



TESTI APPROVATI

Edizione provvisoria

P9_TA-PROV(2021)0009

Intelligenza artificiale: questioni relative all'interpretazione e applicazione del diritto internazionale

Risoluzione del Parlamento europeo del 20 gennaio 2021 sull'intelligenza artificiale: questioni relative all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE è interessata relativamente agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale (2020/2013(INI))

Il Parlamento europeo,

- visto il preambolo al trattato sull'Unione europea e i suoi articoli 2, 3, 10, 19, 20, 21, 114, 167, 218, 225 e 227,
- visto il diritto di petizione di cui agli articoli 20 e 227 del trattato sul funzionamento dell'Unione europea,
- vista la Carta dei diritti fondamentali dell'Unione europea,
- vista la direttiva 2000/43/CE del Consiglio, del 29 giugno 2000, che attua il principio della parità di trattamento fra le persone indipendentemente dalla razza e dall'origine etnica¹ (direttiva sull'uguaglianza razziale),
- vista la direttiva 2000/78/CE del Consiglio, del 27 novembre 2000, che stabilisce un quadro generale per la parità di trattamento in materia di occupazione e di condizioni di lavoro² (direttiva sulla parità di trattamento in materia di occupazione),
- visti 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)³ (GDPR) e 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

¹ GU L 180 del 19.7.2000, pag. 22.

² GU L 303 del 2.12.2000, pag. 16.

³ GU L 119 del 4.5.2016, pag. 1.

Consiglio¹,

- visto il regolamento (UE) 2018/1488 del Consiglio, del 28 settembre 2018, che istituisce l'impresa comune per il calcolo ad alte prestazioni europeo²,
- vista la proposta di regolamento del Parlamento europeo e del Consiglio del 6 giugno 2018 che istituisce il programma Europa digitale per il periodo 2021-2027 (COM(2018)0434),
- vista la sua risoluzione del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica³,
- vista la sua risoluzione del 1° giugno 2017 sulla digitalizzazione dell'industria europea⁴,
- vista la sua risoluzione del 12 settembre 2018 sui sistemi d'arma autonomi⁵,
- vista la sua risoluzione dell'11 settembre 2018 sull'uguaglianza linguistica nell'era digitale⁶,
- vista la sua risoluzione del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale (IA)⁷,
- vista la comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni dell'11 dicembre 2019 sul Green Deal europeo (COM/2019/640),
- 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 al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni del 19 febbraio 2020 dal titolo "Una strategia europea per i dati" (COM(2020)0066),
- vista la comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni del 19 febbraio 2020 dal titolo "Plasmare il futuro digitale dell'Europa" (COM(2020)0067),
- vista la relazione sugli orientamenti etici per un'intelligenza artificiale affidabile pubblicata l'8 aprile 2019 dal gruppo di esperti ad alto livello sull'intelligenza artificiale istituito dalla Commissione nel giugno 2018,
- visti la Convenzione quadro del Consiglio d'Europa per la protezione delle minoranze nazionali, il protocollo n. 12 della Convenzione per la salvaguardia dei diritti dell'uomo

¹ GU L 119 del 4.5.2016, pag. 89.

² GU L 252 dell'8.10.2018, pag. 1.

³ GU C 252 del 18.7.2018, pag. 239.

⁴ GU C 307 del 30.8.2018, pag. 163.

⁵ GU C 433 del 23.12.2019, pag. 86.

⁶ GU C 433 del 23.12.2019, pag. 42.

⁷ GU C 449 del 23.12.2020, pag. 37.

- e delle libertà fondamentali e la Carta europea delle lingue regionali e minoritarie,
- vista la Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi, adottata dal gruppo di lavoro sulla qualità della giustizia del Consiglio d'Europa (CEPEJ-GT-QUAL) nel dicembre 2018,
 - vista la raccomandazione del Consiglio dell'OCSE sull'intelligenza artificiale, adottata il 22 maggio 2019,
 - visto l'articolo 54 del suo regolamento,
 - visti i pareri della commissione per gli affari esteri, della commissione per il mercato interno e la protezione dei consumatori, della commissione per i trasporti e il turismo e della commissione per le libertà civili, la giustizia e gli affari interni,
 - vista la relazione della commissione giuridica (A9-0001/2021),

Introduzione

- A. considerando che l'intelligenza artificiale (IA), la robotica e le tecnologie correlate sono in rapida evoluzione ed hanno un impatto diretto su tutti gli aspetti della società, inclusi i principi e i valori sociali ed economici di base;
- B. considerando che l'IA sta provocando una rivoluzione nella dottrina e nel materiale militari attraverso un profondo cambiamento nel modo di operare degli eserciti dovuto, principalmente, all'integrazione e allo sfruttamento delle nuove tecnologie e delle nuove capacità autonome;
- C. considerando che lo sviluppo e la progettazione della cosiddetta "intelligenza artificiale", della robotica e delle tecnologie correlate sono effettuati dagli esseri umani e che le loro scelte determinano la misura in cui tali tecnologie possono offrire benefici alla società;
- D. considerando che un quadro comune dell'Unione deve riguardare lo sviluppo, la diffusione e l'utilizzo dell'intelligenza artificiale, della robotica e delle tecnologie correlate e deve garantire il rispetto della dignità umana e dei diritti umani, come sancito dalla Carta dei diritti fondamentali dell'Unione europea;
- E. considerando che l'Unione e gli Stati membri sono investiti di una responsabilità particolare nel garantire che l'intelligenza artificiale, la robotica e le tecnologie correlate - dal momento che possono essere utilizzate in modo transfrontaliero - siano incentrate sull'uomo, vale a dire fondamentalmente intese per essere impiegate al servizio dell'umanità e per il bene comune, onde contribuire al benessere e all'interesse generale dei cittadini; che l'Unione dovrebbe aiutare gli Stati membri a raggiungere tale obiettivo, in particolare quelli che hanno iniziato a riflettere sul possibile sviluppo di norme giuridiche o di modifiche legislative in questo settore;
- F. considerando che i cittadini europei potrebbero beneficiare di un approccio normativo adeguato, efficace, trasparente e coerente a livello unionale, che definisca condizioni sufficientemente chiare affinché le imprese sviluppino applicazioni e pianifichino il proprio modello imprenditoriale, assicurando al contempo che l'Unione e gli Stati membri mantengano il controllo sulle normative da definire in modo tale che non siano

costretti ad adottare o accettare norme stabilite da altri;

