



TEXTES ADOPTÉS

P9_TA(2021)0009

Intelligence artificielle: questions relatives à l'interprétation et à l'application du droit international

Résolution du Parlement européen du 20 janvier 2021 sur l'intelligence artificielle: questions relatives à l'interprétation et à l'application du droit international dans la mesure où l'Union est concernée dans les domaines des utilisations civiles et militaires ainsi qu'à l'autorité de l'État en dehors du champ d'application de la justice pénale (2020/2013(INI))

Le Parlement européen,

- vu le préambule et les articles 2, 3, 10, 19, 20, 21, 114, 167, 218, 225 et 227 du traité sur l'Union européenne,
- vu le droit de pétition consacré par les articles 20 et 227 du traité sur le fonctionnement de l'Union européenne,
- vu la charte des droits fondamentaux de l'Union européenne,
- vu la directive 2000/43/CE du Conseil du 29 juin 2000 relative à la mise en œuvre du principe de l'égalité de traitement entre les personnes sans distinction de race ou d'origine ethnique¹ (directive relative à l'égalité raciale),
- vu la directive 2000/78/CE du Conseil du 27 novembre 2000 portant création d'un cadre général en faveur de l'égalité de traitement en matière d'emploi et de travail² (directive sur l'égalité de traitement en matière d'emploi),
- vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)³ (RGPD), et la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de

¹ JO L 180 du 19.7.2000, p. 22.

² JO L 303 du 2.12.2000, p. 16.

³ JO L 119 du 4.5.2016, p. 1.

sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil¹,

- vu le règlement (UE) 2018/1488 du Conseil du 28 septembre 2018 établissant l'entreprise commune pour le calcul à haute performance européen²,
- vu la proposition de règlement du Parlement européen et du Conseil du 6 juin 2018 établissant le programme pour une Europe numérique pour la période 2021-2027 (COM(2018)0434),
- vu sa résolution du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique³,
- vu sa résolution du 1^{er} juin 2017 sur le passage au numérique des entreprises européennes⁴,
- vu sa résolution du 12 septembre 2018 sur les systèmes d'armes autonomes⁵,
- vu sa résolution du 11 septembre 2018 sur l'égalité des langues à l'ère numérique⁶,
- vu sa résolution du 12 février 2019 sur une politique industrielle européenne globale sur l'intelligence artificielle (IA) et la robotique⁷,
- vu la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions du 11 décembre 2019 sur le pacte vert pour l'Europe (COM(2019)0640),
- vu le livre blanc de la Commission du 19 février 2020 intitulé «Intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance» (COM(2020)0065),
- vu la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 19 février 2020 intitulée «Une stratégie européenne pour les données» (COM(2020)0066),
- vu la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 19 février 2020 intitulée «Façonner l'avenir numérique de l'Europe» (COM(2020)0067),
- vu le rapport du 8 avril 2019 élaboré par le groupe d'experts de haut niveau sur l'intelligence artificielle constitué par la Commission en juin 2018, rapport intitulé «Lignes directrices en matière d'éthique pour une IA digne de confiance»,
- vu la convention-cadre du Conseil de l'Europe pour la protection des minorités nationales, le protocole n° 12 à la convention de sauvegarde des droits de l'homme et

¹ JO L 119 du 4.5.2016, p. 89.

² JO L 252 du 8.10.2018, p. 1.

³ JO C 252 du 18.7.2018, p. 239.

⁴ JO C 307 du 30.8.2018, p. 163.

⁵ JO C 433 du 23.12.2019, p. 86.

⁶ JO C 433 du 23.12.2019, p. 42.

⁷ JO C 449 du 23.12.2020, p. 37.

des libertés fondamentales et la charte européenne des langues régionales ou minoritaires,

- vu la charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement, adoptée par le groupe de travail sur la qualité de la justice du Conseil de l'Europe (CEPEJ-GT-QUAL) en décembre 2018,
- vu la recommandation du Conseil de l'OCDE sur l'intelligence artificielle adoptée le 22 mai 2019,
- vu l'article 54 de son règlement intérieur,
- vu les avis de la commission des affaires étrangères, de la commission du marché intérieur et de la protection des consommateurs, de la commission des transports et du tourisme et de la commission des libertés civiles, de la justice et des affaires intérieures,
- vu le rapport de la commission des affaires juridiques (A9-0001/2021),

Introduction

- A. considérant que l'intelligence artificielle (IA), la robotique et les technologies connexes se développent rapidement et sont susceptibles d'avoir une incidence directe sur tous les aspects de nos sociétés, y compris les valeurs et les principes sociaux et économiques de base;
- B. considérant que l'IA révolutionne totalement la doctrine et la pratique militaires par un changement profond dans la façon dont les armées opèrent, du fait notamment de l'intégration et de l'exploitation de nouvelles technologies et de capacités autonomes;
- C. considérant que le développement et la conception de l'«intelligence artificielle», de la robotique et des technologies connexes sont le fait de l'être humain, et que ce sont les choix qu'il effectue qui déterminent les avantages potentiels de la technologie pour la société;
- D. considérant qu'un cadre commun de l'Union doit couvrir le développement, le déploiement et l'utilisation de l'IA, de la robotique et des technologies connexes, et doit garantir le respect de la dignité humaine et des droits de l'homme, tels qu'ils sont consacrés dans la charte des droits fondamentaux de l'Union européenne;
- E. considérant que l'Union et ses États membres ont la responsabilité particulière de veiller à ce que l'IA, la robotique et les technologies connexes – compte tenu du fait qu'elles peuvent être utilisées par-delà les frontières – soient centrées sur l'humain, c'est-à-dire à ce qu'elles soient destinées à être utilisées au bénéfice de l'humanité et du bien commun et aient pour but de contribuer au bien-être et à l'intérêt général de leurs citoyens; que l'Union doit aider les États membres à relever ce défi, en particulier ceux qui ont commencé à réfléchir à l'évolution éventuelle de normes juridiques ou à des modifications législatives dans ce domaine;
- F. considérant que les citoyens européens pourraient bénéficier d'une approche réglementaire appropriée, efficace, transparente et cohérente au niveau de l'Union qui définisse des conditions suffisamment claires pour que les entreprises mettent au point des applications et planifient leurs modèles d'entreprise, tout en veillant à ce que

l'Union et ses États membres conservent le contrôle des réglementations, afin qu'ils ne soient pas obligés d'adopter ou d'accepter des normes fixées par d'autres;

