e di classificazione, danneggiando le persone che appartengono a determinati gruppi razziali o etnici, le persone LGBTI, i bambini, gli anziani e le donne; ricorda che gli individui non hanno soltanto il diritto a essere identificati correttamente ma anche di non essere identificati, salvo quando richiesto per legge per interessi pubblici imperativi e legittimi; sottolinea che le previsioni di IA basate sulle caratteristiche di un gruppo specifico di persone finiscono con l'amplificare e riprodurre le forme esistenti di discriminazione; ritiene che sarebbe opportuno compiere grandi sforzi per evitare la discriminazione e le distorsioni automatizzate; chiede ulteriori misure di salvaguardia rigorose nel caso in cui i sistemi di IA per le attività di contrasto o il settore giudiziario siano usati sui minori o in relazione ad essi;
10. sottolinea l'asimmetria di potere tra coloro che impiegano le tecnologie di intelligenza artificiale e coloro che ne sono soggetti; sottolinea che è imperativo che l'utilizzo degli strumenti di IA da parte delle autorità di contrasto e giudiziarie non diventi un fattore di

disuguaglianza, frattura sociale o esclusione; sottolinea l'impatto dell'impiego degli strumenti di IA sul diritto alla difesa degli indagati, la difficoltà di ottenere informazioni significative sul loro funzionamento e la conseguente difficoltà nel confutarne i risultati in tribunale, in particolare per gli individui sottoposti a indagini;

11. prende atto dei rischi associati in particolare alle fughe di dati, alle violazioni della sicurezza dei dati e all'accesso non autorizzato ai dati personali e ad altre informazioni riguardanti, ad esempio, le indagini penali o le cause giudiziarie elaborate dai sistemi di IA; sottolinea che gli aspetti legati alla sicurezza e alla protezione dei sistemi di IA utilizzati nelle attività di contrasto e dalle attività giudiziarie 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; sottolinea l'importanza della sicurezza sin dalla progettazione nonché di un controllo umano specifico prima di utilizzare determinate applicazioni critiche e pertanto invita le autorità di contrasto e giudiziarie a utilizzare esclusivamente applicazioni di IA che rispettino il principio della tutela della vita privata e della protezione dei dati sin dalla progettazione onde evitare la funzione di scorrimento;
12. sottolinea che nessun sistema di IA impiegato dalle autorità di contrasto o giudiziarie dovrebbe poter nuocere all'integrità fisica degli esseri umani né attribuire diritti o imporre obblighi giuridici agli individui;
13. prende atto delle sfide relative alla corretta individuazione delle responsabilità giuridica e imputabilità per i potenziali danni, data la complessità dello sviluppo e del funzionamento dei sistemi di IA; ritiene sia necessario istituire un regime chiaro ed equo per attribuire la responsabilità giuridica e imputabilità delle potenziali conseguenze negative prodotte da tali tecnologie digitali avanzate; sottolinea tuttavia che il primo e principale scopo deve innanzi tutto essere la prevenzione di tali conseguenze; invita, pertanto, ad applicare con coerenza il principio di precauzione per tutte le applicazioni di IA nel contesto delle attività di contrasto; sottolinea che la responsabilità giuridica e l'imputabilità devono sempre ricadere su una persona fisica o giuridica, che deve sempre essere identificata per le decisioni assunte con il sostegno dell'IA; sottolinea, pertanto, l'esigenza di assicurare la trasparenza delle strutture aziendali che producono e gestiscono i sistemi di IA;
14. ritiene essenziale, per l'efficacia dell'esercizio dei diritti alla difesa e per la trasparenza dei sistemi di giustizia penale nazionali, che uno specifico quadro giuridico chiaro e preciso disciplini le condizioni, le modalità e le conseguenze dell'utilizzo degli strumenti di IA nei settori dell'attività di contrasto e giudiziario, nonché i diritti delle persone interessate, e procedure efficaci e facilmente accessibili di reclamo e di ricorso, compreso il ricorso per via giudiziaria; sottolinea il diritto delle parti di un procedimento penale di accedere al processo di raccolta dei dati e quello relativo alle valutazioni correlate eseguite da o ottenute mediante l'uso delle applicazioni di IA; sottolinea la necessità che le autorità esecutive coinvolte nella cooperazione giudiziaria valutino, quando esaminano una richiesta di estradizione (o di consegna) verso un altro Stato membro o paese non-UE, se l'utilizzo degli strumenti di IA nel paese richiedente possa indebolire manifestamente il diritto fondamentale a un processo equo; invita la Commissione a redigere orientamenti su come condurre una valutazione nel contesto della cooperazione giudiziaria in ambito penale; insiste sul fatto che gli Stati membri, ai sensi delle leggi applicabili, dovrebbero garantire che gli individui siano informati quando sottoposti all'utilizzo delle applicazioni di IA da parte delle autorità di contrasto