- G. considerando che gli orientamenti in materia di etica, quali i principi adottati dal gruppo di esperti ad alto livello sull'intelligenza artificiale, costituiscono un buon punto di partenza ma non sono sufficienti per garantire che le imprese agiscano in modo equo e assicurino una protezione efficace degli individui;
- H. considerando che tale responsabilità specifica implica segnatamente la necessità di analizzare le questioni relative all'interpretazione e all'applicazione del diritto internazionale legate alla partecipazione attiva dell'UE ai negoziati internazionali, nella misura in cui l'UE è interessata relativamente agli impieghi civili e militari di questo tipo di IA, robotica e tecnologie correlate, e le questioni di autorità dello Stato nei confronti di tali tecnologie restano al di fuori dell'ambito della giustizia penale;
- I. considerando che è essenziale fornire un quadro giuridico adeguato e completo per gli aspetti etici di tali tecnologie nonché per la responsabilità, la trasparenza e la responsabilità (in particolare per l'IA, la robotica e le tecnologie correlate considerate ad alto rischio); che tale quadro deve riflettere il fatto che i valori umanisti intrinsecamente europei e universali sono applicabili all'intera catena del valore nello sviluppo, nell'attuazione e negli impieghi dell'IA; che tale quadro etico deve applicarsi allo sviluppo (ivi comprese la ricerca e l'innovazione), alla diffusione e all'utilizzo dell'intelligenza artificiale, nel massimo rispetto del diritto unionale e dei valori sanciti dalla Carta dei diritti fondamentali dell'Unione europea;
- J. considerando che tale analisi mira a esaminare in che misura le norme del diritto internazionale pubblico e privato e del diritto dell'UE siano adeguate a tali tecnologie nonché a mettere in risalto le sfide e i rischi che queste pongono per l'autorità dello Stato, in modo da poterli gestire in modo adeguato e proporzionato;
- K. considerando che la Commissione europea non contempla gli aspetti militari dell'utilizzo dell'intelligenza artificiale nel proprio Libro bianco;
- L. considerando che un approccio europeo armonizzato a questi problemi richiede una definizione comune di intelligenza artificiale e il rispetto dei valori fondamentali dell'Unione europea, dei principi della Carta dei diritti fondamentali dell'Unione europea e della legislazione internazionale in materia di diritti umani;
- M. considerando che l'IA offre possibilità inedite di migliorare le prestazioni nel settore dei trasporti, affrontando le sfide della crescente domanda di spostamenti, della sicurezza e della dimensione ambientale e rendendo nel contempo più intelligenti, più efficienti e più convenienti tutti i modi di trasporto;
- N. osserva che è indispensabile affrontare a livello di UE il tema dell'intelligenza artificiale nella difesa ai fini dello sviluppo delle capacità dell'Unione in tale settore;

Definizione di intelligenza artificiale

1. ritiene che sia necessario disporre di un quadro giuridico europeo comune, con definizioni armonizzate e principi etici comuni, anche per l'utilizzo dell'intelligenza artificiale a fini militari; chiede, quindi, alla Commissione europea di adottare le seguenti definizioni:

- “sistema di intelligenza artificiale (IA)”: un sistema basato su software o integrato in dispositivi hardware che mostra un comportamento che simula l'intelligenza, tra l'altro raccogliendo e trattando dati, analizzando e interpretando il proprio ambiente e intraprendendo azioni, con un certo grado di autonomia, per raggiungere obiettivi specifici;
 - "autonomo": sistema basato sull'intelligenza artificiale che opera interpretando determinati dati forniti e utilizzando una serie di istruzioni predeterminate, senza essere limitato a tali istruzioni, nonostante il comportamento del sistema sia legato e volto al conseguimento dell'obiettivo impartito e ad altre scelte operate dallo sviluppatore in sede di progettazione;
2. sottolinea che le politiche di sicurezza e difesa dell'Unione europea e dei suoi Stati membri sono guidate dai principi sanciti nella Carta europea dei diritti fondamentali e nella Carta delle Nazioni Unite – nella quale si invitano tutti gli Stati ad astenersi dalla minaccia o dall'uso della forza nelle loro reciproche relazioni – nonché dal diritto internazionale, dai principi dei diritti umani e del rispetto della dignità umana e da una visione comune dei valori universali rappresentati dai diritti inviolabili e inalienabili della persona, dalla libertà, dalla democrazia, dall'uguaglianza e dallo Stato di diritto; sottolinea che tutte le attività nel settore della difesa nel quadro dell'Unione devono rispettare questi valori universali, promuovendo nel contempo la pace, la stabilità, la sicurezza e il progresso in Europa e nel mondo;

Diritto internazionale pubblico e impieghi militari dell'intelligenza artificiale

3. ritiene che l'IA utilizzata in un contesto militare e civile debba essere soggetta ad un significativo controllo umano, in modo tale che in qualsiasi momento un umano abbia i mezzi per correggerla, bloccarla o disattivarla in caso di comportamento imprevisto, intervento accidentale, attacchi informatici o interferenza di terzi con tecnologie basate sull'IA o qualora terzi acquisiscano tale tecnologia;
4. ritiene che il rispetto del diritto internazionale pubblico, in particolare del diritto umanitario, che si applica inequivocabilmente a tutti i sistemi d'arma e ai relativi operatori, rappresenti un requisito fondamentale che gli Stati membri devono soddisfare, soprattutto con riferimento alla protezione della popolazione civile o all'adozione di misure precauzionali in caso di attacchi, per esempio aggressioni militari e guerra informatica;
5. sottolinea che l'IA e le tecnologie a essa correlate possono svolgere un ruolo anche in guerre irregolari o non convenzionali; propone che la ricerca, lo sviluppo e l'utilizzo dell'intelligenza artificiale in tali casi siano sottoposti alle stesse condizioni cui sono soggetti in conflitti convenzionali;
6. mette in rilievo che il ricorso all'IA offre l'opportunità di consolidare la sicurezza dell'Unione europea e dei relativi cittadini e che è essenziale che l'UE adotti un approccio integrato nei prossimi dibattiti internazionali al riguardo;
7. invita la comunità di ricerca sull'intelligenza artificiale a integrare questo principio in tutti i sistemi basati sull'intelligenza artificiale summenzionati destinati all'impiego militare; ritiene che nessuna autorità possa prevedere una deroga a tali principi o certificare un tale sistema;

8. ribadisce che un processo decisionale autonomo non dovrebbe esonerare gli esseri umani dalla responsabilità e che le persone devono sempre avere la responsabilità ultima dei processi decisionali, in modo da poter identificare l'essere umano responsabile della decisione;
9. sottolinea che, durante l'impiego dell'IA in un contesto militare, gli Stati, le parti di un conflitto e i singoli devono sempre rispettare i loro obblighi ai sensi del diritto internazionale applicabile e assumersi la responsabilità delle azioni risultanti dall'uso di tali sistemi; sottolinea che, in ogni circostanza, le azioni e gli effetti previsti, accidentali o indesiderati dei sistemi basati sull'IA devono essere considerati responsabilità degli Stati membri, delle parti di un conflitto e dei singoli individui;
10. plaude alle possibilità di utilizzare i sistemi di intelligenza artificiale a fini di addestramento ed esercitazione, il cui potenziale non dovrebbe essere sottovalutato, in particolare considerato che l'UE conduce esercitazioni di natura duplice, civile e militare;
11. sottolinea che, durante le fasi di progettazione, sviluppo, collaudo, distribuzione e impiego dei sistemi basati sull'IA, si debba tenere debitamente conto dei rischi potenziali, in particolare del rischio di causare morti e feriti accidentali tra i civili, perdite accidentali di vite umane e danni alle infrastrutture civili, nonché dei rischi relativi all'impegno non intenzionale, alla manipolazione, alla proliferazione, agli attacchi informatici, all'interferenza da parte di terzi con tecnologie autonome basate sull'IA o qualora terzi acquisiscano tale tecnologia;
12. ricorda che il principio di novità, conformemente al parere consultivo della Corte internazionale di giustizia, dell'8 luglio 1996, non può essere invocato a sostegno di qualsiasi deroga in merito al rispetto delle attuali norme del diritto internazionale umanitario;
13. ritiene che, oltre alle operazioni di sostegno, l'IA andrà a beneficio anche del personale di servizio delle forze armate attraverso il trattamento di massa dei loro dati sanitari e l'estensione del monitoraggio sanitario, individuerà i fattori di rischio connessi al loro ambiente e alle loro condizioni di lavoro e proporrà garanzie adeguate per limitare l'impatto sanitario sul personale di servizio;
14. ribadisce che gli sforzi normativi devono essere sostenuti da validi sistemi di certificazione e sorveglianza, nonché da chiari meccanismi di verificabilità, spiegabilità, responsabilità e tracciabilità, in modo che il quadro normativo non diventi obsoleto a seguito degli sviluppi tecnologici.
15. sottolinea l'importanza, in un mondo iperconnesso, della partecipazione dell'Unione europea alla creazione di un quadro giuridico internazionale per l'uso dell'intelligenza artificiale: esorta l'UE ad assumere un ruolo guida e, insieme alle Nazioni Unite e alla comunità internazionale, un ruolo attivo nella promozione di tale quadro globale che disciplini l'uso dell'IA per scopi militari e di altro tipo, garantendo che tale utilizzo rimanga entro i limiti rigorosi stabiliti dal diritto internazionale e dal diritto internazionale umanitario, in particolare le convenzioni di Ginevra del 12 agosto 1949; sottolinea che tale quadro non deve mai violare o consentire violazioni delle prescrizioni della coscienza pubblica e dell'umanità, come stabilito nella clausola Martens, ed essere in linea con le norme di sicurezza e i requisiti in materia di