- G. considérant que les lignes directrices en matière d'éthique, telles que les principes adoptés par le groupe d'experts de haut niveau sur l'intelligence artificielle, constituent un bon point de départ mais qu'elles ne sont pas suffisantes pour garantir que les entreprises agissent loyalement et assurent la protection effective des individus;
- H. considérant que cette responsabilité particulière implique notamment d'examiner les questions relatives à l'interprétation et à l'application du droit international dans le cadre de la participation active de l'Union européenne aux négociations internationales, dans la mesure où l'Union est concernée par les utilisations civiles et militaires de ce type d'IA, de robotique et de technologies connexes, et que les questions relatives à l'autorité de l'État vis-à-vis de ces technologies se situent en dehors du champ d'application de la justice pénale;
- I. considérant qu'il est essentiel de fournir un cadre juridique approprié et complet pour les aspects éthiques de ces technologies ainsi que pour la responsabilité, la transparence et l'obligation de rendre des comptes (en particulier pour l'IA, la robotique et les technologies connexes considérées comme à haut risque); que ce cadre doit refléter le fait que les valeurs humanistes intrinsèquement européennes et universelles sont applicables à l'ensemble de la chaîne de valeur dans le cadre du développement, de la mise en œuvre et de l'utilisation de l'IA; que ce cadre éthique doit s'appliquer au développement (y compris à la recherche et à l'innovation), au déploiement et à l'utilisation de l'IA, dans le plein respect du droit de l'Union et des valeurs énoncées dans la charte des droits fondamentaux de l'Union européenne;
- J. considérant que cet examen a pour but de rechercher dans quelle mesure les règles du droit international, tant public que privé, et du droit de l'Union sont adaptées à ces technologies, ainsi que de mettre en lumière les défis et les risques auxquels ces dernières confrontent l'autorité de l'État, de sorte que la gestion de ces défis et risques puisse s'effectuer de manière appropriée et proportionnée;
- K. considérant que la Commission européenne ne tient pas compte des aspects militaires de l'utilisation de l'intelligence artificielle dans son livre blanc;
- L. considérant qu'une approche européenne harmonisée de ces problèmes nécessite d'adopter une définition commune de l'intelligence artificielle et de veiller à ce que les valeurs fondamentales de l'Union européenne, les principes de la charte des droits fondamentaux de l'Union européenne et la législation internationale sur les droits de l'homme soient respectés;
- M. considérant que l'IA offre des possibilités sans précédent d'améliorer les performances du secteur des transports, puisqu'elle permet de répondre à la demande croissante de déplacements et aux préoccupations en matière de sécurité et d'environnement, tout en rendant tous les modes de transport plus intelligents, plus efficaces et plus pratiques;
- N. considérant qu'il est indispensable, pour renforcer les capacités de l'Union dans ce secteur, de soulever la question de l'IA dans le domaine de la défense au niveau européen;

Définition de l'intelligence artificielle

1. estime qu'il est nécessaire d'adopter un cadre juridique européen commun assorti de définitions harmonisées et de principes éthiques communs, y compris pour l'utilisation de l'IA à des fins militaires; invite par conséquent la Commission à adopter les définitions suivantes:
 - «système d'IA», un système qui est soit fondé sur des logiciels, soit intégré dans des dispositifs matériels, et qui affiche un comportement simulant l'intelligence, notamment en collectant et en traitant des données, en analysant et en interprétant son environnement et en agissant, avec un certain degré d'autonomie, pour atteindre des objectifs spécifiques;
 - «autonome», un système d'IA qui fonctionne en interprétant certaines données entrées et en utilisant un ensemble d'instructions prédéterminées, sans se limiter à de telles instructions, bien que le comportement du système vise à atteindre l'objectif qui lui a été assigné et qu'il soit soumis aux contraintes découlant de cet objectif et d'autres choix de conception posés par son développeur;
2. souligne que les politiques de sécurité et de défense de l'Union européenne et de ses États membres sont guidées par les principes consacrés par la charte des droits fondamentaux de l'Union européenne et la charte des Nations unies – cette dernière invitant l'ensemble des États à s'abstenir, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force – ainsi que par le droit international, par les principes des droits de l'homme et du respect de la dignité humaine, et par une compréhension commune des valeurs universelles que constituent les droits inviolables et inaliénables de la personne humaine, la liberté, la démocratie, l'égalité et l'état de droit; observe que toutes les activités liées à la défense dans le cadre de l'Union doivent respecter ces valeurs universelles tout en prônant la paix, la stabilité, la sécurité et le progrès, tant en Europe que dans le monde;

Droit international public et utilisations militaires de l'intelligence artificielle

3. considère que l'IA utilisée dans un contexte militaire et civil doit faire l'objet d'un véritable contrôle humain, de sorte qu'à tout moment, une personne humaine ait la possibilité de la corriger, de l'interrompre ou de la désactiver en cas de comportement imprévu, d'intervention accidentelle, de cyberattaques, d'ingérence de tiers dans une technologie fondée sur l'IA ou d'acquisition par des tiers d'une telle technologie;
4. estime que le respect du droit international public, en particulier du droit humanitaire, qui s'applique sans équivoque à tous les systèmes d'armes et à leurs opérateurs, est une exigence fondamentale à laquelle les États membres doivent se conformer, notamment lorsqu'il s'agit de protéger la population civile ou de prendre des mesures de précaution en cas d'attaque telle que l'agression militaire ou la cyberguerre;
5. souligne que l'IA et les technologies connexes peuvent également jouer un rôle dans la guerre irrégulière ou non conventionnelle; suggère que la recherche, le développement et l'utilisation de l'IA dans ces cas de figure soient soumis aux mêmes conditions que son utilisation dans des conflits conventionnels;

6. souligne que le recours à l'IA est l'occasion de renforcer la sécurité de l'Union européenne et de ses citoyens et qu'il est essentiel que l'Union adopte une démarche cohérente dans les prochains débats qui auront lieu à ce sujet au niveau international;
7. invite la communauté des chercheurs dans le domaine de l'IA à intégrer ce principe dans tous les systèmes précités fondés sur l'IA et destinés à un usage militaire; estime qu'aucune autorité ne peut établir d'exception à ces principes ou certifier un tel système;
8. réaffirme que la prise de décision autonome ne devrait pas exonérer l'être humain de sa responsabilité et que les humains doivent toujours assumer la responsabilité ultime des processus de prise de décision, de sorte que l'identité de la personne responsable de la décision puisse être établie;
9. souligne que lors du recours à l'IA dans un contexte militaire, les États membres, les parties à un conflit et les particuliers doivent, à tout moment, respecter les obligations qui leur incombent en vertu du droit international applicable et assumer la responsabilité des actions résultant de l'utilisation de ces systèmes; souligne qu'en toutes circonstances, les actions et effets prévisibles, accidentels ou indésirables des systèmes fondés sur l'IA doivent être considérés comme relevant de la responsabilité des États membres, des parties à un conflit et des individus;
10. se félicite des possibilités d'utiliser les systèmes d'intelligence artificielle à des fins de formation et d'exercices, dont le potentiel ne doit pas être sous-estimé, d'autant plus que l'Union mène des exercices à double caractère civil et militaire;
11. met l'accent sur la nécessité de prendre dûment en compte à tout moment, lors des phases de conception, de développement, d'essai, de déploiement et d'utilisation de systèmes fondés sur l'IA, les risques potentiels, notamment celui de victimes collatérales parmi la population civile, de pertes accidentelles de vies humaines et de dommages aux infrastructures civiles, ainsi que les risques liés à l'engagement involontaire, à la manipulation, à la prolifération, aux cyberattaques, à l'ingérence de tiers dans une technologie autonome fondée sur l'IA et à l'acquisition par des tiers d'une telle technologie;
12. rappelle que le principe de nouveauté, conformément à l'avis consultatif de la Cour internationale de Justice du 8 juillet 1996, ne peut être invoqué en soutien à une quelconque dérogation quant au respect des normes actuelles du droit international humanitaire;
13. estime que l'IA, en plus de soutenir les opérations, profitera également aux membres des forces armées en traitant massivement les données relatives à leur santé et en étendant la surveillance de leur santé, recensera les facteurs de risque liés à leur environnement et à leurs conditions de travail et proposera des garanties appropriées pour limiter les incidences sur la santé du personnel militaire;
14. réaffirme que les efforts réglementaires doivent être soutenus par des systèmes de certification et de surveillance rigoureux, ainsi que par des mécanismes clairs d'audit, d'explication, de responsabilité et de traçabilité, afin que le cadre réglementaire ne soit pas dépassé par les évolutions technologiques;

