Wednesday 20 January 2021

P9_TA(2021)0009

Artificial intelligence: questions of interpretation and application of international law

European Parliament resolution of 20 January 2021 on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (2020/2013(INI))

(2021/C 456/04)

The European Parliament,

— having regard to the preamble to the Treaty on European Union, and to Articles 2, 3, 10, 19, 20, 21, 114,167, 218, 225 and 227 thereof,

— having regard to the right to petition enshrined in Articles 20 and 227 of the Treaty on the Functioning of the European Union,

— having regard to the Charter of Fundamental Rights of the European Union,

— having regard to Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin ([1]) (Racial Equality Directive),

— having regard to Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation ([2]) (Equal Treatment in Employment Directive),

— having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ([3]) (GDPR), and to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA ([4]),

— having regard to Council Regulation (EU) 2018/1488 of 28 September 2018 establishing the European High Performance Computing Joint Undertaking ([5]),

— having regard to the proposal for a regulation of the European Parliament and of the Council of 6 June 2018 establishing the Digital Europe programme for the period 2021-2027 (COM(2018)0434),

— having regard to its resolution of 16 February 2017 setting out recommendations to the Commission on civil law rules on robotics ([6]),

— having regard to its resolution of 1 June 2017 on digitising European industry ([7]),

— having regard to its resolution of 12 September 2018 on autonomous weapon systems ([8]),

— having regard to its resolution of 11 September 2018 on language equality in the digital age ([9]),

([1]) OJ L 180, 19.7.2000, p. 22.
([2]) OJ L 303, 2.12.2000, p. 16.
([3]) OJ L 119, 4.5.2016, p. 1.
([4]) OJ L 119, 4.5.2016, p. 89.
([5]) OJ L 252, 8.10.2018, p. 1.
([6]) OJ C 252, 18.7.2018, p. 239.
([7]) OJ C 307, 30.8.2018, p. 163.
([8]) OJ C 433, 23.12.2019, p. 86.
([9]) OJ C 433, 23.12.2019, p. 42.

— having regard to its resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics ([10]),

— having regard to the communication of 11 December 2019 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Green Deal (COM(2019)0640),

— having regard to the Commission White Paper of 19 February 2020 on Artificial Intelligence — A European approach to excellence and trust (COM(2020)0065),

— having regard to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 19 February 2020 on a European Strategy for data (COM(2020)0066),

— having regard to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 19 February 2020 on Shaping Europe's digital future (COM(2020)0067),

— having regard to the report of 8 April 2019 of the High-Level Expert Group on Artificial Intelligence set up by the Commission in June 2018, entitled 'Ethics Guidelines for Trustworthy AI',

— having regard to the Council of Europe's Framework Convention for the Protection of National Minorities, Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms, and the European Charter for Regional or Minority Languages,

— having regard to the European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment adopted by the Council of Europe Working Group on quality of justice (CEPEJ-GT-QUAL) in December 2018,

— having regard to the OECD Council Recommendation on Artificial Intelligence adopted on 22 May 2019,

— having regard to Rule 54 of its Rules of Procedure,

— having regard to the opinions of the Committee on Foreign Affairs, the Committee on the Internal Market and Consumer Protection, the Committee on Transport and Tourism and the Committee on Civil Liberties, Justice and Home Affairs,

— having regard to the report of the Committee on Legal Affairs (A9-0001/2021),

Introduction

A. whereas artificial intelligence (AI), robotics and related technologies are being developed quickly, and have a direct impact on all aspects of our societies, including basic social and economic principles and values;

B. whereas AI is causing a revolution in military doctrine and equipment through a profound change in the way armies operate, owing mainly to the integration and use of new technologies and autonomous capabilities;

C. whereas the development and design of so-called 'artificial intelligence', robotics and related technologies are done by humans, and their choices determine the potential of technology to benefit society;

D. whereas a common Union framework must cover the development, deployment and use of AI, robotics and related technologies, and must ensure respect for human dignity and human rights, as enshrined in the Charter of Fundamental Rights of the European Union;

E. whereas the Union and its Member States have a particular responsibility to make sure that AI, robotics and related technologies — as they can be used cross borders — are human-centred, i.e. basically intended for use in the service of humanity and the common good, in order to contribute to the well-being and general interest of their citizens; whereas the Union should help the Member States to achieve this, in particular those which begun to reflect on the possible development of legal standards or legislative changes in this field;

([10]) OJ C 449, 23.12.2020, p. 37.