protezione dei consumatori; esorta l'UE e gli Stati membri a definire solidi sistemi di sorveglianza e valutazione per lo sviluppo delle tecnologie di IA, in particolare quelle utilizzate per scopi militari negli Stati autoritari;

16. mette in rilievo che la robotica non solo consentirà al personale militare di rimanere a distanza, ma offrirà anche una migliore autoprotezione, per esempio nel caso di operazioni in ambienti contaminati, spegnimenti di incendi, sminamenti a terra o in mare e azioni di difesa da sciami di droni;
17. sottolinea che lo sviluppo, la diffusione, l'utilizzo e la gestione dell'IA devono rispettare i diritti, i valori e le libertà fondamentali sanciti dai trattati dell'UE e invita gli Stati membri a non diffondere sistemi di IA ad alto rischio che rappresentino una minaccia per i diritti fondamentali; prende atto della pubblicazione del Libro bianco della Commissione sull'intelligenza artificiale e invita a esaminare in modo più approfondito i potenziali rischi per i diritti fondamentali dell'utilizzo dell'IA da parte delle autorità pubbliche come pure delle agenzie, degli organismi e delle istituzioni dell'Unione europea;
18. chiede alla Commissione di agevolare le attività di ricerca e le discussioni circa le opportunità offerte dall'utilizzo dell'IA per i soccorsi in caso di calamità, la prevenzione delle crisi e il mantenimento della pace;
19. accoglie con favore la creazione di un gruppo di esperti governativi delle Nazioni Unite per promuovere un comportamento responsabile nel ciberspazio da parte degli Stati nel contesto della sicurezza internazionale e invita l'UE a partecipare a pieno titolo al lavoro di tale gruppo;
20. invita il vicepresidente della Commissione/alto rappresentante per gli affari esteri e la politica di sicurezza (VP/AR) a preparare il terreno per negoziati globali intesi a creare un regime di controllo delle armi basate sull'IA e ad aggiornare tutti gli strumenti previsti dai trattati relativi al controllo delle armi, al disarmo e alla non proliferazione, al fine di tenere in considerazione i sistemi basati sull'IA in situazione di guerra; chiede che la posizione comune del Consiglio che definisce norme comuni per il controllo delle esportazioni di tecnologia e attrezzature militari tenga pienamente in considerazione e contempli i sistemi d'arma basati sull'IA;
21. rammenta che tali norme devono sempre rispettare i principi, ribaditi dalla Convenzione di Roma del 17 luglio 1998, di proibizione di crimini di genocidio, contro l'umanità e dei crimini di guerra;
22. pone in evidenza i chiari rischi correlati alle decisioni prese dagli esseri umani qualora si basino unicamente su dati, profili e raccomandazioni generati dalle macchine; sottolinea che la progettazione generale dei sistemi di IA dovrebbe comprendere anche orientamenti sulla supervisione e sul controllo umani; chiede che sia introdotto un obbligo in materia di trasparenza e spiegabilità delle applicazioni di IA e la necessità di un intervento umano e che siano adottate altre misure, quali audit indipendenti e prove di stress specifiche per favorire e garantire la conformità; sottolinea che tali audit dovrebbero essere condotti periodicamente da un'autorità indipendente incaricata di vigilare sulle applicazioni di IA ad alto rischio utilizzate dalle autorità pubbliche o dalle forze armate;

23. pone l'accento sull'importanza di verificare in che modo le tecnologie di IA ad alto rischio giungano a una decisione; rammenta che i principi di non discriminazione e proporzionalità devono essere rispettati e che le questioni relative alla causalità e alla responsabilità, nonché alla trasparenza, la rendicontabilità e la spiegabilità, devono essere chiarite per determinare se, o in che misura, lo Stato, in qualità di attore del diritto internazionale pubblico, ma anche nell'esercizio della propria autorità, possa agire servendosi di sistemi basati sull'intelligenza artificiale, che dispongono di una certa autonomia, senza violare gli obblighi derivanti dal diritto internazionale, come quelli in materia di giusto processo;
24. insiste sull'importanza di investire nelle competenze umane, comprese quelle digitali, al fine di adattarsi ai progressi scientifici che includono soluzioni basate sull'IA per le persone che esercitano professioni regolamentate, tra cui le attività connesse all'esercizio dei poteri dell'autorità statale, quali l'amministrazione della giustizia; invita gli Stati membri e la Commissione a tenere debitamente conto di tale aspetto nel quadro dell'attuazione della direttiva 2005/36/CE¹;
25. insiste sulla necessità che i sistemi di IA rispettino sempre i principi di responsabilità, equità, governabilità, precauzione, responsabilità, imputabilità, prevedibilità, tracciabilità, attendibilità, affidabilità, trasparenza, spiegabilità, capacità di individuare eventuali cambiamenti nelle circostanze e nell'ambiente operativo, distinzione tra combattenti e non combattenti e proporzionalità; sottolinea che detto principio subordina la legittimità di un'azione militare al rispetto di un equilibrio tra l'obiettivo e i mezzi utilizzati, e che la valutazione della proporzionalità debba essere sempre effettuata da una persona umana;
26. sottolinea che, nell'uso dei sistemi di IA nel settore della sicurezza e della difesa, la comprensione completa della situazione da parte dell'operatore umano, la prevedibilità, l'affidabilità e la resilienza del sistema basato sull'IA, nonché la capacità dell'operatore umano di individuare possibili cambiamenti di circostanze e ambiente operativo e la sua possibilità di intervenire in un attacco o di interromperlo sono necessari per garantire che i principi del diritto internazionale umanitario, in particolare la distinzione, la proporzionalità e la precauzione negli attacchi, siano pienamente applicati all'intera catena di comando e controllo; sottolinea che i sistemi basati sull'IA devono consentire agli umani responsabili di esercitare un controllo significativo, di assumere la piena responsabilità dei sistemi e rispondere di tutti i loro utilizzi; invita la Commissione a promuovere il dialogo, una più stretta cooperazione e sinergie tra Stati membri, ricercatori, accademici, attori della società civile e settore privato, in particolare le imprese leader, e il settore militare per garantire che i processi decisionali riguardanti la regolamentazione dell'IA nel settore della difesa siano inclusivi;
27. evidenzia che il Parlamento ha chiesto l'elaborazione e l'adozione urgente di una posizione comune sui sistemi d'arma autonomi letali (SALA), il divieto dello sviluppo, della produzione e dell'utilizzo di sistemi di detto tipo in grado di sferrare attacchi senza un controllo umano significativo, nonché l'avvio di negoziati fruttuosi per vietare tali armi; ricorda, a tale riguardo, la sua risoluzione del 12 settembre 2018 sui sistemi d'arma autonomi; ricorda che l'espressione "sistemi d'arma autonomi letali" (SALA)

