



TEXTS ADOPTED

P9_TA(2020)0275

Framework of ethical aspects of artificial intelligence, robotics and related technologies

European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL))

The European Parliament,

- having regard to Article 225 of the Treaty on the Functioning of the European Union,
- having regard to Article 114 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 Regulation (EU) 2018/1488 of 28 September 2018 establishing the European High Performance Computing Joint Undertaking¹,
- 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 origin² (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 occupation³ (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)⁴ (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

¹ OJ L 252, 8.10.2018, p. 1.

² OJ L 180, 19.7.2000, p. 22.

³ OJ L 303, 2.12.2000, p. 16.

⁴ OJ L 119, 4.5.2016, p. 1.

- movement of such data, and repealing Council Framework Decision 2008/977/JHA¹,
- having regard to the Interinstitutional Agreement of 13 April 2016 on Better Law-Making²,
 - 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 the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 11 December 2019 on The European Green Deal (COM(2019)0640),
 - 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 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 Council of the European Union’s conclusions on Shaping Europe’s Digital future of June 2020,
 - having regard to its resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics³,
 - having regard to its resolution of 1 June 2017 on digitising European industry⁴,
 - having regard to its resolution of 12 September 2018 on autonomous weapon systems⁵,
 - having regard to its resolution of 11 September 2018 on language equality in the digital age⁶,
 - having regard to its resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics⁷,
 - having regard to the report of 8 April 2019 of the High-Level Expert Group on Artificial Intelligence set up by the Commission entitled ‘Ethics Guidelines for Trustworthy AI’,

¹ OJ L 119, 4.5.2016, p. 89.

² OJ L 123, 12.5.2016, p. 1.

³ OJ C 252, 18.7.2018, p. 239.

⁴ OJ C 307, 30.8.2018, p. 163.

⁵ OJ C 433, 23.12.2019, p. 86.

⁶ Texts adopted, P8_TA(2018)0332.

⁷ Texts adopted, P8_TA(2019)0081.

- having regard to the European Added Value Assessment study carried out by the European Parliamentary Research Service, entitled 'European framework on ethical aspects of artificial intelligence, robotics and related technologies: European Added Value Assessment'¹,
- having regard to the briefings and studies prepared at the request of the Panel for the Future of Science and Technology (STOA), managed by the Scientific Foresight Unit within the European Parliamentary Research Service, entitled “What if algorithms could abide by ethical principles?”, “Artificial Intelligence *ante portas*: Legal & ethical reflections”, “A governance framework for algorithmic accountability and transparency”, “Should we fear artificial intelligence?” and “The ethics of artificial intelligence: Issues and initiatives”,
- 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 OECD Council Recommendation on Artificial Intelligence adopted on 22 May 2019,
- having regard to Rules 47 and 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, the Committee on Civil Liberties, Justice and Home Affairs, the Committee on Employment and Social Affairs, the Committee on the Environment, Public Health and Food Safety and the Committee on Culture and Education,
- having regard to the report of the Committee on Legal Affairs (A9-0186/2020),

Introduction

- A. whereas the development, deployment and use of artificial intelligence (also referred to as ‘AI’), robotics and related technologies is carried out by humans, and their choices determine the potential of such technologies to benefit society;
- B. whereas artificial intelligence, robotics and related technologies that have the potential to generate opportunities for businesses and benefits for citizens and that can directly impact all aspects of our societies, including fundamental rights and social and economic principles and values, as well as have a lasting influence on all areas of activity, are being promoted and developed quickly;
- C. whereas artificial intelligence, robotics and related technologies will lead to substantial changes to the labour market and in the workplace; whereas they can potentially replace workers performing repetitive activities, facilitate human-machine collaborative working systems, increase competitiveness and prosperity and create new job opportunities for qualified workers, while at the same time posing a serious challenge in terms of reorganisation of the workforce;
- D. whereas the development of artificial intelligence, robotics and related technologies can

¹ [https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU\(2020\)654179](https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)654179).

also contribute to reaching the sustainability goals of the European Green Deal in many different sectors; whereas digital technologies can boost the impact of policies as regards environmental protection; whereas they can also contribute to reducing traffic congestion and emissions of greenhouse gases and air pollutants;