F. whereas European citizens could benefit from an appropriate, effective, transparent and coherent regulatory approach at Union level that defines sufficiently clear conditions for companies to develop applications and plan their business models, while ensuring that the Union and its Member States retain control over the regulations to be established, so that they are not forced to adopt or accept standards set by others;

G. whereas ethical guidance, such as the principles adopted by the High Level Expert Group on Artificial Intelligence, provides a good starting point but is not enough to ensure that businesses act fairly and guarantee the effective protection of individuals;

H. whereas this particular responsibility implies a need to examine questions of interpretation and application of international law related to the active participation of the EU in international negotiations, in so far as the EU is affected by the civil and military uses of this kind of AI, robotics and related technologies, and questions of state authority over such technologies lie outside the scope of criminal justice;

I. whereas it is essential to provide an appropriate and comprehensive legal framework for the ethical aspects of these technologies as well as for liability, transparency and accountability (in particular for AI, robotics and related technologies considered to be high risk); whereas this framework must reflect that the intrinsically European and universal humanist values are applicable to the entire value chain in the development, implementation and uses of IA; whereas this ethical framework must apply to the development (including research and innovation), deployment and use of IA, in full respect of Union law and the values set out in the Charter of Fundamental Rights of the European Union;

J. whereas the purpose of this examination is to determine to what extent the rules of international public and private law and EU law are geared to dealing with these technologies, and to highlight the challenges and risks which the latter pose for state authority, so that they can be properly and proportionately managed;

K. whereas the European Commission does not consider the military aspects of the use of artificial intelligence in its White Paper;

L. whereas a harmonised European approach to these problems calls for a common definition of AI, and for steps to ensure that the fundamental values of the European Union, the principles of the Charter of Fundamental Rights and international human rights legislation are upheld;

M. whereas AI is providing unprecedented opportunities to enhance performance in the transport sector by addressing the challenges of increasing travel demand, safety and environmental concerns, while making all transport modes smarter, more efficient and more convenient;

N. whereas addressing AI in defence at the EU level is indispensable for the development of EU capabilities in this sector;

Definition of artificial intelligence

1. Considers that it is necessary to adopt a common European legal framework with harmonised definitions and common ethical principles, including the use of AI for military purposes; calls on the Commission, therefore, to adopt the following definitions:

— 'AI system' means a system that is either software-based or embedded in hardware devices, and that displays behaviour simulating intelligence by, inter alia, collecting and processing data, analysing and interpreting its environment, and by taking action, with some degree of autonomy, to achieve specific goals;

— 'autonomous' means an AI system that operates by interpreting certain input, and by using a set of predetermined instructions, without being limited to such instructions, despite the system's behaviour being constrained by and targeted at fulfilling the goal it was given and other relevant design choices made by its developer;

2. Highlights that the security and defence policies of the European Union and its Member States are guided by the principles enshrined in the European Charter of Fundamental Rights and the UN Charter — the latter calling on all states to refrain from the threat or use of force in their relations with each other — as well as by international law, by the principles of human rights and respect for human dignity, and by a common understanding of the universal values of the inviolable

and inalienable rights of the human person, of freedom, of democracy, of equality and of the rule of law; highlights that all defence-related activities within the Union framework must respect these universal values while promoting peace, stability, security and progress in Europe and in the world;

International public law and military uses of artificial intelligence

3. Considers that AI used in a military and a civil context must be subject to meaningful human control, so that at all times a human has the means to correct, halt or disable it in the event of unforeseen behaviour, accidental intervention, cyber-attacks or interference by third parties with AI-based technology or where third parties acquire such technology;

4. Considers that the respect for international public law, in particular humanitarian law, which applies unequivocally to all weapons systems and their operators, is a fundamental requirement with which Member States must comply, especially when protecting the civilian population or taking precautionary measures in the event of an attack such as military aggression or cyberwarfare;

5. Highlights that AI and related technologies can also play a part in irregular or unconventional warfare; suggests that research, development, and use of AI in such cases should be subject to the same conditions as use in conventional conflicts;

6. Emphasises that the use of AI provides an opportunity to strengthen the security of the European Union and its citizens, and that it is essential for the EU to adopt an integrated approach in future international debates on this topic;

7. Calls on the AI research community to integrate this principle into all the aforementioned AI-based systems intended for military use; considers that no authority may establish any exception to those principles or certify such a system;

8. Reiterates that autonomous decision-making should not absolve humans from responsibility, and that people must always have ultimate responsibility for decision-making processes so that the human responsible for the decision can be identified;

9. Stresses that during the use of AI a military context, Member States, parties to a conflict and individuals must at all times comply with their obligations under applicable international law and take responsibility for actions resulting from the use of such systems; underlines that under all circumstances the anticipated, accidental or undesirable actions and effects of AI-based systems must be considered the responsibility of Member States, parties to a conflict and individuals;

10. Welcomes the possibilities for using artificial intelligence systems for training and exercises, whose potential should not be underestimated, especially given that the EU conducts exercises of a dual civilian and military nature;

11. Highlights that during the design, development, testing, deployment and use phases of AI-enabled systems, due account must be taken of potential risks at any time, with particular regard to accidental civilian casualties and injury, accidental loss of life, and damage to civilian infrastructure, as well as risks related to unintended engagement, manipulation, proliferation, cyber-attacks, interference by third parties with AI-based autonomous technology, or where third parties acquire such technology;