¹ Direttiva 2005/36/CE del Parlamento europeo e del Consiglio, del 7 settembre 2005, relativa al riconoscimento delle qualifiche professionali (GU L 255 del 30.9.2005, pag. 22).

designa sistemi d'arma privi di un controllo umano significativo sulle funzioni critiche della selezione e dell'attacco di bersagli individuali; sottolinea che la decisione di selezionare un bersaglio e intraprendere un'azione letale con l'ausilio di sistemi d'arma con un certo livello di autonomia deve essere sempre presa da operatori umani che esercitano un controllo e una supervisione significativi e la necessaria discrezionalità, in linea con i principi di proporzionalità e necessità; sottolinea che i sistemi basati sull'IA non possono sostituire, in alcuna circostanza, il processo decisionale umano in tale ambito;

28. osserva, inoltre, che i sistemi d'arma autonomi, in quanto categoria particolare di IA nel settore militare, dovrebbero essere discussi e concordati a livello internazionale, nello specifico in seno alla Convenzione delle Nazioni Unite su talune armi convenzionali; richiama l'attenzione sul dibattito internazionale in corso sui SALA per regolamentare le tecnologie militari emergenti, che finora non ha condotto a un accordo; sottolinea che solo di recente l'UE ha accettato di discutere degli effetti prodotti dagli sviluppi dell'IA e della digitalizzazione sul settore della difesa; ritiene che l'UE possa svolgere un ruolo decisivo nell'aiutare gli Stati membri ad armonizzare il loro approccio all'IA nel settore militare, al fine di guidare le discussioni internazionali;
29. ribadisce la necessità di una strategia a livello europeo contro i SALA e di un divieto per i cosiddetti "robot assassini";
30. evidenzia che l'IA impiegata in un contesto militare deve soddisfare una serie di requisiti minimi, segnatamente essere in grado di distinguere tra combattenti, non combattenti e combattenti sul campo di battaglia, riconoscere quando un combattente si arrende o è fuori combattimento, non avere effetti indiscriminati, non causare sofferenze inutili alle persone, non essere falsato né formato intenzionalmente sulla base di dati incompleti e rispettare i principi del diritto internazionale umanitario, di proporzionalità nell'uso della forza e di precauzione prima dell'intervento;
31. ritiene che l'uso di sistemi d'arma autonomi letali sollevi questioni etiche e giuridiche fondamentali circa la capacità degli esseri umani di controllare tali sistemi e chiede che la tecnologia basata sull'IA non sia in grado di prendere decisioni autonome riguardanti i principi giuridici di distinzione, proporzionalità e precauzione;
32. chiede che a livello internazionale siano adottate misure trasparenti di riduzione dei rischi riguardo allo sviluppo e all'utilizzo dell'IA in ambito militare, in particolare in relazione ai principi di integrità territoriale, non intervento e uso della forza; pone l'accento sull'importanza di tenere conto degli aspetti militari nell'affrontare le questioni giuridiche ed etiche nell'ambito del quadro europeo in materia di IA; ricorda la sua posizione sul divieto di sviluppo, produzione e uso dei SALA; si rammarica del fatto che a livello mondiale non esistano convenzioni esplicite sull'uso di tali armi;
33. riconosce che le moderne dinamiche della corsa agli armamenti tra i principali Stati nazionali militari per lo sviluppo di SALA procedono a un ritmo più rapido rispetto alla promozione di norme e quadri giuridici comuni e all'applicazione e all'attuazione universali ed efficaci degli stessi, poiché le informazioni sullo sviluppo e sulla distribuzione di tali sistemi sono classificate e gli Stati nazionali hanno un interesse intrinseco a creare le capacità offensive più rapide e più efficaci, indipendentemente dai quadri giuridici o dai principi attuali o potenzialmente futuri;

34. ritiene che i SALA debbano essere utilizzati solo come ultima risorsa e siano leciti solo se soggetti a un rigoroso controllo umano, con una persona in grado di assumere il comando in qualsiasi momento, in quanto un intervento e una supervisione umani significativi sono essenziali nell'adottare decisioni letali e gli esseri umani dovrebbero sempre essere responsabili quando decidono tra la vita e la morte; è dell'avviso che i sistemi totalmente privi del controllo umano ("human off the loop") e della supervisione umana dovrebbero essere vietati senza eccezioni e in qualsiasi circostanza;
35. invita il VP/AR, gli Stati membri e il Consiglio europeo a delineare e adottare con urgenza una posizione comune sui sistemi d'arma autonomi che assicuri un controllo umano significativo sulle funzioni critiche dei sistemi d'arma, anche durante il dispiegamento, nonché a parlare con una sola voce nelle sedi pertinenti e ad agire di conseguenza; invita, in tale contesto, il VP/AR, gli Stati membri e il Consiglio a condividere le migliori prassi e a raccogliere contributi dagli esperti, dal mondo accademico e dalla società civile, come indicato nella posizione del 12 settembre 2018 sui sistemi d'arma autonomi, secondo cui gli attacchi dovrebbero sempre essere condotti con un intervento umano significativo;
36. incoraggia gli Stati a valutare se e come i dispositivi militari autonomi abbiano contribuito alla loro sicurezza nazionale e che cosa la loro sicurezza nazionale potrebbe ottenere dai sistemi d'arma basati sull'IA, in particolare per quanto riguarda il potenziale di tali tecnologie di sostenere e migliorare il processo decisionale umano in conformità del diritto internazionale umanitario e dei suoi principi; ricorda che in qualsiasi sistema d'arma autonomo letale o arma con un alto livello di autonomia può verificarsi un malfunzionamento a causa di un codice non compilato correttamente o di un attacco informatico perpetrato da uno Stato nemico o da un soggetto non statale;
37. insiste affinché i SALA siano utilizzati solo in casi specifici e conformemente alle procedure di autorizzazione dettagliate in anticipo in documenti per i quali lo Stato interessato — a prescindere dal fatto che faccia o meno parte dell'Organizzazione del Trattato del Nord Atlantico — garantisce l'accessibilità al pubblico o almeno al proprio parlamento nazionale;
38. ritiene che i SALA debbano rispettare le disposizioni della convenzione del 10 ottobre 1980 su certe armi convenzionali, compreso il divieto per le armi "che possono essere considerate dannose";
39. propone, al fine di impedirne la diffusione incontrollata, che i SALA siano inseriti nell'elenco delle armi soggette alle disposizioni del trattato sul commercio delle armi del 2 aprile 2013, di cui all'articolo 2 di detto trattato;
40. esige che sia imposto il divieto di antropomorfizzare i SALA onde evitare qualsiasi confusione tra una persona umana e un robot;
41. accoglie con favore il fatto che il Consiglio e il Parlamento abbiano concordato di escludere i sistemi d'arma autonomi letali "senza la possibilità di un significativo controllo umano sulle decisioni relative alla selezione e all'ingaggio nell'effettuare attacchi" dalle azioni finanziate dal Fondo europeo per la difesa (FED); ricorda la sua posizione secondo cui l'uso, lo sviluppo o la produzione di SALA senza un significativo controllo umano non è ammissibile ai finanziamenti del FED;