- E. whereas, for sectors like public transport, AI-supported intelligent transport systems can be used to minimise queuing, optimise routing, enable persons with disabilities to be more independent, and increase energy efficiency thereby enhancing decarbonisation efforts and reducing the environmental footprint;
- F. whereas these technologies bring about new business opportunities which can contribute to the recovery of Union industry after the current health and economic crisis if greater use is made of them, for instance, in the transport industry; whereas such opportunities can create new jobs, as the uptake of these technologies has the potential to increase businesses' productivity levels and contribute to efficiency gains; whereas innovation programmes in this area can enable regional clusters to thrive;
- G. whereas the Union and its Member States have a particular responsibility to harness, promote and enhance the added value of artificial intelligence and make sure that AI technologies are safe and contribute to the well-being and general interest of their citizens as they can make a huge contribution to reaching the common goal of improving the lives of citizens and fostering prosperity within the Union, by contributing to the development of better strategies and innovation in a number of areas and sectors; whereas, in order to exploit the full potential of artificial intelligence and make users aware of the benefits and challenges that AI technologies bring, it is necessary to include AI or digital literacy in education and training, including in terms of promoting digital inclusion, and to conduct information campaigns at Union level that give an accurate representation of all aspects of AI development;
- H. whereas a common Union regulatory framework for the development, deployment and use of artificial intelligence, robotics and related technologies ('regulatory framework for AI') should allow citizens to share the benefits drawn from their potential, while protecting citizens from the potential risks of such technologies and promoting the trustworthiness of such technologies in the Union and elsewhere; whereas that framework should be based on Union law and values and guided by the principles of transparency, explainability, fairness, accountability and responsibility;
- I. whereas such a regulatory framework is of key importance in avoiding the fragmentation of the Internal Market resulting from differing national legislation and will help foster much needed investment, develop data infrastructure and support research; whereas it should consist of common legal obligations and ethical principles as laid down in the proposal for a Regulation requested in the annex to this resolution; whereas it should be established according to the better regulation guidelines;
- J. whereas the Union has a strict legal framework in place to ensure, inter alia, the protection of personal data and privacy and non-discrimination, to promote gender equality, environmental protection and consumers' rights; whereas such a legal framework consisting of an extensive body of horizontal and sectorial legislation, including the existing rules on product safety and liability, will continue to apply in relation to artificial intelligence, robotics and related technologies, although certain adjustments of specific legal instruments may be necessary to reflect the digital transformation and address new challenges posed by the use of artificial intelligence;

- K. whereas there are concerns that the current Union legal framework, including the consumer law and employment and social acquis, data protection legislation, product safety and market surveillance legislation, as well as antidiscrimination legislation, may no longer be fit for purpose to effectively tackle the risks created by artificial intelligence, robotics and related technologies;
- L. whereas in addition to adjustments to existing legislation, legal and ethical questions relating to AI technologies should be addressed through an effective, comprehensive and future-proof regulatory framework of Union law reflecting the Union's principles and values as enshrined in the Treaties and the Charter of Fundamental Rights of the European Union ('Charter') that should refrain from over-regulation, by only closing existing legal loopholes, and increase legal certainty for businesses and citizens alike, namely by including mandatory measures to prevent practices that would undoubtedly undermine fundamental rights;
- M. whereas any new regulatory framework needs to take into consideration all the interests at stake; whereas careful examination of the consequences of any new regulatory framework on all actors in an impact assessment should be a prerequisite for further legislative steps; whereas the crucial role of small and medium-sized enterprises (SMEs) and start-ups especially in the Union economy justifies a strictly proportionate approach to enable them to develop and innovate;
- N. whereas artificial intelligence, robotics and related technologies can have serious implications for the material and immaterial integrity of individuals, groups, and society as a whole, and potential individual and collective harm must be addressed with legislative responses;
- O. whereas, in order to respect a Union regulatory framework for AI, specific rules for the Union's transport sector may need to be adopted;
- P. whereas AI technologies are of strategic importance for the transport sector, including due to them raising the safety and accessibility of all modes of transport, and creating new employment opportunities and more sustainable business models; whereas a Union approach to the development of artificial intelligence, robotics and related technologies in transport has the potential to increase the global competitiveness and strategic autonomy of the Union economy;
- Q. whereas human error is still involved in about 95% of all road traffic accidents in the Union; whereas the Union aimed to reduce annual road fatalities in the Union by 50% by 2020 compared to 2010, but, in view of stagnating progress, renewed its efforts in its EU Road Safety Policy Framework 2021-2030 - Next steps towards "Vision Zero"; whereas in this regard, AI, automation and other new technologies have great potential and vital importance for increasing road safety by reducing the possibilities for human error;
- R. whereas the Union's regulatory framework for AI should also reflect the need to ensure that workers' rights are respected; whereas regard should be had to the European Social Partners Framework Agreement on Digitalisation of June 2020;
- S. whereas the scope of the Union's regulatory framework for AI should be adequate, proportionate and thoroughly assessed; whereas it should cover a wide range of technologies and their components, including algorithms, software and data used or