12. Recalls that according to the Advisory Opinion of the International Court of Justice of 8 July 1996, the principle of originality cannot be cited in support of any derogation regarding compliance with current norms of international humanitarian law;

13. Considers that, in addition to supporting operations, AI will also benefit service staff of the armed forces through the mass processing of their health data and expanding health monitoring, will identify risk factors related to their environment and working conditions and propose appropriate safeguards to limit health impacts on service personnel;

14. Reiterates that regulatory efforts must be supported by meaningful certification and surveillance schemes, as well as by clear auditability, explainability, accountability, and traceability mechanisms, so that the regulatory framework does not become outdated as a result of technological developments.

15. Stresses the importance, in a hyper-connected world, of European Union involvement in the creation of an international legal framework for the use of artificial intelligence: urges the EU to take the lead and assume, with the United Nations and the international community, an active role in promoting this global framework governing the use of AI for military and other purposes, ensuring that this use remains within the strict limits set by international law and international humanitarian law, in particular the Geneva Conventions of 12 August 1949; stresses that this framework must never breach. or permit breaches of, the dictates of public conscience and humanity as stated in the Martens clause, and be in line with safety rules and consumer protection requirements; urges the EU and the Member States to define robust surveillance and evaluation systems for the development of AI technologies, particularly those used for military purposes in authoritarian states;

16. Highlights that robotics will not only enable military personnel to stay at a distance, but also provide better self-protection, for example in operations in contaminated environments, fire-fighting, mine clearance on land or at sea, and defence against drone swarms;

17. Stresses the fact that the development, deployment, use and management of AI must respect the fundamental rights, values and freedoms enshrined in the EU Treaties, and calls on Member States to refrain from deploying high-risk AI systems that pose threats to fundamental rights; takes note of the publication of the Commission's White Paper on Artificial Intelligence, and encourages more in-depth research into the potential risk to fundamental rights resulting from the use of AI by state authorities and agencies, bodies and institutions of the European Union;

18. Calls on the Commission to facilitate research into and discussion on the opportunities for using AI in disaster relief, crisis prevention and peacekeeping;

19. Welcomes the creation of a UN Group of Governmental Experts (GGE) on Advancing responsible State behaviour in cyberspace in the context of international security, and calls for the EU to fully participate in its work;

20. Calls on the Vice President of the Commission / High Representative for Foreign Affairs and Security Policy (VP/HR) to pave the way for global negotiations with a view to putting in place an AI arms control regime and updating all existing treaty instruments on arms control, disarmament and non-proliferation so as to take into account AI-enabled systems used in warfare; calls for the Council Common Position defining common rules governing control of exports of military technology and equipment to fully take into account and cover AI-enabled weapons systems;

21. Reiterates that these rules must always be consistent with the principles referred to in the Rome Convention of 17 July 1998 regarding the prohibition of crimes of genocide, crimes against humanity and war crimes;

22. Points to the clear risks involved in decisions made by humans if they rely solely on the data, profiles and recommendations generated by machines; points out that the overall design of AI systems should also include guidelines on human supervision and oversight; calls for an obligation to be imposed regarding transparency and explainability of AI applications and the necessity of human intervention, as well as other measures, such as independent audits and specific stress tests to facilitate and enforce compliance; stresses that such audits should be conducted periodically by an independent authority that would supervise high-risk AI applications used by state authorities or the military;

23. Emphasises the importance of verifying how high-risk AI technologies arrive at decisions; recalls that the principles of non-discrimination and proportionality need to be respected, and that questions of causality, liability and responsibility, as well as transparency, accountability and explainability, need to be clarified to determine whether, or to what extent, the state as an actor in public international law, but also in exercising its own authority, can act with the help of AI-based systems with a certain autonomy, without breaching obligations stemming from international law, such as due process;

24. Insists on the importance of investing in human skills, including digital skills, in order to adapt to scientific progress involving AI-driven solutions, for individuals exercising regulated professions, including activities connected with the exercise of state authority, such as the administration of justice; calls on the Member States and the Commission to duly take this into account as part of the implementation of Directive 2005/36/EC ([11]);

25. Insists that AI systems must always comply with the principles of responsibility, equity, governability, precaution, accountability, attributability, predictability, traceability, reliability, trustworthiness, transparency, explainability, the ability to detect possible changes in circumstances and operational environment, the distinction between combatants and non-combatants, and proportionality; stresses that the latter principle makes the legality of a military action conditional on a balance between the objective pursued and the means used, and that the assessment of proportionality must always be made by a human being;