15. souligne l'importance que revêt, dans un monde hyperconnecté, la participation de l'Union européenne à la création d'un cadre juridique international pour l'utilisation de l'intelligence artificielle; invite instamment l'Union à prendre l'initiative et à jouer, avec les Nations unies et la communauté internationale, un rôle actif dans la promotion de ce cadre mondial régissant l'utilisation de l'IA à des fins militaires ou autres, en veillant à ce que cette utilisation observe les limites strictes fixées par le droit international et le droit humanitaire international, en particulier les conventions de Genève du 12 août 1949; souligne que ce cadre ne doit jamais enfreindre ou autoriser d'enfreindre les exigences de la conscience publique et le principe d'humanité tels que figurant dans la clause de Martens, et qu'il doit respecter les règles de sécurité et les exigences de protection des consommateurs; demande instamment à l'Union et aux États membres de définir des systèmes robustes de surveillance et d'évaluation pour le développement des technologies d'IA, en particulier celles utilisées à des fins militaires dans des États autoritaires;
16. souligne que la robotique permettra non seulement au personnel militaire de rester à distance, mais aussi d'offrir une meilleure autoprotection, par exemple dans le cadre d'opérations dans des environnements contaminés, de la lutte contre les incendies, du déminage sur terre ou en mer et de la défense contre les essaims de drones;
17. souligne que le développement, le déploiement, l'utilisation et la gestion de l'IA doivent respecter les droits fondamentaux, les valeurs et les libertés consacrés par les traités de l'Union, et invite les États membres à s'abstenir de déployer des systèmes d'IA à haut risque susceptibles de menacer les droits fondamentaux; prend acte de la publication du livre blanc de la Commission sur l'intelligence artificielle et demande que les risques potentiels, pour les droits fondamentaux, liés à l'utilisation de l'IA par les pouvoirs publics et par les institutions, organes et organismes de l'Union soient examinés de manière plus approfondie;
18. invite la Commission à faciliter la recherche sur les possibilités qu'offre l'utilisation de l'IA dans le cadre des opérations de secours en cas de catastrophe, de la prévention des crises et du maintien de la paix, et à encourager le débat sur ce sujet;
19. se félicite de la création d'un groupe d'experts gouvernementaux des Nations unies chargé de promouvoir un comportement responsable des États dans le cyberspace dans le contexte de la sécurité internationale et invite l'Union à participer pleinement à ses travaux;
20. invite le vice-président de la Commission / haut représentant pour les affaires étrangères et la politique de sécurité (VP/HR) à ouvrir la voie à des négociations mondiales en vue de mettre en place un régime de contrôle des armes recourant à l'IA et de mettre à jour tous les instruments existants prévus par les traités relatifs au contrôle des armes, au désarmement et à la non-prolifération afin de prendre en compte les systèmes fondés sur l'IA utilisés en temps de guerre; demande que la position commune du Conseil définissant des règles communes régissant le contrôle des exportations de technologie et d'équipements militaires tienne pleinement compte des systèmes d'armes fondés sur l'IA et s'y applique;
21. réaffirme que ces règles doivent toujours respecter les principes, rappelés par la convention de Rome du 17 juillet 1998, de prohibition des crimes de génocide, des crimes contre l'humanité et des crimes de guerre;

22. met l'accent sur les risques manifestes qu'implique toute décision prise par un être humain qui s'appuierait exclusivement sur des données, des profils et des recommandations générés par des machines; met l'accent sur le fait que la conception globale des systèmes d'IA devrait également intégrer des lignes directrices sur la supervision et la surveillance humaines; demande que soient imposées une obligation en matière de transparence et d'explicabilité des applications d'IA, ainsi que la nécessité d'une intervention humaine, et que d'autres mesures soient prévues, comme des audits indépendants et des tests de résistance spécifiques visant à faciliter et à assurer le respect de la conformité; souligne que ces audits devraient être effectués périodiquement par une autorité indépendante qui superviserait les applications d'IA à haut risque utilisées par les pouvoirs publics ou les autorités militaires;
23. souligne qu'il importe de vérifier par quel procédé les technologies d'IA à haut risque parviennent à des décisions; rappelle que les principes de non-discrimination et de proportionnalité doivent être respectés et que les questions de causalité, de responsabilité, de transparence, d'obligation de rendre compte et d'explicabilité doivent être clarifiées pour déterminer si, et dans quelle mesure, l'État, en tant que sujet de droit international et autorité souveraine, peut agir avec l'aide de systèmes d'IA dotés d'une certaine autonomie sans enfreindre les obligations découlant du droit international, telles que le droit à un procès équitable;
24. insiste sur l'importance d'investir dans les compétences humaines, y compris dans le domaine numérique, pour permettre aux personnes qui exercent des professions réglementées, y compris des activités liées à l'exercice de l'autorité de l'État, comme l'administration de la justice, de s'adapter aux avancées scientifiques en matière de solutions fondées sur l'IA; invite les États membres et la Commission à en tenir dûment compte dans le cadre de la mise en œuvre de la directive 2005/36/CE¹;
25. insiste sur le fait que les systèmes d'IA doivent toujours respecter les principes de responsabilité, d'équité, de gouvernabilité, de précaution, d'obligation de rendre compte, d'imputabilité, de prévisibilité, de traçabilité, de fiabilité, de loyauté, de transparence, d'explicabilité, de capacité à détecter d'éventuels changements de circonstances et d'environnement opérationnel, de distinction entre combattants et non-combattants, et de proportionnalité; souligne que ce dernier principe subordonne la légalité d'une action militaire au respect d'un équilibre entre l'objectif poursuivi et les moyens utilisés, et que l'appréciation de cette proportionnalité doit toujours émaner d'une personne humaine;
26. souligne que, lors de l'utilisation de systèmes fondés sur l'IA dans le domaine de la sécurité et de la défense, la pleine compréhension de la situation par l'opérateur humain, la prévisibilité, la fiabilité et la résilience du système fondé sur l'IA ainsi que la capacité de l'opérateur humain à détecter d'éventuels changements de circonstances et d'environnement opérationnel et sa capacité à intervenir lors d'une attaque ou à y mettre fin sont nécessaires pour garantir que les principes du droit international humanitaire, en particulier de discrimination, de proportionnalité et de précaution lors d'une attaque, soient pleinement appliqués tout au long de la chaîne de commandement et de contrôle; souligne que les systèmes fondés sur l'IA doivent permettre aux humains qui en ont la responsabilité d'exercer un véritable contrôle, d'assumer une responsabilité pleine et