o giudiziarie;

15. osserva che se gli esseri umani fanno affidamento unicamente sui dati, i profili e le raccomandazioni generati dalle macchine, non saranno in grado di condurre una valutazione indipendente; evidenzia le ripercussioni negative potenzialmente gravi, in particolare nel settore delle attività di contrasto e della giustizia, qualora le persone ripongano eccessiva fiducia nella natura apparentemente oggettiva e scientifica degli strumenti di IA e non considerino la possibilità che tali strumenti conducano a risultati errati, incompleti, non pertinenti o discriminatori; evidenzia che dovrebbe essere evitata l'eccessiva fiducia nei risultati forniti dai sistemi di IA e sottolinea l'esigenza che le autorità acquisiscano conoscenze e dimestichezza per mettere in dubbio o respingere una raccomandazione algoritmica; ritiene importante avere aspettative realistiche rispetto a tali soluzioni tecnologiche e non promettere soluzioni perfette per l'attività di contrasto e l'individuazione di tutti i reati commessi;
16. sottolinea che, nei contesti giudiziari e di contrasto, la decisione che produce effetti giuridici o analoghi deve sempre essere presa da un essere umano, il quale possa essere ritenuto responsabile per le decisioni adottate; ritiene che le persone soggette a sistemi basati sull'IA debbano avere la possibilità di accedere a un mezzo di ricorso; ricorda che, ai sensi del diritto dell'UE, una persona ha il diritto di non essere sottoposta a una decisione che produca effetti giuridici o abbia effetti significativi nei suoi confronti fondata esclusivamente su un trattamento automatizzato dei dati; sottolinea inoltre che il processo decisionale automatizzato non si deve basare su categorie particolari di dati personali, a meno che non siano in vigore misure adeguate a salvaguardia dei diritti, delle libertà e dei legittimi interessi dell'interessato; sottolinea che il diritto dell'Unione proibisce la profilazione che risulti nella discriminazione nei confronti delle persone fisiche sulla base di categorie speciali di dati personali; sottolinea che le decisioni nel settore delle attività di contrasto hanno quasi sempre un effetto giuridico sulla persona interessata, in virtù della natura esecutiva delle autorità di contrasto e delle loro azioni; osserva che l'uso dell'IA può influire sulle decisioni umane e avere un impatto su tutte le fasi dei procedimenti penali; è, pertanto, del parere che le autorità che utilizzano i sistemi di IA debbano osservare norme giuridiche estremamente rigorose e garantire l'intervento dell'essere umano, in particolare quando si analizzano i dati derivanti da tali sistemi; chiede pertanto che siano mantenute la competenza esclusiva dei giudici e l'adozione di decisioni caso per caso; chiede un divieto sull'uso dell'IA e delle relative tecnologie per l'emanazione delle decisioni giudiziarie;
17. chiede la spiegabilità, la trasparenza, la tracciabilità e la verifica degli algoritmi quali elementi necessari della vigilanza 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; sottolinea che, al fine di assicurare la trasparenza tecnica, l'affidabilità e la precisione, dovrebbe essere consentito l'acquisto da parte delle autorità di contrasto e giudiziarie nell'Unione esclusivamente di strumenti e sistemi con algoritmi e logica che possano essere sottoposti a revisione e siano accessibili almeno per le forze di polizia, le autorità giudiziarie e per enti indipendenti, per consentirne la valutazione, la revisione e il controllo, e che non siano sistemi chiusi e contrassegnati come proprietari da parte dei fornitori; sottolinea inoltre che la documentazione dovrebbe essere fornita in un