26. Stresses that in the use of AI-enabled systems in security and defence, the comprehensive situational understanding of the human operator, the predictability, reliability, and resilience of the AI-enabled system, as well as the human operator's ability to detect possible changes in circumstances and operational environment, and their ability to intervene in or discontinue an attack are needed to ensure that international humanitarian law principles, in particular distinction, proportionality and precaution in attack, are fully applied across the entire chain of command and control; stresses that AI-enabled systems must allow the humans in charge to exert meaningful control, to assume full responsibility over the systems, and be accountable for all of their uses; calls on the Commission to foster dialogue, closer cooperation and synergies between Member States, researchers, academics, civil society actors, the private sector, in particular leading companies, and the military, to ensure that policy-making processes for defence-related AI regulations are inclusive;

27. Stresses that Parliament has called for the drafting and urgent adoption of a common position on lethal autonomous weapon systems (LAWS), preventing the development, production and the use of LAWS capable of attack without meaningful human control, as well as the initiation of effective negotiations for their prohibition; recalls in this regard its resolution of 12 September 2018 on autonomous weapon systems; recalls that the term 'Lethal Autonomous Weapons Systems' (LAWS) refers to weapons systems without meaningful human control over the critical functions of targeting and attacking individual targets; emphasises that the decision to select a target and to take lethal action by means of weapons systems with a certain degree of autonomy must always be made by human operators exercising meaningful control, oversight and the necessary judgment in line with the principles of proportionality and necessity; stresses that AI-enabled systems can under no circumstances be allowed to replace human decision-making in this field;

28. Notes, moreover, that autonomous weapons systems, as a particular category of AI in the military domain, should be discussed and agreed internationally, specifically in the UN Convention on Certain Conventional Weapons forum; draws attention to the ongoing international debate on LAWS to regulate emerging military technologies, which has so far failed reach agreement; points out that the EU has only recently agreed to discuss the effects of AI developments and digitalisation on the defence sector; believes that the EU can play a crucial role in helping Member States to harmonise their approach to military AI, in order to lead international discussions;

29. Insists on the need for an EU-wide strategy against LAWS and a ban on so-called 'killer robots';

30. Emphasises that the AI used in a military context must meet a minimum set of requirements, namely it should be able to distinguish between combatants, non-combatants, and combatants on the battlefield, recognise when a combatant surrenders or is hors de combat, not have indiscriminate effects, not cause unnecessary human suffering, not be biased or trained on intentionally incomplete data, and comply with the principles of international humanitarian law, proportionality in the use of force and precaution before intervention;

31. Considers that the use of lethal autonomous weapon systems raises fundamental ethical and legal questions about the ability of humans to control these systems, and requires that AI-based technology should not be able to make autonomous decisions involving the legal principles of distinction, proportionality and precaution;

([11]) Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications (OJ L 255, 30.9.2005, p. 22).

32. Calls for transparent risk-reduction measures at international level for the development and use of military AI, in particular with regard to the principles of territorial integrity, non-intervention and the use of force; stresses the importance of taking into account military aspects when addressing legal and ethical issues in the European framework on AI; recalls its position on a ban on the development, production and use of LAWS; regrets that no explicit global conventions exist on the use of these weapons;

33. Acknowledges that the modern arms-race dynamics resulting from major military nation states developing LAWS are outpacing the progress on and effective universal application and enforcement of common rules and legal frameworks because information on the development and deployment of these systems is classified, and nation states have an inherent interest in creating the fastest and most effective offensive capabilities, irrespective of current or potential future legal frameworks or principles;

34. Considers that LAWS should be used only as a last resort, and are lawful only if they are subject to strict human control, with a human able to take over command at any time, as meaningful human intervention and supervision are essential in the process of making lethal decisions, and since human beings should always be responsible when deciding between life and death; believes that systems without any human control ('human off the loop') and human oversight must be banned with no exceptions and under all circumstances;

35. Calls on the VP/HR, the Member States and the European Council to develop and adopt, as a matter of urgency, a common position on autonomous weapons systems that ensures meaningful human control over the critical functions of weapons systems, including during deployment, to speak with one voice in relevant forums and act accordingly; calls, in this context, on the VP/HR, the Member States and the Council to share best practices and garner input from experts, academics and civil society, as reflected in the 12 September 2018 position on autonomous weapons systems, which states that attacks should always be carried out with significant human intervention;

36. Encourages all states to carry out an assessment of whether and how autonomous military devices have contributed to their national security, and what their national security could gain from AI-enabled weapon systems, in particular from the potential of such technologies to support and enhance human decision-making in compliance with international humanitarian law and its principles; recalls that any LAWS or weapon with a high degree of autonomy can malfunction because of badly written code or a cyber-attack perpetrated by an enemy state or a non-state actor;

37. Stresses that LAWS should be used only in clearly defined cases and in accordance with authorisation procedures laid down in detail in advance in documents to which the state concerned — whether or not it is a member of the North Atlantic Treaty Organisation — guarantees public access, or at least access for its national parliament;