¹ Directive 2005/36/CE du Parlement européen et du Conseil du 7 septembre 2005 relative à la reconnaissance des qualifications professionnelles (JO L 255 du 30.9.2005, p. 22).

entière à l'égard de ces systèmes et de répondre de toutes leurs utilisations; invite la Commission à favoriser le dialogue, une coopération plus étroite et des synergies entre les États membres, les chercheurs, les universitaires, les acteurs de la société civile, le secteur privé, en particulier les entreprises de premier plan, et les forces militaires, pour garantir le caractère inclusif des processus d'élaboration des règles relatives à l'IA appliquée à la défense;

27. souligne que le Parlement a demandé l'élaboration et l'adoption, dans les plus brefs délais, d'une position commune sur les systèmes d'armes létales autonomes (SALA) empêchant la mise au point, la production et l'utilisation de SALA capables d'effectuer des frappes sans véritable contrôle humain, et a réclamé l'ouverture de négociations effectives en vue de leur interdiction; rappelle à cet égard sa résolution du 12 septembre 2018 sur les systèmes d'armes autonomes; rappelle que l'expression «systèmes d'armes létales autonomes» (SALA) désigne des systèmes d'armes dépourvus de véritable contrôle humain sur les fonctions critiques de sélection et d'attaque de cibles individuelles; souligne que la décision de sélectionner une cible et d'entreprendre une action létale au moyen de systèmes d'armes présentant un certain niveau d'autonomie doit toujours être prise par des opérateurs humains exerçant un contrôle et une surveillance véritables ainsi que le jugement nécessaire, conformément aux principes de proportionnalité et de nécessité; souligne que les systèmes fondés sur l'IA ne peuvent en aucun cas se substituer à la décision humaine dans ce domaine;
28. relève de surcroît que les systèmes d'armes autonomes, en tant que catégorie particulière de l'IA dans le domaine militaire, devraient faire l'objet de débats et d'un accord international, en particulier dans le cadre de la convention des Nations unies sur certaines armes classiques; rappelle que le débat international en cours sur les SALA visant à réglementer les nouvelles technologies militaires n'a pas encore abouti à un accord; souligne que l'Union n'a accepté que récemment de discuter des implications de l'évolution de l'IA et de la numérisation dans le secteur de la défense; estime que l'Union européenne peut jouer un rôle crucial pour aider les États membres à harmoniser leur stratégie en matière d'IA militaire, afin de mener des pourparlers à l'échelle internationale;
29. insiste sur la nécessité d'une stratégie à l'échelle de l'Union contre les SALA et d'une interdiction des «robots tueurs»;
30. souligne que l'IA utilisée dans un contexte militaire doit répondre à un ensemble minimal d'exigences, à savoir: être en mesure de faire la distinction entre combattants, non-combattants et combattants sur le champ de bataille, reconnaître lorsqu'un combattant se rend ou est hors de combat, ne pas avoir d'effets indiscriminés, ne pas causer de souffrances inutiles aux personnes, ne pas être partielle ou formée sur des données délibérément incomplètes, et respecter les principes du droit humanitaire international, la proportionnalité dans le recours à la force et la précaution avant l'intervention;
31. estime que l'utilisation de systèmes d'armes létales autonomes soulève des questions éthiques et juridiques fondamentales quant à la capacité des êtres humains à contrôler ces systèmes, et exige que les technologies fondées sur l'IA ne soient pas en mesure de prendre des décisions autonomes impliquant les principes juridiques de distinction, de proportionnalité et de précaution;

32. demande que des mesures transparentes de réduction des risques portant sur le développement et l'utilisation de l'IA à des fins militaires soient prises au niveau international, en particulier en ce qui concerne les principes d'intégrité territoriale, de non-intervention et de recours à la force; souligne qu'il importe de prendre en considération les aspects militaires lors de l'examen des questions juridiques et éthiques dans le cadre européen relatif à l'IA; rappelle sa position sur l'interdiction de la mise au point, de la production et de l'utilisation de SALA; déplore qu'il n'existe pas, à l'échelle mondiale, de convention qui se prononce de manière explicite sur l'utilisation de ces armes;
33. reconnaît que la dynamique moderne résultant de la course aux armements entre les principaux États nations militaires qui développent des SALA connaît un rythme plus rapide que la mise en place, l'application et l'exécution efficaces et universelles de règles et de cadres juridiques communs, parce que l'information sur le développement et le déploiement de ces systèmes est classifiée et que les États nations ont un intérêt propre à créer les capacités offensives les plus rapides et les plus efficaces, indépendamment des cadres ou principes juridiques actuels et potentiels futurs;
34. estime que les SALA ne doivent être utilisés qu'en dernier ressort et ne sont licites qu'à condition d'être soumis à un contrôle humain strict, permettant à une personne humaine d'en reprendre le commandement à tout moment, étant donné qu'une véritable intervention et une véritable surveillance humaine sont essentielles dans les processus de décision susceptibles d'avoir des conséquences mortelles, et que la responsabilité de décisions entre la vie et la mort devrait toujours incomber à des êtres humains; est convaincu que les systèmes totalement soustraits à un contrôle humain («*human off the loop*») et à une surveillance humaine doivent être interdits sans aucune exception et en toutes circonstances;
35. invite le VP/HR, les États membres et le Conseil européen à élaborer et à adopter urgemment une position commune sur les systèmes d'armes autonomes qui garantisse un véritable contrôle humain sur les fonctions critiques des systèmes d'armes, y compris pendant le déploiement, à s'exprimer d'une seule voix dans les enceintes pertinentes et à agir en conséquence; invite, dans ce contexte, le VP/HR, les États membres et le Conseil à partager leurs bonnes pratiques et à recueillir les contributions d'experts, de scientifiques et de la société civile, comme indiqué dans sa résolution du 12 septembre 2018 sur les systèmes d'armes autonomes, qui précise que les attaques doivent toujours reposer sur une véritable intervention humaine;
36. encourage tous les États à procéder à une évaluation pour savoir si et de quelle manière les dispositifs militaires autonomes ont contribué à leur sécurité nationale et connaître le bénéfice que leur sécurité nationale pourrait tirer des systèmes d'armement fondés sur l'IA, en particulier en ce qui concerne le potentiel de ces technologies pour soutenir et améliorer la prise de décision humaine dans le respect du droit humanitaire international et de ses principes; rappelle que tout SALA ou toute arme au niveau d'autonomie élevé peut présenter un dysfonctionnement en raison d'un mauvais codage ou d'une cyberattaque commise par un État ennemi ou un acteur non étatique;
37. insiste pour que les SALA ne soient utilisés que dans des cas précis et selon des procédures d'autorisation fixées à l'avance de façon détaillée dans des textes dont l'État concerné – qu'il soit membre ou non de l'Organisation du traité de l'Atlantique Nord – assure l'accessibilité au public, ou au moins à son parlement national;