produced by them, a targeted risk-based approach is necessary to avoid hampering future innovation and the creation of unnecessary burdens, especially for SMEs; whereas the diversity of applications driven by artificial intelligence, robotics and related technologies complicates finding a single solution suitable for the entire spectrum of risks;

- T. whereas data analysis and AI increasingly impact on the information made accessible to citizens; whereas such technologies, if misused, may endanger fundamental rights to freedom of expression and information as well as media freedom and pluralism;
- U. whereas the geographical scope of the Union's regulatory framework for AI should cover all the components of artificial intelligence, robotics and related technologies developed, deployed or used in the Union, including in cases where part of the technologies might be located outside the Union or not have a specific location;
- V. whereas the Union's regulatory framework for AI should encompass all relevant stages, namely the development, the deployment and the use of the relevant technologies and their components, requiring due consideration of the relevant legal obligations and ethical principles and should set the conditions to make sure that developers, deployers and users are fully compliant with such obligations and principles;
- W. whereas a harmonised approach to ethical principles relating to artificial intelligence, robotics and related technologies requires a common understanding in the Union of the concepts that form the basis of the technologies such as algorithms, software, data or biometric recognition;
- X. whereas action at Union level is justified by the need to avoid regulatory fragmentation or a series of national regulatory provisions with no common denominator, and to ensure a homogenous application of common ethical principles enshrined in law when developing, deploying and using high-risk artificial intelligence, robotics and related technologies; whereas clear rules are needed where the risks are significant;
- Y. whereas common ethical principles are only efficient where they are also enshrined in law, and those responsible for ensuring, assessing and monitoring compliance are identified;
- Z. whereas ethical guidance, such as the principles adopted by the High-Level Expert Group on Artificial Intelligence, provides a good starting point but cannot ensure that developers, deployers and users act fairly and guarantee the effective protection of individuals; whereas such guidance is all the more relevant with regard to high-risk artificial intelligence, robotics and related technologies;
- AA. whereas each Member State should designate a national supervisory authority responsible for ensuring, assessing and monitoring the compliance of the development, deployment and use of high-risk artificial intelligence, robotics and related technologies with the Union's regulatory framework for AI, and for allowing discussions and exchanges of views in close cooperation with relevant stakeholders and civil society; whereas national supervisory authorities should cooperate with each other;
- AB. whereas in order to ensure a harmonised approach across the Union and the optimal functioning of the Digital Single Market, coordination at Union level by the Commission, and/or any relevant institutions, bodies, offices and agencies of the Union

that may be designated in this context, should be assessed as regards the new opportunities and challenges, in particular those of a cross-border nature, arising from ongoing technological developments; whereas, to this end, the Commission should be tasked with finding an appropriate solution to structure such coordination at Union level;