38. Considers that LAWS must comply with the provisions of the Convention of 10 October 1980 on Certain Conventional Weapons, including the prohibition of weapons deemed 'excessively injurious';

39. Suggests, in order to prevent their uncontrolled spread, that LAWS should be included in the list of weapons subject to the provisions of the Arms Trade Treaty of 2 April 2013, listed under Article 2 of this Treaty;

40. Calls for the anthropomorphisation of LAWS to be prohibited in order to rule out any possibility of confusing humans with robots;

41. Welcomes the agreement between the Council and Parliament to exclude lethal autonomous weapons 'without the possibility for meaningful human control over the selection and engagement decisions when carrying out strikes' from actions funded under the European Defence Fund (EDF);recalls its position that the use, the development or the production of LAWS without meaningful human control is not eligible for funding under the EDF;

42. Calls on the Commission to support the research, development, deployment and use of AI for preserving peace and preventing conflicts;

43. Notes that the global AI ecosystem is dominated by American and Chinese digital giants, which are developing domestic capabilities and buying many promising companies; is of the firm opinion, therefore, that in order to avoid lagging behind in artificial intelligence technology, the EU needs to move towards a better balance between basic research and industrial applications, while developing comparative strategic advantages by further building its own potential and resources;

44. Stresses that, insofar as they fall under the definition of machinery set out in Directive 2006/42/EC ([12]), robots should be designed and assembled in compliance with the standards and safety measures provided for therein;

45. Recalls the EU's ambition to be a global actor for peace, and calls for the expansion of its role in global disarmament and non-proliferation efforts, and for its actions and policies to strive for the preservation of international peace and security, ensuring respect for international humanitarian and human rights law and the protection of civilians and civilian infrastructure;

46. Stresses the need to examine the potential impact of AI as a strategic factor for the EU's Common Security and Defence Policy (CSDP), especially in military and civilian missions and operations, and the development of EU capabilities;

47. Recalls that our allies within national, NATO or EU frameworks are themselves in the process of integrating AI into their military systems; believes that interoperability with our allies must be preserved by means of common standards, which are essential for the conduct of operations in coalition; recalls that, apart from that, cooperation on AI should occur within a European framework, which is the only relevant framework for truly generating powerful synergies, as proposed by the EU's AI strategy;

48. Considers that the EU needs to carefully monitor and consider the implications of advances in AI for defence and warfare, including potentially destabilising developments and deployments, and guide ethical research and design, ensuring the integrity of personal data and individual access and control, as well as taking into account economic and humanitarian issues;

49. Recalls its position of 12 September 2018 on autonomous weapons systems, which states that strikes must not be carried out without meaningful human intervention; calls on the VP/HR, the Member States and the European Council to adopt a common position on autonomous weapons systems that ensures meaningful human control over the critical functions of weapons systems, including during deployment; reaffirms its support for the work on LAWS of the UN GGE of the High Contracting Parties to the Convention on Certain Conventional Weapons, which remains the relevant international forum for discussions and negotiations on the legal challenges posed by autonomous weapons systems; calls for all current multilateral efforts to be accelerated so that normative and regulatory frameworks are not outpaced by technological developments and new methods of warfare; calls on the VP/HR, in the framework of the ongoing discussions on the international regulation of LAWS by the states parties to the CCW, to remain engaged and help to advance, without delay, the effort to develop a new global regulatory framework and a legally binding instrument focused on definitions, concepts and characteristics of emerging technologies in the area of LAWS, ethical and legal questions of human control, in particular with regard to their critical functions, such as target selection and engagement, the maintenance of human responsibility and accountability and the necessary degree of human-machine interaction, including the concept of human control and human judgment; calls for these efforts to ensure compliance with international humanitarian and human rights law during the different stages of the lifecycle of AI-enabled weapons, with a view to agreeing specific recommendations for the clarification, consideration and development of aspects of the normative framework relating to emerging technologies in the area of LAWS;

50. Believes that an effective mechanism for enforcing the rules on non-proliferation of LAWS and any future offensive AI-enabled technologies is of paramount importance for global security;

([12]) Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (OJ L 157, 9.6.2006, p. 24).

State authority: examples from civil areas, including health and justice

51. Stresses that Member States must act effectively to reduce their reliance on foreign data and, without significantly distorting the market, ensure that the possession of highly sophisticated AI technologies by powerful private groups does not result in the authority of the state being challenged or even usurped by private entities, especially if these private groups are owned by a third country outside the European Union;

52. Stresses that the use of AI systems in the decision-making process of public authorities can result in biased decisions that negatively affect citizens, and therefore should be subject to strict control criteria regarding their security, transparency, accountability, non-discrimination, social and environmental responsibility, among others; urges Member States to assess the risks related to AI-driven decisions connected with the exercise of State authority, and to provide for safeguards such as meaningful human supervision, transparency requirements and the possibility to contest such decisions;