42. invita la Commissione a sostenere lo studio, lo sviluppo, la diffusione e l'utilizzo dell'IA nel contesto del mantenimento della pace e della prevenzione dei conflitti;
43. osserva che l'ecosistema globale dell'intelligenza artificiale è dominato da giganti del digitale americani e cinesi che stanno sviluppando capacità interne e stanno acquistando molte imprese promettenti; è, pertanto, fermamente convinto che, onde evitare di rimanere indietro nel settore delle tecnologie basate sull'intelligenza artificiale, è essenziale muoversi verso un equilibrio migliore tra la ricerca di base e le applicazioni industriali, sviluppando al contempo vantaggi competitivi strategici attraverso una crescita del proprio potenziale e delle proprie risorse;
44. sottolinea che, nella misura in cui rientrano nella definizione di macchine di cui alla direttiva 2006/42/CE¹, i robot dovrebbero essere progettati e assemblati nel rispetto delle norme e delle misure di sicurezza ivi previste;
45. ricorda l'ambizione dell'UE di essere un attore globale di pace e chiede che essa svolga un ruolo più ampio negli sforzi globali per il disarmo e la non proliferazione e che le sue azioni e politiche perseguano il mantenimento della pace e della sicurezza internazionali, garantendo il rispetto del diritto internazionale umanitario e del diritto internazionale dei diritti umani e la protezione della popolazione civile e delle infrastrutture civili;
46. sottolinea la necessità di esaminare il potenziale impatto dell'IA in quanto fattore strategico per la politica di sicurezza e di difesa comune (PSDC) dell'UE, in particolare con riferimento alle missioni e alle operazioni militari e civili e allo sviluppo delle capacità dell'UE;
47. ricorda che anche i nostri alleati nel quadro nazionale, dell'UE e della NATO stanno integrando l'IA nei loro sistemi militari; ritiene necessario preservare l'interoperabilità con i nostri alleati mediante norme comuni, che sono essenziali per svolgere operazioni in coalizione; ribadisce che, oltre a ciò, la cooperazione in materia di IA dovrebbe svolgersi in un quadro europeo, che rappresenta l'unico contesto adeguato per creare realmente sinergie forti, come proposto dalla strategia dell'UE per l'intelligenza artificiale;
48. ritiene che l'UE debba monitorare attentamente ed esaminare le implicazioni dei progressi conseguiti nell'IA impiegata nel campo della difesa e della guerra, tra cui sviluppi e diffusioni potenzialmente destabilizzanti, nonché guidare una ricerca e una progettazione etiche, assicurando l'integrità dei dati personali e un accesso e un controllo individuali, tenendo inoltre conto delle questioni economiche e umanitarie;
49. ricorda la sua posizione del 12 settembre 2018 sui sistemi d'arma autonomi, che afferma che non devono essere effettuati attacchi senza un intervento umano significativo; invita il VP/AR, gli Stati membri e il Consiglio europeo ad adottare una posizione comune sui sistemi d'arma autonomi che garantisca un controllo umano significativo sulle funzioni essenziali di tali sistemi, anche durante la distribuzione; ribadisce il suo sostegno all'attività in materia di SALA svolta dal gruppo di esperti governativi ONU delle alte

¹ Direttiva 2006/42/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle macchine e che modifica la direttiva 95/16/CE (rifusione) (GU L 157 del 9.6.2006, pag. 24).

parti contraenti della Convenzione su talune armi convenzionali, che resta il forum internazionale di riferimento per i dibattiti e i negoziati sulle sfide giuridiche che tali sistemi comportano; chiede che tutti gli attuali sforzi multilaterali siano accelerati in modo che il quadro normativo e regolamentare non sia superato dagli sviluppi tecnologici e dai nuovi metodi di guerra; invita il VP/AR, nel quadro delle discussioni in corso sulla regolamentazione internazionale dei SALA da parte degli Stati che aderiscono alla CCW, a rimanere coinvolte e a contribuire a proseguire, senza indugio, gli sforzi intesi a sviluppare un nuovo quadro normativo globale e uno strumento giuridicamente vincolante incentrato sulle definizioni, i concetti e le caratteristiche delle tecnologie emergenti nel settore dei SALA, le questioni etiche e giuridiche del controllo umano, in particolare per quanto riguarda le loro funzioni essenziali quali la selezione e l'attacco degli obiettivi, il mantenimento della responsabilità e rendicontabilità umana e il necessario grado di interazione tra l'umano e la macchina, compreso il concetto di controllo e giudizio umani; chiede che tali sforzi garantiscano il rispetto del diritto internazionale umanitario e del diritto internazionale dei diritti umani durante le diverse fasi del ciclo di vita di un'arma basata sull'IA, al fine di concordare raccomandazioni concrete per il chiarimento, l'esame e lo sviluppo di aspetti del quadro normativo sulle tecnologie emergenti nell'ambito dei SALA;

50. ritiene cruciale per la sicurezza globale disporre di un meccanismo efficace per l'applicazione delle norme in materia di non proliferazione dei SALA e di eventuali future tecnologie offensive basate sull'IA;

Autorità dello Stato: esempi inerenti gli ambiti civili, tra cui la sanità e la giustizia

51. pone l'accento sulla necessità che gli Stati membri agiscano in maniera efficace per ridurre la loro dipendenza da dati esteri e garantiscano, senza distorcere significativamente il mercato, che il possesso di tecnologie di intelligenza artificiale più sofisticate da parte di potenti gruppi privati non porti a ricusare l'autorità della potenza pubblica e ancor meno a sostituirla con un'autorità privata, soprattutto se tali gruppi privati sono di proprietà di un paese terzo che non fa parte dell'Unione europea;
52. sottolinea che l'uso di sistemi di IA nei processi decisionali delle pubbliche autorità può condurre a decisioni di parte che comportano conseguenze negative per i cittadini, che devono, pertanto, essere soggette a criteri rigorosi per controllarne, tra l'altro, la sicurezza, la trasparenza, la rendicontabilità, la non discriminazione e la responsabilità sociale e ambientale; esorta gli Stati membri a valutare i rischi connessi alle decisioni basate sull'IA relativamente all'esercizio dell'autorità statale e a prevedere garanzie quali una vigilanza umana significativa, requisiti di trasparenza e la possibilità di contestare tali decisioni;
53. esorta gli Stati membri a valutare i rischi connessi alle tecnologie basate sull'IA prima di automatizzare le attività relative all'esercizio dell'autorità statale, come la corretta amministrazione della giustizia; invita gli Stati membri a considerare la necessità di introdurre garanzie, come la supervisione di un professionista qualificato e l'elaborazione di norme rigorose in materia di deontologia professionale;
54. sottolinea l'importanza di intervenire a livello europeo per contribuire a promuovere gli investimenti, quanto mai necessari, le infrastrutture di dati, la ricerca, anche per quanto riguarda l'utilizzo dell'intelligenza artificiale da parte delle pubbliche autorità, e un quadro etico comune;