Human-centric and human-made artificial intelligence

1. Takes the view that, without prejudice to sector-specific legislation, an effective and harmonised regulatory framework based on Union law, the Charter and international human rights law, and applicable, in particular, to high-risk technologies, is necessary in order to establish equal standards throughout the Union and effectively protect Union values;
2. Believes that any new regulatory framework for AI consisting of legal obligations and ethical principles for the development, deployment and use of artificial intelligence, robotics and related technologies should fully respect the Charter and thereby respect human dignity, autonomy and self-determination of the individual, prevent harm, promote fairness, inclusion and transparency, eliminate biases and discrimination, including as regards minority groups, and respect and comply with the principles of limiting the negative externalities of technology used, of ensuring explainability of technologies, and of guaranteeing that the technologies are there to serve people and not replace or decide for them, with the ultimate aim of increasing every human being's well-being;
3. Emphasises the asymmetry between those who employ AI technologies and those who interact and are subject to them; in this context, stresses that citizens' trust in AI can only be built on an ethics-by-default and ethics-by-design regulatory framework which ensures that any AI put into operation fully respects and complies with the Treaties, the Charter and secondary Union law; considers that building on such an approach should be in line with the precautionary principle that guides Union legislation and should be at the heart of any regulatory framework for AI; calls, in this regard, for a clear and coherent governance model that allows companies and innovators to further develop artificial intelligence, robotics and related technologies;
4. Believes that any legislative action related to artificial intelligence, robotics and related technologies should be in line with the principles of necessity and proportionality;
5. Considers that such an approach will allow companies to introduce innovative products onto the market and create new opportunities, while ensuring the protection of Union values by leading to the development of AI systems which incorporate Union ethical principles by design; considers that such a values-based regulatory framework would represent added value by providing the Union with a unique competitive advantage and make a significant contribution to the well-being and prosperity of Union citizens and businesses by boosting the internal market; underlines that such a regulatory framework for AI will also represent added value as regards promoting innovation in the internal market; believes that for example, in the transport sector, this approach presents Union businesses with the opportunity to become global leaders in this area;
6. Notes that the Union's legal framework should apply to artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced by such technologies;

7. Notes that the opportunities based on artificial intelligence, robotics and related technologies rely on 'Big Data', with a need for a critical mass of data to train algorithms and refine results; welcomes in this regard the Commission's proposal for the creation of a common data space in the Union to strengthen data exchange and support research in full respect of European data protection rules;
8. Considers that the current Union legal framework, in particular on protection and privacy and personal data, will need to fully apply to AI, robotics, and related technologies and needs to be reviewed and scrutinised on a regular basis and updated where necessary, in order to effectively tackle the risks created by these technologies, and, in this regard, could benefit from being supplemented with robust guiding ethical principles; points out that, where it would be premature to adopt legal acts, a soft law framework should be used;
9. Expects the Commission to integrate a strong ethical approach into the legislative proposal requested in the annex to this resolution as a follow up to the White Paper on Artificial Intelligence, including on safety, liability and fundamental rights, which maximises the opportunities and minimises the risks of AI technologies; expects that the legislative proposal requested will include policy solutions to the major recognised risks of artificial intelligence including, amongst others, on the ethical collection and use of Big Data, the issue of algorithmic transparency and algorithmic bias; calls on the Commission to develop criteria and indicators to label AI technology, in order to stimulate transparency, explainability and accountability and incentivise the taking of additional precautions by developers; stresses the need to invest in integrating non-technical disciplines in AI study and research, taking into account the social context;
10. Considers that artificial intelligence, robotics and related technologies must be tailored to human needs in line with the principle whereby their development, deployment and use should always be at the service of human beings and never the other way round, and should seek to enhance well-being and individual freedom, as well as preserve peace, prevent conflicts and strengthen international security, while at the same time maximising the benefits offered and preventing and reducing its risks;
11. Declares that the development, deployment and use of high-risk artificial intelligence, robotics and related technologies, including but not exclusively by human beings, should always be ethically guided, and designed to respect and allow for human agency and democratic oversight, as well as allow the retrieval of human control when needed by implementing appropriate control measures;

Risk assessment

12. Stresses that any future regulation should follow a differentiated and future oriented risk-based approach to regulating artificial intelligence, robotics and related technologies, including technology-neutral standards across all sectors, with sector-specific standards where appropriate; notes that, in order to ensure uniform implementation of the system of risk assessment and that there is compliance with related legal obligations to ensure a level-playing field among the Member States and to prevent fragmentation of the internal market, an exhaustive and cumulative list of high-risk sectors and high-risk uses or purposes is needed; stresses that such a list must be the subject of regular re-evaluation and notes that, given the evolving nature of these technologies, the way in which their risk assessment is carried out may need to be reassessed in the future;