53. Urges the Member States to assess the risks related to AI-driven technologies before automating activities connected with the exercise of state authority, such as the administration of justice; calls on the Member States to consider the need to provide for safeguards such as supervision by a qualified professional and strict rules on professional ethics;

54. Stresses the importance of taking action at European level to help promote much-needed investment, data infrastructure, research, including research into the use of artificial intelligence by public authorities and a common ethical framework;

55. Stresses that the European Union needs to strive for strategic resilience so that it never again finds itself unprepared in the event of a crisis, and underlines that this is of crucial significance, especially for artificial intelligence and its military applications; emphasises that supply chains for military AI systems which can lead to technological dependence should be reviewed, and that such dependencies should be phased out; calls for increased investment in European AI for defence and in the critical infrastructure that sustains it;

56. Invites the Commission to assess the consequences of a moratorium on the use of facial recognition systems, and, depending on the results of this assessment, to consider a moratorium on the use of these systems in public spaces by public authorities and in premises meant for education and healthcare, as well as on the use of facial recognition systems by law enforcement authorities in semi-public spaces such as airports, until the technical standards can be considered fully fundamental rights-compliant, the results derived are non-biased and non-discriminatory, and there are strict safeguards against misuse that ensure the necessity and proportionality of using such technologies;

57. Emphasises the importance of cybersecurity for AI, in both offensive and defensive scenarios; notes in this regard the importance of international cooperation and of the publication and sharing of IT security vulnerabilities and remedies; calls for international cybersecurity cooperation for effective AI use and deployment, and for safeguards against misuse of AI and cyber-attacks; notes, furthermore, the dual-use nature of IT systems (i.e. use for civil and military purposes) and of AI, and calls for its effective regulation;

58. Believes that Member States should promote AI technologies that work for people, and that persons who have been the subject of a decision taken by a public authority based on the information from an AI system should be informed thereof, should receive the information referred to in the preceding paragraph without delay, be offered the possibility of contesting that decision, and to opt for this appeal to be resolved without the intervention of an AI system; calls on the Member States to consider the need to establish safeguards, as provided for in Directive (EU) 2018/958 ([13]), such as supervision by a qualified professional and rules on professional ethics;

59. Underlines that making predictions based on sharing data, access to data, or its use, must be governed by the requirements of quality, integrity, transparency, security, privacy and control; stresses the need, throughout the development, deployment and use of AI, robotics and related technologies, to respect the EU legal framework on data protection and privacy, in order to increase citizens' security and their trust in those technologies;

([13]) Directive (EU) 2018/958 of the European Parliament and of the Council of 28 June 2018 on a proportionality test before adoption of new regulation of professions (OJ L 173, 9.7.2018, p. 25).

60. Observes the rapid development of AI applications that recognise unique characteristic elements, such as facial characteristics, movements and attitudes; warns of issues of invasion of privacy, non-discrimination and the protection of personal data related to the use of automated recognition applications;

61. Underlines that any decision about a natural person that is based solely on automated processing, including profiling, and which produces an adverse legal effect on the data subject or significantly affects that person, is prohibited under the GDPR unless authorised by Union or Member State law, subject to appropriate measures to safeguard the data subject's rights, freedoms and legitimate interests;

62. Calls for the explainability of algorithms, for transparency and regulatory oversight when artificial intelligence is used by public authorities, and for impact assessments to be conducted before tools using AI technologies are deployed by state authorities; calls on the Commission and the European Data Protection Board to issue guidelines and recommendations and develop best practices in order to further specify the criteria and conditions applicable to decisions based on profiling and the use of AI by public authorities;

63. Notes that artificial intelligence is playing an increasingly fundamental role in healthcare, in particular through algorithms to assist diagnosis, robot-assisted surgery, smart prostheses, personalised treatments based on the three-dimensional modelling of an individual patient's body, social robots to help elderly people, digital therapies designed to improve the independence of some mentally ill people, predictive medicine and epidemic response software;

64. Insists, nevertheless, that all uses of AI in the area of public health must guarantee the protection of patients' personal data and prevent the uncontrolled dissemination of those data;

65. Call for all uses of AI in public health to uphold the principle of the equal treatment of patients in terms of access to treatment, preserve the patient-doctor relationship, and be consistent with the Hippocratic Oath at all times, so that the doctor is always able to deviate from the solution suggested by AI, thereby maintaining responsibility for any decision;

66. Notes that the use of AI in fighting crime and cybercrime could bring a wide range of possibilities and opportunities; affirms, at the same time, that the principle that what is illegal offline is illegal online should continue to prevail;

67. Notes that AI is increasingly being used in the field of justice in order to take decisions which are more rational, more in keeping with the law in force, and quicker; welcomes the fact that the use of AI is expected to speed up judicial proceedings;

68. Considers that it is necessary to clarify whether it is appropriate for law enforcement decisions to be partially delegated to AI, while maintaining human control over the final decision;