55. sottolinea che l'Unione europea deve impegnarsi per conseguire la resilienza strategica, in modo da non trovarsi mai più impreparata dinanzi a una crisi ed evidenzia che tale aspetto assume un'importanza cruciale in particolar modo per l'intelligenza artificiale e le sue applicazioni militari; evidenzia che le catene di approvvigionamento per i sistemi militari di IA che potrebbero portare a una dipendenza tecnologica andrebbero riesaminate e che tali dipendenze dovrebbero essere progressivamente eliminate; chiede maggiori investimenti nell'IA europea per la difesa e nelle infrastrutture essenziali che la sostengono;
56. invita la Commissione a valutare le conseguenze di una moratoria sull'utilizzo dei sistemi di riconoscimento facciale e, in funzione dell'esito di tale valutazione, a prendere in considerazione l'introduzione di una moratoria sull'utilizzo di tali sistemi da parte delle autorità dello Stato nei luoghi pubblici e nei locali destinati all'istruzione e all'assistenza sanitaria, come pure di una moratoria sull'utilizzo dei sistemi di riconoscimento facciale da parte delle autorità di contrasto in spazi semi-pubblici come gli aeroporti, fino a quando le norme tecniche non saranno considerate pienamente conformi ai diritti fondamentali, i risultati ottenuti non saranno privi di distorsioni e di discriminazioni e non vi saranno rigorose garanzie contro gli utilizzi impropri in grado di assicurare la necessità e la proporzionalità dell'utilizzo di tali tecnologie;
57. pone l'accento sull'importanza della cibersicurezza per l'IA in scenari sia offensivi che difensivi; rileva, a tale riguardo, l'importanza della cooperazione internazionale e della pubblicazione e condivisione delle vulnerabilità e delle misure correttive nel settore della sicurezza informatica; sollecita una cooperazione internazionale in materia di cibersicurezza ai fini di un utilizzo e una diffusione efficaci dell'IA, nonché l'introduzione di garanzie contro gli utilizzi impropri dell'IA e i ciberattacchi; prende altresì atto della natura a duplice uso (vale a dire per finalità civili e militari) dei sistemi informatici e dell'IA e chiede una regolamentazione efficace della materia;
58. ritiene che gli Stati membri dovrebbero promuovere tecnologie di IA che siano al servizio dei cittadini e che le persone nei confronti delle quali un'autorità pubblica ha preso una decisione basandosi sui dati di un sistema di IA debbano esserne informate, ricevere tempestivamente le informazioni di cui al paragrafo precedente, nonché avere la possibilità di contestare tale decisione e scegliere che la questione sia definita senza l'intervento di un sistema di IA; invita gli Stati membri a valutare la necessità di introdurre garanzie, come previsto dalla direttiva (UE) 2018/958¹, quali la supervisione di un professionista qualificato e norme di deontologia professionale;
59. sottolinea che la possibilità di fare previsioni basate sulla condivisione e l'utilizzo dei dati nonché sull'accesso agli stessi deve essere disciplinata da requisiti di qualità, integrità, trasparenza, sicurezza, riservatezza e controllo; pone l'accento sulla necessità di rispettare, in tutte le fasi di sviluppo, diffusione e utilizzo dell'IA, della robotica e delle tecnologie correlate, il quadro giuridico dell'UE in materia di protezione dei dati e riservatezza al fine di accrescere la sicurezza dei cittadini e la loro fiducia in tali tecnologie;
60. osserva il rapido sviluppo delle applicazioni di IA in grado di riconoscere elementi

¹ Direttiva (UE) 2018/958 del Parlamento europeo e del Consiglio, del 28 giugno 2018, relativa a un test della proporzionalità prima dell'adozione di una nuova regolamentazione delle professioni (GU L 173 del 9.7.2018, pag. 25).

caratteristici univoci, come caratteristiche del volto, movimenti e atteggiamenti; mette in guardia dai problemi legati all'utilizzo delle applicazioni di riconoscimento automatico in termini di intrusione nella vita privata, non discriminazione e protezione dei dati personali;

61. sottolinea che, a norma del GDPR, è vietata qualsiasi decisione su una persona fisica basata esclusivamente sull'elaborazione automatizzata, compresa la profilazione, che produca un effetto giuridico negativo sull'interessato o che abbia ripercussioni significative su detta persona, a meno che tale decisione sia autorizzata dal diritto dell'Unione o dello Stato membro e sia subordinata all'esistenza di misure adeguate atte a salvaguardare i diritti, le libertà e gli interessi legittimi dell'interessato;
62. chiede che là dove l'intelligenza artificiale è utilizzata dalle autorità pubbliche siano garantite la spiegabilità degli algoritmi, la trasparenza e la sorveglianza regolamentare, e che siano effettuate valutazioni d'impatto prima del ricorso da parte di autorità statali a strumenti che utilizzano tecnologie di IA; invita la Commissione e il comitato europeo per la protezione dei dati a pubblicare orientamenti e raccomandazioni e a sviluppare buone prassi per specificare ulteriormente i criteri e le condizioni applicabili alle decisioni basate sulla profilazione e sull'uso dell'IA da parte delle autorità pubbliche;
63. osserva che l'intelligenza artificiale svolge un ruolo sempre più cruciale nell'assistenza sanitaria, in particolare attraverso gli algoritmi di supporto alla diagnosi, la chirurgia robotica, le protesi intelligenti, le terapie personalizzate basate sulla modellizzazione tridimensionale del corpo del paziente, i robot sociali per l'assistenza agli anziani, le terapie digitali volte a migliorare l'indipendenza di alcune persone affette da disturbi mentali, la medicina predittiva e i software di anticipazione delle epidemie;
64. insiste, tuttavia, sulla necessità che tutti gli usi dell'IA nella sanità pubblica debbano garantire la protezione dei dati personali dei pazienti e prevenire la loro diffusione incontrollata;
65. chiede che tutti gli usi dell'IA nel settore della sanità pubblica rispettino il principio della parità di trattamento dei pazienti in termini di accesso alle cure, preservino il rapporto tra paziente e medico e siano coerenti in ogni momento con il giuramento di Ippocrate, di modo che il medico abbia sempre la possibilità di discostarsi dalla soluzione proposta dall'IA, mantenendo pertanto la responsabilità di qualsiasi decisione;
66. osserva che l'utilizzo dell'IA nel contrasto alla criminalità e alla cybercriminalità potrebbe offrire un'ampia gamma di possibilità e opportunità; afferma nel contempo che dovrebbe continuare a prevalere il principio secondo cui ciò che è illegale offline lo è anche online;
67. osserva che l'IA è utilizzata sempre più sovente nel settore della giustizia al fine di prendere decisioni più razionali, maggiormente conformi alle leggi vigenti e più rapide; plaude al fatto che il ricorso all'IA dovrebbe accelerare i procedimenti giudiziari;
68. ritiene che occorra chiarire se sia opportuno che le decisioni inerenti all'applicazione della legge siano in parte delegate all'IA, pur mantenendo un controllo umano sulla decisione finale;
69. sottolinea che l'utilizzo dell'IA nel settore giudiziario potrebbe migliorare l'analisi e la

raccolta dei dati e la protezione delle vittime e che tale utilizzo potrebbe essere esplorato nell'ambito di attività di ricerca e sviluppo e accompagnato da valutazioni d'impatto, in particolare in relazione alle garanzie volte ad assicurare un giusto processo e ad evitare distorsioni e discriminazioni, applicando nel contempo il principio di precauzione; ricorda tuttavia che ciò non può sostituire il coinvolgimento di esseri umani nella pronuncia delle sentenze o nell'adozione delle decisioni;