38. estime que les SALA doivent respecter les dispositions de la convention du 10 octobre 1980 sur certaines armes classiques, notamment l'interdiction de produire des «effets traumatiques excessifs»;
39. suggère, afin d'éviter leur dissémination incontrôlée, que les SALA soient inscrits dans la liste des armes soumises aux dispositions du traité sur le commerce des armes du 2 avril 2013, liste figurant à l'article 2 dudit traité;
40. réclame, pour éviter toute confusion entre une personne humaine et un robot, l'interdiction de l'anthropomorphisation des SALA;
41. se félicite à cet égard de l'accord conclu entre le Conseil et le Parlement pour exclure des actions financées au titre du Fonds européen de défense (FED) les armes létales autonomes «sans la possibilité d'un contrôle humain significatif sur les décisions de sélection et d'engagement prises dans le cadre de frappes»; rappelle sa position selon laquelle l'utilisation, le développement et la production de SALA sans véritable contrôle humain ne peuvent pas bénéficier d'un financement au titre du FED;
42. invite la Commission à soutenir la recherche, le développement, le déploiement et l'utilisation de l'IA dans le cadre du maintien de la paix et de la prévention des conflits;
43. signale que l'écosystème mondial de l'IA est dominé par les géants du numérique américains et chinois, qui renforcent leurs capacités nationales et achètent de nombreuses entreprises prometteuses; est dès lors fermement convaincu que, pour éviter de rester à la traîne dans le domaine des technologies de l'intelligence artificielle, l'Union européenne doit œuvrer à un meilleur équilibre entre la recherche fondamentale et les applications industrielles, tout en développant ses avantages stratégiques comparatifs par l'accroissement de son propre potentiel et de ses propres ressources;
44. souligne que, dans la mesure où ils relèvent de la définition des machines figurant dans la directive 2006/42/CE¹, les robots devraient être conçus et assemblés conformément aux normes et aux mesures de sécurité qui y sont prévues;
45. rappelle l'ambition de l'Union de se poser en acteur pour la paix au niveau mondial et l'exhorte à s'engager davantage dans le désarmement et la non-prolifération sur la scène internationale; demande à l'Union de s'efforcer, par ses politiques, de maintenir la paix et la sécurité internationales, de garantir le respect du droit international des droits de l'homme et du droit humanitaire ainsi que la protection des civils et des infrastructures civiles;
46. souligne la nécessité d'examiner l'incidence que peut avoir l'IA, en tant que facteur stratégique, sur la politique de sécurité et de défense commune (PSDC) de l'Union, en particulier en ce qui concerne les missions et les opérations militaires et civiles ainsi que le renforcement des capacités de l'Union;
47. rappelle que nos alliés, que ce soit au niveau national, dans le cadre de l'OTAN ou de l'Union, sont eux-mêmes en train d'intégrer l'IA dans leurs systèmes militaires; estime qu'il y a lieu de préserver l'interopérabilité avec nos alliés à travers des normes communes, qui sont essentielles pour la conduite des opérations en coalition; rappelle

¹ Directive 2006/42/CE du Parlement européen et du Conseil du 17 mai 2006 relative aux machines et modifiant la directive 95/16/CE (JO L 157 du 9.6.2006, p. 24).

par ailleurs que la coopération en matière d'IA devrait se faire dans un cadre européen, seul cadre pertinent pour créer véritablement de puissantes synergies, comme proposé par la stratégie de l'Union en matière d'IA;

48. estime que l'Union doit suivre et examiner de près les implications des progrès de l'IA pour la défense et la guerre, y compris les développements et les déploiements potentiellement déstabilisateurs, et fournir des orientations en matière de recherche et de conception éthiques, en garantissant l'intégrité des données à caractère personnel, l'accès et le contrôle individuels et en tenant compte des questions économiques et humanitaires;
49. rappelle sa position du 12 septembre 2018 sur les systèmes d'armes autonomes selon laquelle les frappes ne doivent pas être effectuées sans véritable contrôle humain; invite le HR/VP, les États membres et le Conseil européen à adopter une position commune sur les systèmes d'armes autonomes garantissant un véritable contrôle humain des fonctions critiques des systèmes d'armes, y compris pendant le déploiement; réaffirme son soutien aux travaux menés sur les SALA par le groupe d'experts gouvernementaux des Nations unies des hautes parties contractantes à la convention sur l'emploi de certaines armes conventionnelles, qui reste le forum international pertinent pour les discussions et les négociations sur les défis juridiques posés par les systèmes d'armes autonomes; demande l'intensification de l'ensemble des efforts multilatéraux actuels afin que les cadres juridiques et réglementaires ne soient pas dépassés par les évolutions technologiques et les nouvelles méthodes de combat; invite le HR/VP, dans le cadre des discussions en cours sur la réglementation internationale des SALA par les États parties à la CCAC, à maintenir son engagement et à contribuer sans délai à faire progresser les travaux d'élaboration d'un nouveau cadre normatif mondial ainsi que d'un instrument juridiquement contraignant axé sur les définitions, les concepts et les caractéristiques des technologies émergentes relevant des SALA, les questions éthiques et juridiques du contrôle humain, notamment en ce qui concerne les fonctions critiques telles que la sélection et l'engagement d'un objectif, le maintien de la responsabilité humaine et de l'obligation de rendre des comptes et le degré d'interaction nécessaire entre l'humain et la machine, y compris la notion de contrôle et de jugement humains; demande que ces efforts assurent le respect du droit international humanitaire et du droit international relatif aux droits de l'homme à chaque étape du cycle de vie d'une arme fondée sur l'IA, en vue de convenir de recommandations spécifiques sur la clarification, l'examen et le développement des aspects du cadre normatif et opérationnel relatifs aux technologies émergentes dans le domaine des SALA;
50. estime qu'il est primordial, pour la sécurité mondiale, de disposer d'un mécanisme efficace pour faire appliquer les règles relatives à la non-prolifération des SALA et de toute technologie offensive nouvelle fondée sur l'IA;

Autorité de l'État: exemples du domaine civil, dont la santé et la justice

51. insiste sur le fait que les États membres doivent agir avec efficacité pour réduire leur dépendance à l'égard des données étrangères et veiller, sans fausser sensiblement le marché, à ce que la détention, par de puissants groupes privés, des technologies les plus élaborées en matière d'IA n'aboutisse pas à contester l'autorité de la puissance publique et encore moins à lui substituer des entités privées, en particulier lorsque le propriétaire de ces groupes privés est un pays tiers;