69. Stresses that the use of AI in justice could improve the analysis and collection of data and the protection of victims, and that this could be explored in research and development and accompanied by impact assessments, in particular regarding safeguards for due process and against bias and discrimination, with the precautionary principle being applied; recalls, however, that this is no substitute for human involvement in sentencing or decision-making;

70. Recalls the importance of the principles of governance, transparency, impartiality, accountability, fairness and intellectual integrity in the use of AI in criminal justice;

71. Urges the Member States to assess the risks related to AI-driven technologies before automating activities connected with the exercise of state authority, especially in the area of justice; calls on them to consider the need to provide safeguards, such as supervision by a qualified professional and rules on professional ethics;

72. Notes that certain AI technologies enable the automation of information processing and action on an unprecedented scale, such as mass civil and military surveillance, which poses a threat to fundamental rights, and paves the way for unlawful intervention in state sovereignty; calls for the scrutiny of mass surveillance activities under international law, including as regards questions of jurisdiction and enforcement; expresses serious concerns about some highly intrusive social scoring applications that have been developed, as they seriously endanger the respect of fundamental rights; calls for an explicit ban on the use of mass social scoring by public authorities as a way to restrict the rights of citizens; calls for the

accountability of private actors under international law to be enhanced, given the decision-making hegemony and control of certain private actors over the development of these technologies; calls, in this context, on the Commission, the Council and the Member States to pay particular attention when negotiating, concluding and ratifying international agreements related to cross-border family cases, such as international child abductions, and to ensure that in this context AI systems are always used under effective human verification, and respect due process within the EU and countries which are signatories of these agreements;

73. Requests that the public is kept informed about the use of AI in the field of justice, and that such uses do not give rise to discrimination resulting from programming biases; stresses that the right of every individual to have access to a public official must be respected, as well as the right of the responsible official to personally take the decision and deviate from the information received from the AI when they deem it necessary in the light of the details of the matter in question; highlights the right of the defendant to appeal the decision in accordance with national legislation, without ever eliminating the final responsibility of the judiciary;

74. Calls, therefore, for all these public and administrative uses be deemed information in the public domain, and for discrimination due to programming biases to be avoided;

75. Stresses the importance of enabling the proper deployment and use of AI; calls on the Member States to provide their civil and military personnel with appropriate training in order to allow them to accurately identify and avoid discrimination and bias in datasets;

76. Is deeply concerned about deepfake technologies that allow increasingly realistic photo, audio and video forgeries to be produced that could be used to blackmail, generate fake news reports, or erode public trust and influence public discourse; believes such practices have the potential to destabilise countries, spreading disinformation and influencing elections; calls, therefore, for an obligation for all deepfake material or any other realistically made synthetic videos to be labelled as 'not original' by the creator, with strict limits on their use for electoral purposes and robust enforcement; calls for adequate research in this field to ensure that technologies to counter these phenomena keep pace with the malicious use of AI;

Transport

77. Takes note of the significant economic potential of AI applications, including for the optimisation of long-term performance, maintenance, failure prediction and construction planning in transport infrastructure and buildings, as well as for safety, energy efficiency and costs; calls on the Commission, therefore, to continue promoting AI research and the exchange of good practices in transport;

78. Stresses the need to promote artificial intelligence to foster the multimodality, interoperability and energy efficiency of all modes of transport, to enhance efficiency in the organisation and management of goods and passenger traffic flows, to make better use of infrastructure and resources along the Trans-European Transport Network (TEN-T), and to address the obstacles to the creation of a true single European transport area;

79. Recalls the benefits of the European Rail Traffic Management System (ERTMS), a seamless automatic train protection system, and supports the development and international standardisation of the automation of train operations;

80. Welcomes the work of the Single European Sky Air Traffic Management Research project (SESAR) on unmanned aircraft systems and air traffic management systems, both civil and military;

81. Recalls that autonomous vehicles have great potential to improve mobility, safety, and bring environmental benefits, and calls on the Commission and the Member States to ensure cooperation among regulators and all stakeholders relevant to the deployment of automated road vehicles in the EU;

82. Points out that the global shipping industry has greatly changed thanks to the integration of AI in recent years; recalls the current comprehensive discussions in the International Maritime Organization on effectively integrating new and emerging technologies, such as autonomous ships, in its regulatory framework;

83. Stresses that intelligent transport systems mitigate traffic congestion, increase safety and accessibility and contribute to improving the management of traffic flows, efficiency and mobility solutions; draws attention to the increased exposure of traditional transport networks to cyber threats; recalls the importance of sufficient resources and further research in security risks in ensuring the safety of automated systems and their data; welcomes the Commission's intention to include cybersecurity as a regular agenda item for discussion within transport-related international organisations;