70. rammenta l'importanza dei principi di governance, trasparenza, imparzialità, responsabilità, equità e integrità intellettuale nell'utilizzo dell'IA nel settore della giustizia penale;
71. esorta gli Stati membri a valutare i rischi connessi alle tecnologie basate sull'IA prima di automatizzare le attività relative all'esercizio dell'autorità statale, in particolare nel settore della giustizia; invita gli Stati membri a considerare la necessità di prevedere garanzie, come la supervisione di un professionista qualificato e norme di deontologia professionale;
72. osserva che alcune tecnologie di IA consentono un'automatizzazione senza precedenti dell'elaborazione delle informazioni e delle attività, come nel caso della sorveglianza di massa in ambito civile e militare, che rappresenta una minaccia per i diritti fondamentali e spiana la strada a interferenze illecite nella sovranità statale; chiede che le attività di sorveglianza di massa siano sottoposte a controllo a norma del diritto internazionale, anche per quanto concerne le questioni relative alla competenza giurisdizionale e all'esecuzione; esprime vive preoccupazioni riguardo allo sviluppo di alcune applicazioni estremamente invasive che attribuiscono un punteggio sociale, poiché esse mettono seriamente a repentaglio il rispetto dei diritti fondamentali; chiede un divieto esplicito che impedisca alle autorità pubbliche di ricorrere all'attribuzione su larga scala di un punteggio sociale per limitare i diritti dei cittadini; chiede che sia rafforzata la responsabilità dei soggetti privati ai sensi del diritto internazionale, in considerazione dell'egemonia decisionale e del controllo che taluni soggetti privati hanno sullo sviluppo delle tecnologie in parola; invita a tale proposito la Commissione, il Consiglio e gli Stati membri a prestare particolare attenzione in sede di negoziazione, conclusione e ratifica di accordi internazionali in materia di controversie familiari transfrontaliere, come i casi internazionali di sottrazione di minori, nonché ad assicurare, al riguardo, che i sistemi di IA siano sempre impiegati sotto un effettivo controllo umano e rispettino il giusto processo, nell'UE e nei paesi firmatari di tali accordi;
73. chiede che il pubblico sia informato dell'uso dell'IA nel settore della giustizia e che tale uso non dia luogo a discriminazioni derivanti da distorsioni nella programmazione; sottolinea che deve essere rispettato il diritto di ogni persona di aver accesso a un pubblico ufficiale, nonché il diritto del pubblico ufficiale interessato di prendere personalmente la decisione e di discostarsi dalle informazioni ricevute dall'IA quando lo reputi necessario alla luce delle specificità della questione in esame; pone l'accento sul diritto della parte convenuta di impugnare la decisione conformemente al diritto nazionale, senza che venga mai meno la responsabilità finale del giudice;
74. chiede, pertanto, che tutti questi utilizzi in ambito pubblico e amministrativo siano considerati informazioni di pubblico dominio e che si evitino discriminazioni dovute a distorsioni nella programmazione;
75. pone l'accento sull'importanza di consentire una diffusione e un utilizzo corretti dell'IA;

invita gli Stati membri a offrire formazioni appropriate al personale civile e militare per consentirgli di individuare con precisione e di evitare le discriminazioni e le distorsioni negli insiemi di dati;

76. esprime profonda preoccupazione per le tecnologie di *deepfake*, che consentono di produrre foto, audio e video falsificati sempre più realistici che potrebbero essere utilizzati per compiere ricatti, creare notizie false o minare la fiducia dei cittadini e influenzare il dibattito pubblico; ritiene che tali pratiche siano in grado di destabilizzare paesi, diffondere la disinformazione e influenzare le consultazioni elettorali; chiede pertanto l'introduzione di un obbligo in base al quale tutti i materiali *deepfake* o altri video artificiali realizzati in modo realistico debbano essere etichettati come "non originali" dal loro creatore, con severi limiti al loro utilizzo a fini elettorali, e che tale obbligo sia applicato rigorosamente; chiede che siano svolte adeguate attività di ricerca in questo campo per garantire che le tecnologie di contrasto dei suddetti fenomeni siano al passo con gli utilizzi dolosi dell'IA;

Trasporti

77. prende atto del notevole potenziale economico delle applicazioni dell'IA, anche in relazione all'ottimizzazione a lungo termine delle prestazioni, alla manutenzione, alla previsione dei guasti e alla pianificazione della costruzione delle infrastrutture di trasporto e degli edifici, nonché sotto il profilo della sicurezza, dell'efficienza energetica e dei costi; invita dunque la Commissione a continuare a promuovere la ricerca nel campo dell'IA e lo scambio di buone prassi nel settore dei trasporti;
78. sottolinea la necessità di promuovere l'intelligenza artificiale per incentivare la multimodalità, l'interoperabilità e l'efficienza energetica di tutti i modi di trasporto, rendere più efficiente l'organizzazione e la gestione dei flussi di traffico merci e passeggeri, utilizzare in modo migliore le infrastrutture e le risorse in tutta la rete transeuropea di trasporto (TEN-T) e affrontare gli ostacoli alla creazione di un vero spazio unico europeo dei trasporti;
79. ricorda i benefici del sistema europeo di gestione del traffico ferroviario (ERTMS), un sistema continuo di protezione automatica dei treni, e sostiene lo sviluppo e la normalizzazione a livello internazionale dell'automazione delle operazioni ferroviarie;
80. accoglie con favore i lavori nel quadro del progetto di ricerca sulla gestione del traffico aereo nel cielo unico europeo (SESAR) concernenti i sistemi di aeromobili senza equipaggio e i sistemi di gestione del traffico aereo, sia civile che militare;
81. ricorda che i veicoli autonomi presentano un elevato potenziale in termini di miglioramento della mobilità e della sicurezza e apportano benefici ambientali, e invita la Commissione e gli Stati membri a garantire la cooperazione tra le autorità di regolamentazione e tutti gli attori pertinenti per la diffusione dei veicoli stradali automatizzati nell'UE;
82. sottolinea che negli ultimi anni il comparto mondiale della navigazione è notevolmente cambiato grazie all'integrazione dell'IA; ricorda le ampie discussioni in corso in seno all'Organizzazione marittima internazionale su un'efficace integrazione nel suo quadro normativo di tecnologie nuove ed emergenti quali le navi autonome;