52. souligne que le recours à des systèmes d'IA dans le processus décisionnel des autorités publiques est susceptible de mener à des décisions biaisées ayant une incidence négative sur les citoyens et qu'il convient dès lors qu'il soit subordonné à des critères de contrôle stricts, notamment en matière de sécurité, de transparence, d'obligation de rendre des comptes, de non-discrimination et de responsabilité sociale et environnementale; invite instamment les États membres à évaluer les risques liés à des décisions prises par l'IA dans le cadre de l'exercice de l'autorité de l'État et à prévoir des garanties telles qu'une surveillance humaine véritable, des exigences de transparence et la possibilité de contester ces décisions;
53. invite instamment les États membres à évaluer les risques liés à l'IA avant d'automatiser les activités placées sous l'autorité de l'État, telles que l'administration de la justice; invite les États membres à envisager la mise en place de garanties, telles que la surveillance par un professionnel qualifié et des règles strictes de déontologie;
54. souligne qu'il importe de prendre des mesures au niveau européen pour contribuer à promouvoir les investissements indispensables, les infrastructures de données et la recherche, et notamment la recherche portant sur l'utilisation de l'intelligence artificielle par les pouvoirs publics et sur un cadre éthique commun;
55. souligne la nécessité pour l'Union européenne d'œuvrer au renforcement de la résilience stratégique afin de ne plus jamais être prise au dépourvu en temps de crise, et souligne l'importance cruciale de cette démarche, surtout en ce qui concerne l'intelligence artificielle et ses applications militaires; souligne que les chaînes d'approvisionnement des systèmes militaires fondés sur l'IA susceptibles de conduire à une dépendance technologique devraient être recalibrées, et que ces situations de dépendance devraient être progressivement éliminées; demande d'intensifier les investissements réalisés dans l'IA européenne dans le domaine de la défense et dans les infrastructures critiques sur lesquelles elle repose;
56. invite la Commission à évaluer les conséquences d'un moratoire sur l'utilisation des systèmes de reconnaissance faciale et, en fonction des résultats de cette évaluation, à envisager l'application d'un moratoire, d'une part, sur l'utilisation de ces systèmes par les autorités publiques dans l'espace public et dans les établissements d'éducation et de soins de santé et, d'autre part, sur l'utilisation des systèmes de reconnaissance faciale par les autorités répressives dans les espaces semi-publics tels que les aéroports, jusqu'à ce qu'il soit considéré que les normes techniques respectent pleinement les droits fondamentaux, que les résultats obtenus ne soient ni biaisés, ni discriminatoires, et que des garanties strictes soient mises en place pour prévenir les abus et veiller à ce que l'utilisation de ces technologies respecte les principes de nécessité et de proportionnalité;
57. souligne l'importance que revêt la cybersécurité pour l'IA, dans les scénarios tant offensifs que défensifs; relève à cet égard l'importance de la coopération internationale, ainsi que de la publication et du partage des failles de sécurité informatique et des mesures correctives; demande qu'une coopération internationale en matière de cybersécurité soit mise en place pour que l'IA puisse être utilisée et déployée efficacement et que des garanties contre les utilisations abusives de l'IA et les cyberattaques soient prévues; relève en outre le double usage (à des fins civiles et militaires) qui est inhérent aux systèmes informatiques et à l'IA, et demande qu'une réglementation efficace soit adoptée en la matière;

58. estime que les États membres devraient promouvoir des technologies de l'IA susceptibles de rendre service aux personnes et que les personnes ayant fait l'objet d'une décision prise par une autorité publique sur la base d'informations d'un système d'IA devraient en être avisées, recevoir rapidement les informations mentionnées au paragraphe précédent et avoir la possibilité de contester cette décision et de choisir que cette contestation soit résolue sans l'intervention d'un système d'IA; invite les États membres à envisager la mise en place de garanties, prévues dans la directive (UE) 2018/958¹, telles que la surveillance par un professionnel qualifié et l'élaboration de règles de déontologie;
59. souligne que le fait d'établir des prévisions à partir du partage de données, de l'utilisation de données et de l'accès à celles-ci doit être régi conformément aux exigences en matière de qualité, d'intégrité, de transparence, de sécurité, de confidentialité et de contrôle; insiste sur le fait qu'il y a lieu, tout au long du développement, du déploiement et de l'utilisation de l'IA, de la robotique et des technologies connexes, de respecter le cadre juridique de l'Union en matière de protection des données et de la vie privée afin d'accroître la sécurité des citoyens et leur confiance dans ces technologies;
60. constate que les applications d'IA évoluent rapidement dans le domaine de la reconnaissance d'éléments caractéristiques uniques, tels que les traits du visage, les mouvements et les attitudes; met en garde contre les problèmes ayant trait aux atteintes à la vie privée, à la non-discrimination et à la protection des données à caractère personnel liés à l'utilisation des applications de reconnaissance automatisée;
61. insiste sur le fait que toute décision concernant une personne physique fondée exclusivement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques défavorables à l'égard de la personne intéressée ou l'affecte de manière conséquente, est interdite en vertu du RGPD, à moins qu'elle ne soit autorisée par le droit de l'Union ou par la législation d'un État membre et subordonnée à des mesures appropriées de sauvegarde des droits et des libertés ainsi que des intérêts légitimes de la personne concernée;
62. demande que l'intelligence artificielle, lorsqu'elle est utilisée par les autorités publiques, s'accompagne systématiquement de l'explicabilité des algorithmes, de transparence ainsi que d'une surveillance réglementaire, et que des analyses d'impact soient effectuées avant que les pouvoirs publics déploient des instruments qui sollicitent des technologies d'IA; invite la Commission et le comité européen de la protection des données à publier des lignes directrices et des recommandations et à définir des bonnes pratiques afin d'apporter des précisions sur les critères et conditions applicables aux décisions fondées sur le profilage et l'utilisation de l'IA par les autorités publiques;
63. constate que l'intelligence artificielle est appelée à jouer un rôle de plus en plus fondamental en matière de santé, notamment grâce aux algorithmes d'aide au diagnostic, à la chirurgie assistée par robot, aux prothèses intelligentes, aux traitements personnalisés reposant sur la modélisation du corps de chaque patient en trois

¹ Directive (UE) 2018/958 du Parlement européen et du Conseil du 28 juin 2018 relative à un contrôle de proportionnalité avant l'adoption d'une nouvelle réglementation de professions (JO L 173 du 9.7.2018, p. 25).

dimensions, aux robots sociaux destinés à assister les personnes âgées, aux thérapies numériques conçues pour améliorer l'autonomie de certains malades mentaux, à la médecine prédictive et aux logiciels d'anticipation des épidémies;

64. insiste toutefois pour que toutes les utilisations de l'IA en matière de santé publique respectent la protection des données personnelles des patients et évitent la dissémination incontrôlée de ces données;
65. demande que toutes les utilisations de l'IA dans le domaine de la santé publique respectent l'égalité des patients dans l'accès aux soins, préservent la relation patient-médecin et respectent en toute circonstance le serment d'Hippocrate de sorte que le médecin ait toujours la possibilité et la responsabilité de s'écarter de la solution donnée par l'IA;
66. fait observer que l'utilisation de l'IA dans la lutte contre la criminalité et la cybercriminalité pourrait offrir un large éventail de possibilités et de perspectives; affirme qu'il convient de veiller en parallèle à ce que le principe selon lequel ce qui est illégal hors ligne l'est également en ligne continue de prévaloir;
67. note que l'IA est de plus en plus souvent utilisée en matière de justice, afin de rendre des décisions à la fois plus rapides, plus rationnelles et mieux conformes au droit en vigueur; salut le fait que l'utilisation de l'IA devrait permettre d'accélérer les procédures judiciaires;
68. estime qu'il convient de déterminer s'il est approprié que les décisions relatives à l'application des lois soient en partie déléguées à l'IA, tout en conservant un contrôle humain sur la décision finale;
69. souligne que, dans le système judiciaire, l'utilisation de l'IA pourrait améliorer l'analyse et la collecte de données, ainsi que la protection des victimes, et qu'elle pourrait faire l'objet de travaux de recherche et de développement, y compris des analyses d'impact, en particulier en ce qui concerne les garanties permettant d'assurer un traitement équitable et de lutter contre les partis pris et les discriminations, tout en veillant à ce que le principe de précaution soit appliqué; rappelle cependant qu'elle ne saurait remplacer l'intervention d'un être humain pour rendre des jugements ou prendre une décision;
70. rappelle l'importance des principes de gouvernance, de transparence, d'impartialité, de responsabilité, d'équité et de rigueur intellectuelle dans l'utilisation de l'IA dans le domaine de la justice pénale;
71. invite instamment les États membres à évaluer les risques liés à l'IA avant d'automatiser les activités participant à l'exercice de la puissance publique, en particulier dans le domaine judiciaire; invite les États membres à envisager la mise en place de garanties, telles que la surveillance par un professionnel qualifié et des règles de déontologie professionnelle;
72. observe que certaines technologies d'IA permettent l'automatisation, à une échelle sans précédent, du traitement de l'information et des actions d'information, comme dans le cas de la surveillance de masse dans les domaines civil et militaire, ce qui représente une menace pour les droits fondamentaux et ouvre la voie aux ingérences illégales dans