linguaggio chiaramente intellegibile sulla natura del servizio, gli strumenti sviluppati, le prestazioni e le condizioni in cui possono funzionare e i rischi che potrebbero comportare; Invita pertanto le autorità giudiziarie e di contrasto a garantire una trasparenza proattiva e piena sulle imprese private che forniscono loro i sistemi di IA per finalità di contrasto e giudiziarie; raccomanda l'impiego di software open source ove possibile;

18. esorta le autorità di contrasto e giudiziarie a identificare e valutare le aree in cui potrebbero risultare vantaggiose soluzioni di IA mirate e a scambiare pratiche migliori sulla diffusione dell'IA; chiede l'adozione da parte degli Stati membri e delle agenzie dell'Unione di una procedura di appalto appropriata per i sistemi di IA ove utilizzati per le attività di contrasto o in ambito giudiziario, al fine di assicurare il rispetto dei diritti fondamentali, e della legislazione applicabile, anche per garantire che la documentazione del software e gli algoritmi siano disponibili e accessibili per la revisione da parte delle autorità di vigilanza competenti; chiede, in particolare, norme vincolanti che impongano la divulgazione in merito a partenariati pubblico-privati, contratti e acquisizioni e delle relative finalità; sottolinea l'esigenza di fornire alle autorità le risorse necessarie, nonché di assicurare loro la competenza richiesta per garantire il pieno rispetto dei requisiti etici, giuridici e tecnici associati alla diffusione dell'IA;
19. chiede una tracciabilità dei sistemi di IA e del processo decisionale che definisca le funzioni, le capacità e i limiti dei sistemi e tenga traccia dell'origine degli attributi che definiscono una decisione mediante obblighi in materia di documentazione; sottolinea l'importanza di conservare la documentazione completa sui dati di addestramento, sul contesto, sulle finalità, sulla precisione e sugli effetti secondari nonché sull'elaborazione da parte dei creatori e degli sviluppatori degli algoritmi e sul rispetto dei diritti fondamentali; sottolinea che deve sempre essere possibile ridurre i calcoli di un sistema di IA a una forma comprensibile per l'essere umano;
20. 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; rammenta che la valutazione preliminare d'impatto sulla protezione dei dati è obbligatoria per qualunque tipo di trattamento, in particolare per l'uso di nuove tecnologie che potrebbero comportare rischi elevati per i diritti e le libertà delle persone fisiche, ed è del parere che questo sia il caso della maggior parte delle tecnologie dell'intelligenza artificiale nel settore delle attività di contrasto e nel settore giudiziario; sottolinea la competenza delle autorità preposte alla protezione dei dati e delle agenzie per i diritti fondamentali per la valutazione di tali sistemi; sottolinea che le valutazioni di impatto sui diritti fondamentali dovrebbero essere condotte quanto più apertamente possibile e con la partecipazione attiva della società civile; chiede che le valutazioni di impatto definiscano in maniera chiara le necessarie salvaguardie per far fronte ai rischi individuati e siano rese disponibili al pubblico, nella massima misura possibile, prima di diffondere i sistemi di IA;
21. sottolinea che soltanto un'efficace governance dell'IA a livello europeo con una valutazione indipendente consente la necessaria attuazione operativa dei principi riguardanti i diritti fondamentali; chiede un audit obbligatorio periodico di tutti i sistemi di IA utilizzati dalle autorità di contrasto e dal potere giudiziario nei casi in cui possa influire in maniera significativa sulla vita delle persone, da parte di un'autorità