13. Considers that the determination of whether artificial intelligence, robotics and related technologies should be considered high-risk, and thus subject to mandatory compliance with legal obligations and ethical principles as laid down in the regulatory framework for AI, should always follow from an impartial, regulated and external ex-ante assessment based on concrete and defined criteria;
14. Considers, in that regard, that artificial intelligence, robotics and related technologies should be considered high-risk when their development, deployment and use entail a significant risk of causing injury or harm to individuals or society, in breach of fundamental rights and safety rules as laid down in Union law; considers that, for the purposes of assessing whether AI technologies entail such a risk, the sector where they are developed, deployed or used, their specific use or purpose and the severity of the injury or harm that can be expected to occur should be taken into account; the first and second criteria, namely the sector and the specific use or purpose, should be considered cumulatively;
15. Underlines that the risk assessment of these technologies should be done on the basis of an exhaustive and cumulative list of high-risk sectors and high-risk uses and purposes; strongly believes that there should be coherence within the Union when it comes to the risk assessment of these technologies, especially when they are assessed both in light of their compliance with the regulatory framework for AI and in accordance with any other applicable sector-specific legislation;
16. Considers that this risk-based approach should be developed in a way that limits the administrative burden for companies, and SMEs in particular, as much as possible by using existing tools; such tools include but are not limited to the Data Protection Impact Assessment list as provided for in Regulation (EU) 2016/679;

Safety features, transparency and accountability

17. Recalls that the right to information of consumers is anchored as a key principle under Union law and underlines that it therefore should be fully implemented in relation to artificial intelligence, robotics and related technologies; opines it should especially encompass transparency regarding interaction with artificial intelligence systems, including automation processes, and regarding their mode of functioning, capabilities, for example how information is filtered and presented, accuracy and limitations; considers that such information should be provided to the national supervisory authorities and national consumer protection authorities;
18. Underlines that consumers' trust is essential for the development and implementation of these technologies, which can carry inherent risks when they are based on opaque algorithms and biased data sets; believes that consumers should have the right to be adequately informed in an understandable, timely, standardised, accurate and accessible manner about the existence, reasoning, possible outcome and impacts for consumers of algorithmic systems, about how to reach a human with decision-making powers, and about how the system's decisions can be checked, meaningfully contested and corrected; underlines, in this regard, the need to consider and respect the principles of information and disclosure on which the consumer law *acquis* has been built; considers it necessary to provide detailed information to end-users regarding the operation of transport systems and AI-supported vehicles;
19. Notes that it is essential that the algorithms and data sets used or produced by artificial

intelligence, robotics, and related technologies are explainable and, where strictly necessary and in full respect of Union legislation on data protection, privacy and intellectual property rights and trade secrets, accessible by public authorities such as national supervisory authorities and market surveillance authorities; further notes that, in accordance with the highest possible and applicable industry standards, documentation should be stored by those who are involved in the different stages of the development of high-risk technologies; notes the possibility that market surveillance authorities may have additional prerogatives in that respect; stresses in this respect the role of lawful reverse-engineering; considers that an examination of the current market surveillance legislation might be necessary to ensure that it responds ethically to the emergence of artificial intelligence, robotics and related technologies;

20. Calls for a requirement for developers and deployers of high-risk technologies to, where a risk assessment so indicates, provide public authorities with the relevant documentation on the use and design and safety instructions, including, when strictly necessary and in full respect of Union legislation on data protection, privacy, intellectual property rights and trade secrets, source code, development tools and data used by the system; notes that such an obligation would allow for the assessment of their compliance with Union law and ethical principles and notes, in that respect, the example provided by the legal deposit of publications of a national library; notes the important distinction between transparency of algorithms and transparency of the use of algorithms;
21. Further notes that, in order to respect human dignity, autonomy and safety, due consideration should be given to vital and advanced medical appliances and the need for independent trusted authorities to retain the means necessary to provide services to persons carrying these appliances, where the original developer or deployer no longer provides them; for example; such services would include maintenance, repairs and enhancements, including software updates that fix malfunctions and vulnerabilities;
22. Maintains that high-risk 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 developed, deployed and used, should be developed by design in a secure, traceable, technically robust, reliable, ethical and legally binding manner and be subject to independent control and oversight; considers especially that all players throughout the development and supply chains of artificial intelligence products and services should be legally accountable and highlights the need for mechanisms to ensure liability and accountability;
23. Underlines that regulation and guidelines concerning explainability, auditability, traceability and transparency, as well as, where so required by a risk assessment and strictly necessary and while fully respecting Union law such as that concerning data protection, privacy, intellectual property rights and trade secrets, access by public authorities to technology, data and computing systems underlying such technologies, are essential to ensuring citizens' trust in those technologies, even if the degree of explainability is relative to the complexity of the technologies; points out that it is not always possible to explain why a model has led to a particular result or decision, black box algorithms being a case in point; considers, therefore, that the respect of these principles is a precondition to guarantee accountability;
24. Considers that citizens, including consumers, should be informed when interacting with a system using artificial intelligence in particular to personalise a product or service for

its users, whether and how they can switch off or limit such personalisation;