83. sottolinea che i sistemi di trasporto intelligenti attenuano la congestione del traffico, aumentano la sicurezza e l'accessibilità e contribuiscono a migliorare la gestione dei flussi di traffico, l'efficienza e le soluzioni di mobilità; richiama l'attenzione sulla maggiore esposizione delle reti di trasporto tradizionali alle minacce informatiche; ricorda l'importanza di risorse adeguate e di ulteriori attività di ricerca sui rischi in termini di sicurezza per garantire la sicurezza dei sistemi automatizzati e dei relativi dati; accoglie con favore l'intenzione della Commissione di includere la sicurezza informatica come punto ricorrente all'ordine del giorno delle discussioni in seno alle organizzazioni internazionali del settore dei trasporti;
84. plaude agli sforzi volti a introdurre sistemi di IA nel settore pubblico e sosterrà la prosecuzione delle discussioni sulla diffusione dell'intelligenza artificiale nei trasporti; invita la Commissione a effettuare una valutazione del ricorso all'IA e a tecnologie simili nel settore dei trasporti e a compilare un elenco non esaustivo dei segmenti ad alto rischio dei sistemi di IA che si sostituiscono alle decisioni prese nel quadro delle prerogative dei pubblici poteri in questo settore;
85. sottolinea che il Fondo europeo per la difesa e la cooperazione strutturata permanente dovrebbero stimolare la cooperazione tra gli Stati membri e le industrie europee della difesa al fine di sviluppare nuove capacità di difesa europee nel settore dell'IA e garantire la sicurezza dell'approvvigionamento, tenendo conto di considerazioni etiche; pone l'accento sulla necessità di evitare la frammentazione creando ponti tra i vari attori e settori di applicazione, promuovendo la compatibilità e l'interoperabilità a tutti i livelli e concentrandosi sul fatto di lavorare insieme sull'architettura e le soluzioni di piattaforme; ricorda inoltre che il prossimo meccanismo per collegare l'Europa, che promuove anche le infrastrutture intelligenti, prevede un fondo per l'adattamento e lo sviluppo di infrastrutture di trasporto civili o militari a duplice uso nelle TEN-T al fine di aumentare le sinergie tra esigenze civili e di difesa e di migliorare la mobilità civile e militare all'interno dell'Unione; evidenzia, pertanto, la necessità di ulteriori investimenti e attività di ricerca nonché di una maggiore leadership da parte europea nelle tecnologie che, oltre ad avere un forte impatto sulla crescita economica, hanno anche un notevole potenziale in termini di duplice uso;
86. sottolinea che nel settore dei trasporti e della mobilità molti investimenti nelle nuove tecnologie sono indotti dal mercato, ma che le tecnologie e i prodotti a duplice uso disponibili in commercio sono spesso utilizzati in modo innovativo per scopi militari; evidenzia dunque la necessità di tenere conto del potenziale di duplice uso delle soluzioni basate sull'IA in sede di definizione delle norme per l'uso dell'IA in vari ambiti del comparto commerciale e militare; chiede che nella messa a punto di tecnologie, prodotti e principi operativi della difesa siano integrati norme e principi etici rigorosi;
87. osserva che il trasporto efficace di merci, munizioni, armamenti e truppe è una componente essenziale per il successo delle operazioni militari; sottolinea che ci si attende che l'IA svolgerà un ruolo cruciale e offrirà numerose possibilità nel campo della logistica e del trasporto militari; segnala che in tutto il mondo gli Stati, compresi gli Stati membri dell'UE, stanno integrando armi e altri sistemi basati sull'intelligenza artificiale nelle piattaforme terrestri, navali e aeree; ricorda che le applicazioni dell'IA nel settore dei trasporti potrebbero assicurare nuove capacità e consentire nuove forme di tattica, come la combinazione di più sistemi, quali droni, imbarcazioni o carri armati senza equipaggio, in operazioni indipendenti e coordinate;

Diritto internazionale privato

88. osserva che l'internazionalizzazione delle attività umane, online o nel mondo reale, comporta un aumento costante delle controversie rientranti nel diritto internazionale privato, controversie che l'IA può aiutare a risolvere creando modelli per individuare la giurisdizione competente e il diritto applicabile in ciascun caso, ma anche per identificare i conflitti di leggi più spinosi e proporre soluzioni per risolverli;
89. ritiene, tuttavia, che il pubblico debba essere debitamente informato circa gli impieghi dell'IA nel campo del diritto internazionale privato e che tali impieghi debbano evitare discriminazioni dovute alla programmazione - che favorirebbero sistematicamente un diritto nazionale a scapito di un altro -, rispettare i diritti del giudice predeterminato dalla legge, consentire possibilità di ricorso a norma della legge applicabile e permettere al giudice di ignorare la soluzione suggerita dall'IA;
90. sottolinea che la circolazione di veicoli autonomi nell'Unione europea, che è suscettibile di dar luogo a un numero particolarmente elevato di controversie internazionali private, deve essere oggetto di specifiche norme europee che stabiliscano il regime giuridico applicabile in caso di danni transfrontalieri;
91. segnala che, a seguito della crescente importanza delle attività di ricerca e sviluppo del settore privato e dei massicci investimenti di paesi terzi, l'UE si trova confrontata a una forte concorrenza; appoggia dunque gli sforzi profusi dall'UE per sviluppare ulteriormente i suoi vantaggi competitivi e ritiene che, in un mondo iperconnesso, l'Unione dovrebbe puntare ad assumere un ruolo guida nell'elaborazione delle norme relative all'IA, adottando una strategia efficace nei confronti dei suoi partner esterni e intensificando gli sforzi volti a stabilire norme etiche globali per l'IA a livello internazionale che siano in linea con le norme di sicurezza e i requisiti in materia di protezione dei consumatori, nonché con i valori dell'Unione e i diritti dei suoi cittadini, inclusi i diritti fondamentali; ritiene che ciò sia essenziale anche ai fini della competitività e della sostenibilità delle imprese europee; invita la Commissione e gli Stati membri a rafforzare la cooperazione con i paesi terzi e le organizzazioni internazionali, quali l'ONU, l'OCSE, il G7 e il G20, e ad avviare un dialogo più ampio per affrontare le sfide derivanti dallo sviluppo di questa tecnologia in rapida evoluzione; ritiene che tali sforzi dovrebbero puntare, in particolare, alla definizione di norme comuni e al miglioramento dell'interoperabilità dei sistemi basati sull'IA; invita la Commissione a promuovere il dialogo, una più stretta cooperazione e sinergie tra Stati membri, ricercatori, accademici, attori della società civile, settore privato, in particolare le imprese leader, e settore militare per garantire che i processi decisionali riguardanti la regolamentazione dell'IA nel settore della difesa siano inclusivi;

Principi guida

92. ritiene che le tecnologie di IA e i sistemi di rete dovrebbero mirare a garantire ai cittadini la certezza del diritto; sottolinea, pertanto, che le norme in materia di conflitto tra leggi e giurisdizioni dovrebbero continuare ad applicarsi, tenendo conto al contempo degli interessi dei cittadini e della necessità di ridurre il rischio di scelta opportunistica del foro; rammenta che l'IA non può sostituirsi agli esseri umani nei procedimenti giudiziari quando si tratta di pronunciare sentenze o adottare decisioni definitive, di qualsiasi tipo esse siano, poiché tali decisioni devono essere sempre prese da un essere umano ed essere soggette a una rigorosa verifica umana nonché alla garanzia del giusto

processo; insiste sul fatto che, quando vengono utilizzati elementi di prova forniti da tecnologie basate sull'IA, le autorità giudiziarie dovrebbero essere tenute a motivare le loro decisioni;

93. ricorda che l'IA costituisce un progresso scientifico che non deve minare il diritto bensì, al contrario, deve essere sempre disciplinata da quest'ultimo — nell'Unione europea dal diritto delle sue istituzioni e dei suoi Stati membri — e che, in nessun caso, l'intelligenza artificiale, la robotica e le tecnologie a esse correlate possono violare i diritti fondamentali, la democrazia, lo Stato di diritto;
94. sottolinea che gli usi dell'IA a fini di difesa dovrebbero essere responsabili, equi, tracciabili, affidabili e governabili;
95. ritiene che l'intelligenza artificiale, la robotica e le tecnologie correlate, compresi i software, gli algoritmi e i dati utilizzati o prodotti da tali tecnologie, a prescindere dal settore di utilizzo, debbano essere sviluppati in modo sicuro e tecnicamente rigoroso;

o

o o

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