indipendente, per testare e valutare i sistemi di algoritmi, il contesto, le finalità, la precisione, le prestazioni e la portata una volta che questi siano operativi, al fine di individuare, indagare, diagnosticare e rettificare eventuali effetti indesiderati e negativi e assicurare che i sistemi di IA funzionino come previsto; chiede, a tal fine, un quadro istituzionale chiaro, compresa una sorveglianza della regolamentazione e un controllo di vigilanza appropriati, al fine di garantirne la completa attuazione e garantire un dibattito democratico pienamente informato sulla necessità e proporzionalità dell'IA nel settore della giustizia penale; sottolinea che i risultati di questi audit dovrebbero essere resi disponibili in registri pubblici in modo che i cittadini sappiano quali sistemi di IA sono utilizzati e quali misure sono adottate per rimediare alla violazione dei diritti fondamentali;

22. sottolinea che gli insiemi di dati e i sistemi algoritmici utilizzati per condurre classificazioni, valutazioni e previsioni nelle diverse fasi del trattamento dei dati per lo sviluppo dell'IA e delle relative tecnologie potrebbero anche risultare in un trattamento differenziale e in una discriminazione sia diretta che indiretta di gruppi di persone, in particolare poiché i dati utilizzati per formare gli algoritmi di polizia predittiva rispecchiano le attuali priorità di sorveglianza e, di conseguenza, potrebbero finire con il riprodurre e amplificare le discriminazioni esistenti; sottolinea, pertanto, che le tecnologie di IA, in particolare se diffuse per l'uso nelle attività di contrasto e nel settore giudiziario, richiedono una ricerca e un contributo interdisciplinari, anche da ambiti quali gli studi scientifici e tecnologici, gli studi critici sulla razza, gli studi sulla disabilità e altre discipline in sintonia con il contesto sociale, comprese le modalità di costruzione delle differenze, il lavoro di classificazione e le sue conseguenze; sottolinea pertanto la necessità di investire sistematicamente nell'integrazione di tali discipline nello studio e nella ricerca sull'IA a tutti i livelli; sottolinea inoltre che è importante che i team che progettano, sviluppano, testano, eseguono la manutenzione, diffondono e forniscono tali sistemi di IA per le attività di contrasto e giudiziarie rispecchino, ove possibile, la diversità della società in generale, quale strumento non tecnico per ridurre il rischio di discriminazioni;
23. sottolinea inoltre che l'affidabilità e la responsabilità adeguate richiedono una significativa formazione specializzata per quanto riguarda le disposizioni etiche, i potenziali pericoli, le limitazioni e l'uso appropriato della tecnologia dell'intelligenza artificiale, in particolare per il personale di polizia e giudiziario; sottolinea che una formazione e qualifiche professionali adeguate dovrebbero garantire che i decisori siano formati in merito alle potenziali distorsioni, dal momento che le serie di dati possono basarsi su dati discriminatori e pregiudiziali; sostiene la promozione di iniziative di sensibilizzazione e formazione volte ad assicurare che le persone che operano nell'ambito delle attività di contrasto e giudiziario siano consapevoli e comprendano i limiti, le possibilità e i rischi associati all'utilizzo dei sistemi di IA, compreso il rischio di distorsioni automatiche; ricorda che l'inclusione nelle serie di dati in materia di addestramento dei sistemi di IA di casi di razzismo da parte delle forze di polizia nell'adempimento dei propri doveri comporterà inevitabilmente distorsioni di natura razzista nei risultati, nei punteggi e nelle raccomandazioni basati sull'IA; ribadisce pertanto il suo invito agli Stati membri affinché promuovano politiche contro la discriminazione ed elaborino piani d'azione nazionali contro il razzismo nel settore delle attività di polizia e nel sistema giudiziario;
24. osserva che la polizia predittiva è tra le applicazioni di IA utilizzate nell'ambito delle attività di contrasto ma avverte che se da un lato la polizia predittiva può analizzare gli