25. Points out in this regard that, if they are to be trustworthy, artificial intelligence, robotics and their related technologies must be technically robust and accurate;
26. Stresses that the protection of networks of interconnected AI and robotics is important and strong measures must be taken to prevent security breaches, data leaks, data poisoning, cyber-attacks and the misuse of personal data, and that this will require the relevant agencies, bodies and institutions both at Union and national level to work together and in cooperation with end users of these technologies; calls on the Commission and Member States to ensure that Union values and respect for fundamental rights are observed at all times when developing and deploying AI technology in order to ensure the security and resilience of the Union's digital infrastructure;

Non-bias and non-discrimination

27. Recalls that artificial intelligence, depending on how it is developed and used, has the potential to create and reinforce biases, including through inherent biases in the underlying datasets, and therefore, create various forms of automated discrimination, including indirect discrimination, concerning in particular groups of people with similar characteristics; calls on the Commission and the Member States to take any possible measure to avoid such biases and to ensure the full protection of fundamental rights;
28. Is concerned by the risks of biases and discrimination in the development, deployment and use of high-risk artificial intelligence, robotics and related technologies, including the software, algorithms and data used or produced by such technologies; recalls that, in all circumstances, they should respect Union law, as well as human rights and dignity, and autonomy and self-determination of the individual, and ensure equal treatment and non-discrimination for all;
29. Stresses that AI technologies should be designed to respect, serve and protect Union values and physical and mental integrity, uphold the Union's cultural and linguistic diversity and help satisfy essential needs; underlines the need to avoid any use that might lead to inadmissible direct or indirect coercion, threaten to undermine psychological autonomy and mental health or lead to unjustified surveillance, deception or inadmissible manipulation;
30. Firmly believes that the fundamental human rights enshrined in the Charter should be strictly respected so as to ensure that these emerging technologies do not create gaps in terms of protection;
31. Affirms that possible bias in and discrimination by software, algorithms and data can cause manifest harm to individuals and to society, therefore they should be addressed by encouraging the development and sharing of strategies to counter these, such as de-biasing datasets in research and development, and by the development of rules on data processing; considers this approach to have the potential to turn software, algorithms and data into an asset in fighting bias and discrimination in certain situations, and a force for equal rights and positive social change;
32. Maintains that ethical values of fairness, accuracy, confidentiality and transparency should be the basis of these technologies, which in this context entails that their operations should

be such that they do not generate biased outputs;

33. Underlines the importance of the quality of data sets used for artificial intelligence, robotics and related technologies depending on their context, especially regarding the representativeness of the training data, on the de-biasing of data sets, on the algorithms used, and on data and aggregation standards; stresses that those data sets should be auditable by national supervisory authorities whenever called upon to ensure their conformity with the previously referenced principles;
34. Highlights that, in the context of the widespread disinformation war, particularly driven by non-European actors, AI technologies might have ethically adverse effects by exploiting biases in data and algorithms or by deliberately altering training data by a third country, and could be also exposed to other forms of dangerous malign manipulation in unpredictable ways and with incalculable consequences; there is therefore an increased need for the Union to continue investment in research, analysis, innovation and cross-border and cross-sector knowledge transfer in order to develop AI technologies that would be clearly free of any sort of profiling, bias and discrimination, and could effectively contribute to combating fake news and disinformation, while at the same time respecting data privacy and the Union's legal framework;
35. Recalls the importance of ensuring effective remedies for individuals and calls on the Member States to ensure that accessible, affordable, independent and effective procedures and review mechanisms are available to guarantee an impartial human review of all claims of violations of citizens' rights, such as consumer or civil rights, through the use of algorithmic systems, whether stemming from public or private sector actors; underlines the importance of the draft Directive of the European Parliament and of the Council on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC on which a political agreement was reached on 22 June 2020, as regards future cases challenging the introduction or ongoing use of a AI system entailing a risk of violating consumer rights, or seeking remedies for a violation of rights; asks the Commission and the Member States to ensure that national and Union consumer organisations have sufficient funding to assist consumers in exercising their right to a remedy in cases where their rights have been violated;
36. Considers therefore that any natural or legal person should be able to seek redress for a decision made by artificial intelligence, robotics or related technology to his or her detriment in breach of Union or national law;
37. Considers that, as a first point of contact in cases of suspected breaches of the Union's regulatory framework in this context, national supervisory authorities could equally be addressed by consumers with requests for redress in view of ensuring the effective enforcement of the aforementioned framework;