la souveraineté des États; demande que les activités de surveillance de masse fassent l'objet d'un contrôle conformément au droit international, notamment en ce qui concerne les questions de juridiction et d'application du droit; se déclare vivement préoccupé par le fait que certaines applications de notation sociale hautement intrusives qui ont été mises au point portent gravement atteinte au respect des droits fondamentaux; demande que le recours à la notation sociale à grande échelle par les autorités publiques pour limiter les droits des citoyens soit explicitement interdit; demande que la responsabilité des acteurs privés soit renforcée en vertu du droit international compte tenu de l'hégémonie décisionnelle et du contrôle que certains acteurs privés exercent sur le développement de ces technologies; invite la Commission, le Conseil et les États membres, dans ce contexte, à se montrer particulièrement attentifs dans le cadre des négociations, de la conclusion et de la ratification d'accords internationaux relatifs aux affaires familiales transfrontalières, telles que les enlèvements internationaux d'enfants, et à veiller à ce que, dans ce contexte, les systèmes d'IA soient toujours utilisés sous surveillance humaine effective et dans le respect de la légalité, au sein de l'Union et dans les pays signataires de ces accords;

73. demande que le public reste informé de l'utilisation de l'IA dans le domaine de la justice et que cette utilisation n'entraîne pas d'augmentation des discriminations par des biais de programmation; souligne que le droit de chaque individu d'accéder à un agent public soit respecté, ainsi que le droit de l'agent public concerné de prendre personnellement la décision et de s'écarter de l'information reçue de l'IA quand il l'estime nécessaire au regard des détails de l'affaire; insiste sur le droit du justiciable de faire appel de la décision conformément au droit national et demande que le juge ne puisse en aucun cas s'affranchir de sa responsabilité finale;
74. demande par conséquent que toutes ces utilisations dans les sphères publique et administrative soient considérées comme des informations relevant du domaine public et qu'elles n'entraînent pas de discriminations dues à des biais de programmation;
75. souligne qu'il importe de faire en sorte que l'IA puisse être déployée et utilisée correctement; invite les États membres à proposer une formation appropriée à leur personnel civil et militaire afin de leur permettre de déceler avec précision les discriminations et les partis pris et de les éviter dans les ensembles de données;
76. se déclare profondément préoccupé par les techniques de trucages vidéo ultra-réalistes («deepfake») permettant de créer des photos et des enregistrements audio et vidéo falsifiés de plus en plus réalistes qui peuvent être utilisés pour exercer un chantage, produire de fausses informations de presse, entamer la confiance de la population ou influencer le discours public; estime que ces pratiques sont susceptibles de déstabiliser des États en diffusant de fausses informations et en influençant les élections; demande dès lors que les créateurs soient tenus de signaler, à propos des trucages vidéo ultra-réalistes ou de tout autre montage vidéo réaliste, qu'il ne s'agit pas de la vidéo originale, que le recours à cette technique, lorsqu'elle poursuit des visées électorales, soit strictement encadré, et que cette obligation soit rigoureusement appliquée; demande que des travaux de recherche appropriés soient menés dans ce domaine afin de s'assurer que les technologies destinées à enrayer ces phénomènes ne se laissent pas distancer par l'utilisation malveillante de l'IA;

Transports

77. prend acte du potentiel économique important des applications d'IA, notamment pour l'optimisation des performances à long terme, la maintenance, la prévision des pannes et la planification de la construction des infrastructures de transport et des bâtiments ainsi que pour la sécurité, l'efficacité énergétique et les coûts; invite par conséquent la Commission à continuer de promouvoir la recherche sur l'IA et l'échange de bonnes pratiques dans le domaine des transports;
78. souligne la nécessité de renforcer l'intelligence artificielle pour favoriser la multimodalité, l'interopérabilité et l'efficacité énergétique de tous les modes de transport afin de renforcer l'efficacité de l'organisation et de la gestion des flux de transport de marchandises et de passagers, de mieux utiliser les infrastructures et les ressources le long du réseau transeuropéen de transport (RTE-T) et de lever les obstacles à la création d'un véritable espace européen unique des transports;
79. rappelle les avantages du système européen de gestion du trafic ferroviaire (ERTMS), un système intégré de protection automatique des trains, et soutient le renforcement et la normalisation internationale de l'automatisation des opérations ferroviaires;
80. salue les travaux effectués dans le cadre du projet de recherche sur la gestion du trafic aérien dans le ciel unique européen (SESAR) dans le domaine des systèmes d'aéronefs sans équipage et des systèmes de gestion du trafic aérien, tant civils que militaires;
81. rappelle le fort potentiel des véhicules autonomes pour améliorer la mobilité, la sécurité et l'environnement et invite la Commission et les États membres à assurer la coopération entre les régulateurs et toutes les parties prenantes concernées par le déploiement de véhicules routiers automatisés dans l'Union;
82. souligne que le secteur du transport maritime mondial a considérablement évolué grâce à l'intégration de l'IA ces dernières années; rappelle les discussions approfondies en cours au sein de l'Organisation maritime internationale sur la bonne intégration des technologies nouvelles et émergentes, telles que les navires autonomes, dans son cadre réglementaire;
83. souligne que les systèmes de transport intelligents peuvent atténuer la congestion du trafic, renforcer la sécurité et l'accessibilité et améliorer la gestion des flux de trafic, l'efficacité et les solutions en matière de mobilité; attire l'attention sur l'exposition accrue des réseaux traditionnels de transport aux cybermenaces; rappelle l'importance de ressources suffisantes et de recherches plus poussées sur les risques en matière de sécurité pour garantir la sécurité des systèmes automatisés et de leurs données; se félicite de l'intention de la Commission d'inscrire la cybersécurité à l'ordre du jour des débats au sein des organisations internationales compétentes en matière de transport;
84. se félicite des efforts visant à mettre en place des systèmes d'IA dans le secteur public et soutiendra la poursuite des discussions sur le déploiement de l'IA dans les transports; demande à la Commission de procéder à une évaluation de l'utilisation de l'IA et des technologies connexes du secteur des transports et d'établir une liste non exhaustive de secteurs à haut risque au regard des systèmes d'IA qui se substituent aux décisions prises dans le cadre des prérogatives des pouvoirs publics dans ce domaine;
85. souligne que le Fonds européen de la défense et la coopération structurée permanente devraient encourager la coopération entre les États membres et les industries de la