insiemi di dati forniti per l'identificazione di modelli e correlazioni, essa non può dare una risposta alla questione della causalità, non può fare previsioni affidabili sui comportamenti degli individui e pertanto non può costituire l'unica base per un intervento; sottolinea che diverse città degli Stati Uniti hanno interrotto l'uso dei sistemi di polizia predittiva in seguito agli audit; ricorda che durante la missione della commissione LIBE negli Stati Uniti nel febbraio 2020, i membri sono stati informati dai dipartimenti di polizia di New York City e Cambridge, Massachusetts, che avevano eliminato gradualmente i loro programmi di polizia predittiva a causa della loro inefficacia, dell'impatto discriminatorio e dell'insuccesso pratico ed erano tornati a sistemi di polizia di quartiere; osserva che ciò ha portato a una riduzione del tasso di criminalità; si oppone, pertanto, all'utilizzo dell'IA da parte delle autorità di contrasto per fare previsioni sui comportamenti degli individui o di gruppi sulla base di dati storici e condotte precedenti, dell'appartenenza a un gruppo, l'ubicazione o qualunque altra caratteristica al fine di identificare le persone che potrebbero commettere un reato;

25. prende atto dei diversi tipi di utilizzo del riconoscimento facciale, come, ma non solo, la verifica/autenticazione (abbinamento di un volto dal vivo a una foto in un documento di identità, per es. i bordi intelligenti), l'identificazione (ricerca della corrispondenza tra una fotografia e un database di immagini) e la rilevazione (individuazione di volti in tempo reale da fonti quali la televisione a circuito chiuso e ricerca di una corrispondenza con i database, per es. sorveglianza in tempo reale), ciascuna delle quali ha diverse implicazioni per la protezione dei diritti fondamentali; è fermamente convinto che la diffusione dei sistemi di riconoscimento facciale da parte delle autorità di contrasto dovrebbe essere limitata a finalità chiaramente giustificate nel pieno rispetto dei principi di proporzionalità e di necessità e della legge vigente; ribadisce che, come minimo, l'utilizzo della tecnologia di riconoscimento facciale deve essere conforme ai requisiti di minimizzazione dei dati, precisione dei dati, limite di conservazione, sicurezza e affidabilità dei dati, ed essere lecito, equo e trasparente e perseguire una finalità specifica, esplicita e legittima chiaramente definita nel diritto degli Stati membri o dell'Unione; è del parere che i sistemi di verifica e autenticazione possano continuare ad essere diffusi e utilizzati con successo solo se i relativi effetti indesiderati saranno mitigati e se i criteri di cui sopra saranno soddisfatti;
26. chiede, inoltre, un divieto permanente dell'utilizzo dei sistemi di analisi e/o riconoscimento automatici negli spazi pubblici di altre caratteristiche umane quali l'andatura, le impronte digitali, il DNA, la voce e altri segnali biometrici e comportamentali;
27. chiede, tuttavia, una moratoria sulla diffusione dei sistemi di riconoscimento facciale per le attività di contrasto con funzione di identificazione, a meno che non siano usate strettamente ai fini dell'identificazione delle vittime di reati, finché le norme tecniche non possano essere considerate pienamente conformi con i diritti fondamentali, i risultati ottenuti siano privi di distorsioni e non discriminatori, il quadro giuridico fornisca salvaguardie rigorose contro l'utilizzo improprio e un attento controllo democratico e adeguata vigilanza, e vi sia la prova empirica della necessità e proporzionalità della diffusione di tali tecnologie; osserva che i sistemi non dovrebbero essere utilizzati o diffusi nei casi in cui i criteri di cui sopra non siano soddisfatti;
28. esprime profonda preoccupazione per l'utilizzo di database privati di riconoscimento facciale da parte delle autorità di contrasto e dei servizi di intelligence, come Clearview AI, una banca dati di oltre tre miliardi di immagini raccolte illegalmente dai social