84. Welcomes the efforts to introduce AI systems in the public sector, and will support further discussions on AI deployment in transport; calls on the Commission to carry out an evaluation of the use of AI and similar technologies in the transport sector, and to compile a non-exhaustive list of high-risk segments in AI systems replacing decisions within the framework of prerogatives of public power in this area;

85. Underlines that the European Defence Fund and Permanent Structured Cooperation should stimulate cooperation between Member States and European defence industries to develop new European defence capabilities in AI, and ensure security of supply, taking ethical considerations into account; emphasises the need to avoid fragmentation by building bridges between various actors and application domains, by promoting compatibility and interoperability at all levels, and by focusing on joint work on architecture and platform solutions; recalls, moreover, that the next Connecting Europe Facility, which also promotes smart infrastructure, will provide for a fund for the adaptation and the development of civilian or military dual-use transport infrastructure in the TEN-T in order to increase synergies between civil and defence needs, and with a view to improving civil and military mobility within the Union; emphasises, therefore, the need for further European investment, research, and leadership in technologies with both high economic growth impact as well as significant dual-use potential;

86. Stresses that many investments in new technologies in transport and mobility are market-driven, but that dual-use commercial off-the-shelf technologies and products are often used in innovative ways for military purposes; highlights, therefore, that the dual-use potential of AI-enabled solutions needs to be taken into account when drafting standards for the use of AI in various areas of the commercial and military sectors; calls for high ethical standards and policy to be included in the development of defence technologies, products and operating principles;

87. Points out that the effective transportation of goods, ammunition, armaments and troops is an essential component of successful military operations; stresses that AI is expected to play a crucial role and create numerous possibilities in military logistics and transport; points out that countries throughout the world, including EU Member States, are embedding AI weapons and other systems in land, naval, airborne platforms; recalls that AI applications in the transport sector could provide new capabilities and allow new forms of tactics, such as the combination of many systems such as drones, unmanned boats or tanks in an independent and coordinated operation;

International private law

88. Notes that, given that an increasing number of disputes under international private law are arising from the internationalisation of human activities, either online or in the real world, AI can help to resolve them by creating models to identify the competent jurisdiction and applicable law for each case, and also to identify the most sensitive conflicts of laws and propose ways of resolving them;

89. Considers, however, that the public must be properly informed about the uses of AI in international private law, that these uses must not lead to discrimination through programming, which would result in one nation's laws being systematically favoured over another's, must respect the rights of the court predetermined by law, permit appeals in accordance with the applicable law, and allow any judge to disregard the solution suggested by AI;

90. Stresses that the circulation of autonomous vehicles in the European Union, which is liable to give rise to a particularly high number of disputes under international private law, must be the subject of specific European rules stipulating the legal regime applicable in the event of cross-border damage;

91. Points out that with the increasing importance of research and development in the private sector, and massive investments from third countries, the EU is facing strong competition; supports, therefore, the EU's efforts to further develop its competitive advantages, and believes that the EU should aim to act as a norm-setter for AI in a hyper-connected world by adopting an effective strategy towards its external partners, stepping up its efforts to set global ethical norms for

AI at international level in line with safety rules and consumer protection requirements, as well as with European values and citizens' rights, including fundamental rights; considers that this is also key for the competitiveness and sustainability of European companies; calls on the Commission and Member States to strengthen cooperation with third countries and international organisations, such as the UN, OECD, G7 and G20, and to engage in a broader dialogue to address challenges arising from the development of this rapidly changing technology; considers that these efforts should seek, in particular, to establish common standards and improve the interoperability of AI-enabled systems; calls on the Commission to foster dialogue, closer cooperation and synergies between Member States, researchers, academics, civil society actors, the private sector, in particular leading companies, and the military, in order to ensure that policy-making processes for defence-related AI regulations are inclusive;

Guiding principles

92. Considers that AI technologies and network systems should aim to provide legal certainty for citizens; underlines, therefore, that rules on conflict of laws and jurisdictions should continue to apply, while taking into account citizens' interests, as well as the need to reduce the risk of forum-shopping; recalls that AI cannot replace humans in the judicial process when it comes to passing sentence or taking a final decision of any kind, as such decisions must always be taken by a human, and be strictly subject to human verification and due process; insists that when using evidence provided by AI-assisted technologies, the judicial authorities should have the obligation to provide reasons for their decisions;

93. Recalls that AI is a scientific advance which must not undermine the law, but must on the contrary always be governed by it — in the European Union by the law emanating from its institutions and its Member States — and that under no circumstances can AI, robotics and related technologies contravene fundamental rights, democracy and the rule of law;

94. Stresses that AI used for defence purposes should be responsible, equitable, traceable, reliable and governable;

95. Considers that artificial intelligence, robotics and related technologies, including the software, algorithms and data used or produced by such technologies, regardless of the field in which they are used, should be developed in a secure and technically rigorous manner;

o

o o

96. Instructs its President to forward this resolution to the Council and the Commission.