défense du continent afin de développer de nouvelles capacités de défense européennes dans le domaine de l'IA et de garantir la sécurité de l'approvisionnement, en tenant compte des considérations éthiques; insiste sur la nécessité d'éviter la fragmentation en établissant des liens entre les différents acteurs et domaines d'application, en favorisant la compatibilité et l'interopérabilité à tous les niveaux et en se concentrant sur l'élaboration commune de solutions pour l'architecture et les plateformes; rappelle, en outre, que le prochain mécanisme pour l'interconnexion en Europe, qui encourage également les infrastructures intelligentes, prévoira un fonds pour l'adaptation et le développement d'infrastructures de transport civil ou militaire à double usage dans le RTE-T pour renforcer les synergies entre les besoins civils et de défense et améliorer la mobilité militaire au sein de l'Union; souligne dès lors la nécessité d'accroître les investissements, la recherche et le leadership européens dans les technologies ayant à la fois une forte incidence sur la croissance économique et un potentiel important de double usage;

86. souligne que de nombreux investissements dans les nouvelles technologies dans le domaine des transports et de la mobilité sont déterminés par le marché, mais que les technologies et les produits commerciaux à double usage sont souvent utilisés de manière innovante à des fins militaires; souligne dès lors que le potentiel de double usage des solutions utilisant l'IA doit être pris en compte dans l'élaboration de normes d'utilisation de l'IA dans plusieurs domaines des secteurs commerciaux et militaires; demande que des normes et des principes éthiques rigoureux soient pris en compte dans l'élaboration des technologies, des produits et des principes de fonctionnement dans le domaine de la défense;
87. souligne que le transport efficace de marchandises, de munitions, d'armements et de troupes est une composante essentielle du succès des opérations militaires; met en avant le rôle crucial que l'IA sera appelée à jouer et les perspectives multiples qu'elle pourrait ouvrir dans la logistique et les transports militaires; signale que plusieurs pays du monde, y compris des États membres de l'Union européenne, intègrent des armes d'intelligence artificielle et d'autres systèmes à des plateformes terrestres, navales ou aéroportées; rappelle que l'utilisation de l'IA dans le secteur des transports pourrait apporter de nouvelles capacités et permettre des tactiques nouvelles, comme la combinaison de nombreux systèmes tels que des drones, des embarcations ou des chars sans équipage, dans le cadre d'une opération indépendante et coordonnée;

Droit international privé

88. note que, un nombre croissant de litiges relevant du droit international privé étant engendré par l'internationalisation des activités humaines, en ligne ou dans le monde réel, l'IA peut aider à les résoudre en créant des modèles permettant de repérer la juridiction compétente et le droit applicable pour chaque affaire, mais aussi d'identifier les conflits de lois les plus délicats et de proposer des solutions pour les régler;
89. estime toutefois que les utilisations de l'IA en droit international privé doivent faire l'objet d'une information appropriée du public et éviter les discriminations par des biais de programmation, qui aboutiraient à favoriser systématiquement un droit national plutôt qu'un autre, et qu'elles doivent également respecter le droit conféré au juge par la loi, le droit de faire appel selon le droit applicable et le droit de tout juge de rejeter la solution suggérée par l'AI;

90. souligne que la circulation de véhicules autonomes dans l'Union européenne, susceptible de donner naissance à un nombre particulièrement élevé de litiges de droit international privé, doit faire l'objet d'une réglementation européenne particulière précisant le régime juridique applicable en cas de dommages transfrontaliers;
91. relève qu'au regard de l'importance croissante de la recherche et du développement dans le secteur privé et des investissements considérables de pays tiers, l'Europe est confrontée à une forte concurrence; soutient, par conséquent, les efforts déployés par l'Union pour continuer à développer ses avantages concurrentiels et estime que, dans un monde hyperconnecté, l'Union devrait s'efforcer de définir des normes pour l'IA en adoptant une stratégie efficace à l'égard de ses partenaires extérieurs et en renforçant son action pour fixer des normes éthiques pour l'IA à l'échelle mondiale dans le respect des règles de sécurité et des exigences de protection des consommateurs et conformément aux valeurs de l'Union et aux droits des citoyens, dont les droits fondamentaux; estime que cela est également essentiel pour la compétitivité et le caractère durable des entreprises européennes; invite la Commission et les États membres à renforcer leur coopération et le dialogue avec les pays tiers et les organisations internationales telles que les Nations unies, l'OCDE, le G7 et le G20 afin de relever les défis découlant de l'évolution rapide de cette technologie; estime que ces efforts doivent notamment viser à établir des normes communes et à améliorer l'interopérabilité des systèmes reposant sur l'IA; invite la Commission à favoriser le dialogue, une coopération plus étroite et des synergies entre les États membres, les chercheurs, les universitaires, les acteurs de la société civile, le secteur privé, en particulier les entreprises de premier plan, et les forces militaires, pour garantir le caractère inclusif des processus d'élaboration des règles relatives à l'IA appliquée à la défense;

Principes directeurs

92. estime que les technologies et les systèmes de réseaux d'IA devraient viser à assurer la sécurité juridique des citoyens; souligne par conséquent que les règles relatives aux conflits de lois et aux conflits de compétences devraient continuer à s'appliquer compte tenu de l'intérêt des citoyens ainsi que de la nécessité de réduire le risque de recherche de la juridiction la plus indulgente; rappelle que l'IA ne saurait remplacer l'être humain dans le processus judiciaire lorsqu'il est question de rendre des jugements ou de prendre une quelconque décision définitive étant donné que ces décisions doivent toujours être prises par un être humain et être strictement soumises à une vérification humaine et à une procédure régulière; souligne que, lors du recours à des éléments de preuve émanant de technologies faisant appel à l'IA, les autorités judiciaires devraient avoir l'obligation de motiver leurs décisions;
93. rappelle que l'IA est un progrès scientifique qui ne doit pas entraîner de régression du droit, mais qu'elle doit au contraire toujours être encadrée par celui-ci — dans l'Union européenne par le droit émanant de ses institutions et de ses États membres — et qu'en aucun cas l'IA, la robotique et les technologies connexes ne peuvent enfreindre les droits fondamentaux, la démocratie et l'état de droit;
94. souligne que l'IA au service de la défense doit être responsable, équitable, traçable, fiable et gouvernable;

95. estime que l'intelligence artificielle, la robotique et les technologies connexes, y compris les logiciels, les données et les algorithmes utilisés ou produits par ces technologies, indépendamment du domaine dans lequel elles sont utilisées, devraient être développées de manière sûre et rigoureuse sur le plan technique;

o

o o

96. charge son Président de transmettre la présente résolution au Conseil et à la Commission.