network e da altre fonti Internet, comprese immagini di cittadini dell'Unione; invita gli Stati membri a obbligare le autorità di contrasto a indicare se stanno utilizzando la tecnologia Clearview AI o tecnologie equivalenti di altri fornitori; rammenta il parere del comitato europeo per la protezione dei dati secondo cui l'utilizzo di un servizio quale Clearview AI da parte delle autorità di contrasto nell'Unione europea non sarebbe probabilmente coerente con il regime di protezione dei dati dell'UE; chiede un divieto sull'utilizzo di database privati di riconoscimento facciale per le attività di contrasto;

29. prende atto dello studio di fattibilità della Commissione sui possibili cambiamenti della decisione di Prüm<sup>1</sup>, comprese le immagini facciali; prende atto delle ricerche precedenti secondo cui nessun metodo di identificazione nuovo, ad esempio il riconoscimento facciale o dell'iride, sarebbe affidabile in un contesto forense quanto il DNA o le impronte digitali; rammenta alla Commissione che qualsiasi proposta legislativa deve basarsi su fatti comprovati e rispettare il principio di proporzionalità; esorta la Commissione a non estendere il quadro delle decisioni di Prüm a meno che non vi siano solide prove scientifiche dell'affidabilità del riconoscimento facciale in un contesto forense rispetto al DNA o alle impronte digitali, dopo aver condotto una valutazione d'impatto completa e tenendo conto delle raccomandazioni del Garante europeo della protezione dei dati (GEPD) e del comitato europeo per la protezione dei dati;
30. sottolinea che l'uso dei dati biometrici è correlato in senso più ampio al principio di dignità umana, che è la base di tutti i diritti fondamentali garantiti dalla Carta; ritiene che l'utilizzo e la raccolta di dati biometrici per finalità di identificazione a distanza, ad esempio attraverso il riconoscimento facciale in luoghi pubblici, nonché i cancelli per il controllo automatizzato alle frontiere utilizzati per i controlli negli aeroporti, possano presentare rischi specifici per i diritti fondamentali, le cui implicazioni potrebbero variare notevolmente a seconda delle finalità, del contesto e dell'ambito di impiego; sottolinea, inoltre, la controversa validità scientifica della tecnologia di riconoscimento utilizzata, come le fotocamere che rilevano i movimenti degli occhi e le variazioni delle dimensioni della pupilla, nel contesto delle attività di contrasto; è del parere che l'uso dell'identificazione biometrica nel contesto delle attività di contrasto e giudiziarie dovrebbe sempre essere considerato ad "alto rischio" e pertanto soggetto a ulteriori requisiti, come previsto dalle raccomandazioni del gruppo di esperti di alto livello della Commissione sull'IA;
31. esprime profonda preoccupazione per i progetti di ricerca finanziati nell'ambito di Orizzonte 2020 che diffondono l'intelligenza artificiale alle frontiere esterne, come il progetto iBorderCtrl, un "sistema intelligente di rilevamento delle menzogne" che permette di tracciare il profilo dei viaggiatori sulla base di un'intervista computerizzata effettuata con la webcam del passeggero prima del viaggio, e un'analisi basata sull'intelligenza artificiale di 38 microgesti, testata in Ungheria, Lettonia e Grecia; invita, pertanto, la Commissione, tramite strumenti legislativi e non legislativi e, ove necessario, mediante procedure d'infrazione, a introdurre il divieto di trattamento dei dati biometrici, comprese le immagini facciali, per finalità di applicazione della legge, tale da determinare sorveglianza di massa negli spazi accessibili al pubblico; invita, inoltre, la Commissione a interrompere il finanziamento della ricerca o diffusione della biometrica o di programmi che potrebbero portare alla sorveglianza di massa

---

<sup>1</sup> Decisione 2008/615/GAI del Consiglio, del 23 giugno 2008, sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera (GU L 210 del 6.8.2008, pag. 1).

indiscriminata nei luoghi pubblici; sottolinea, in questo contesto, che andrebbe prestata particolare attenzione e dovrebbe essere applicato un quadro rigoroso all'utilizzo dei droni nelle operazioni di polizia;

32. appoggia le raccomandazioni del gruppo di esperti di alto livello sull'IA della Commissione a favore del divieto del sistema di "scoring" su larga scala dei cittadini; osserva che qualsiasi forma di "citizen scoring" normativo su larga scala da parte delle autorità pubbliche, in particolare nel settore delle attività di contrasto e in ambito giudiziario, conduce alla perdita di autonomia, indebolisce il principio di non discriminazione e non può essere considerato conforme ai diritti fondamentali, in particolare la dignità umana, come sancita dal diritto dell'Unione;
33. chiede una maggiore trasparenza generale per dar vita a una comprensione globale circa l'utilizzo delle applicazioni di IA nell'Unione; invita gli Stati membri a fornire informazioni complete sugli strumenti utilizzati dalle proprie autorità di contrasto e giudiziarie, sulle tipologie di strumenti utilizzati, sulle finalità per cui sono utilizzati, sui tipi di reati cui si applicano e i nomi delle società o organizzazioni che hanno sviluppato tali strumenti; invita anche le autorità di contrasto e giudiziarie a informare il pubblico e ad assicurare una trasparenza sufficiente in merito all'utilizzo dell'intelligenza artificiale e delle relative tecnologie nell'esercizio dei loro poteri, compresa la pubblicazione dei tassi di falsi positivi e falsi negativi della tecnologia in questione; chiede alla Commissione di redigere e aggiornare le informazioni in un'unica sede; invita la Commissione a pubblicare e aggiornare informazioni sull'utilizzo dell'IA da parte delle agenzie dell'Unione incaricate delle attività di contrasto e giudiziarie; invita il comitato europeo per la protezione dei dati a valutare la legittimità delle tecnologie e applicazioni di IA utilizzate dalle autorità di contrasto e giudiziarie;
34. rammenta che le applicazioni di IA, comprese quelle utilizzate nel contesto delle attività di contrasto e nel settore giudiziario, sono in rapido sviluppo a livello globale; esorta tutti i portatori di interessi europei, compresi gli Stati membri e la Commissione, a garantire, attraverso la cooperazione internazionale, il coinvolgimento di partner extra-UE al fine di elevare gli standard a livello internazionale e individuare un quadro giuridico ed etico comune e complementare per l'utilizzo dell'IA, in particolare per le autorità di contrasto e giudiziarie, che rispetti appieno la Carta, l'acquis europeo in materia di protezione dei dati e, in senso più ampio, i diritti umani;
35. chiede all'Agenzia per i diritti fondamentali dell'UE, in collaborazione con il comitato europeo per la protezione dei dati e il Garante europeo della protezione dei dati, di elaborare orientamenti, raccomandazioni e buone pratiche completi al fine di precisare ulteriormente i criteri e le condizioni per lo sviluppo, l'uso e la diffusione di applicazioni e soluzioni di IA per l'uso da parte delle autorità di contrasto e giudiziarie; si impegna a condurre uno studio sull'attuazione della direttiva sulla protezione dei dati<sup>1</sup> al fine di stabilire in che modo la protezione dei dati personali è stata garantita nelle attività di trattamento da parte delle autorità di contrasto e giudiziarie, in particolare nelle fasi di

---

<sup>1</sup> 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 (GU L 119 del 4.5.2016, pag. 89).

sviluppo e diffusione delle nuove tecnologie; invita, inoltre, la Commissione a valutare se sia necessario adottare una specifica azione legislativa volta a precisare ulteriormente i criteri e le condizioni per lo sviluppo, l'uso e la diffusione di applicazioni e soluzioni di IA da parte delle autorità di contrasto e giudiziarie;

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