Social responsibility and gender balance

38. Emphasises that socially responsible artificial intelligence, robotics and related technologies have a role to play in contributing to finding solutions that safeguard and promote fundamental rights and values of our society such as democracy, the rule of law, diverse and independent media and objective and freely available information, health and economic prosperity, equality of opportunity, workers' and social rights, quality education, protection of children, cultural and linguistic diversity, gender equality, digital literacy, innovation and creativity; recalls the need to ensure that the

interests of all citizens, including those who are marginalised or in vulnerable situations, such as persons with disabilities, are adequately taken into account and represented;

39. Underlines the importance of achieving a high level of overall digital literacy and training highly skilled professionals in this area as well as ensuring the mutual recognition of such qualifications throughout the Union; highlights the need of having diverse teams of developers and engineers working alongside key societal actors to prevent gender and cultural biases being inadvertently included in AI algorithms, systems and applications; supports the creation of educational curricula and public-awareness activities concerning the societal, legal, and ethical impact of artificial intelligence;
40. Stresses the vital importance of guaranteeing freedom of thought and expression, thus ensuring that these technologies do not promote hate speech or violence; thus considers hindering or restricting freedom of expression exercised digitally to be unlawful under the fundamental principles of the Union, except where the exercise of this fundamental right entails illegal acts;
41. Stresses that artificial intelligence, robotics and related technologies can contribute to reducing social inequalities and asserts that the European model for their development must be based on citizens' trust and greater social cohesion;
42. Stresses that the deployment of any artificial intelligence system should not unduly restrict users' access to public services such as social security; therefore calls on the Commission to assess how this objective can be achieved;
43. Stresses the importance of responsible research and development aiming at maximising the full potential of artificial intelligence, robotics and related technologies for citizens and the public good; calls for mobilisation of resources by the Union and its Member States in order to develop and support responsible innovation;
44. Stresses that technological expertise will be increasingly important and it will therefore be necessary to update continuously training courses, in particular for future generations, and to promote the vocational retraining of those already in the labour market; maintains, in this regard, that innovation and training should be promoted not only in the private sector but also in the public sector;
45. Insists that the development, deployment and use of these technologies should not cause injury or harm of any kind to individuals or society or the environment and that, accordingly, developers, deployers and users of these technologies should be held responsible for such injury or harm in accordance with the relevant Union and national liability rules;
46. Calls on Member States to assess whether job losses resulting from the deployment of these technologies should lead to appropriate public policies such as a reduction of working time;
47. Maintains that a design approach based on Union values and ethical principles is strongly needed to create the conditions for widespread social acceptance of artificial intelligence, robotics and related technologies; considers this approach, aimed at developing trustworthy, ethically responsible and technically robust artificial intelligence, to be an important enabler for sustainable and smart mobility that is safe and accessible;
48. Draws attention to the high added value provided by autonomous vehicles for persons with

reduced mobility, as such vehicles allow such persons to participate more effectively in individual road transport and thereby facilitate their daily lives; stresses the importance of accessibility, especially when designing MaaS-systems (Mobility as a Service);

49. Calls on the Commission to further support the development of trustworthy AI systems in order to render transport safer, more efficient, accessible, affordable and inclusive, including for persons with reduced mobility, particularly persons with disabilities, taking account of Directive (EU) 2019/882 of the European Parliament and of the Council¹ and of Union law on passenger rights;
50. Considers that AI can help to better utilise the skills and competences of people with disabilities and that the application of AI in the workplace can contribute to inclusive labour markets and higher employment rates for people with disabilities;

Environment and sustainability

51. States that artificial intelligence, robotics and related technologies should be used by governments and businesses to benefit people and the planet, contribute to the achievement of sustainable development, the preservation of the environment, climate neutrality and circular economy goals; the development, deployment and use of these technologies should contribute to the green transition, preserve the environment, and minimise and remedy any harm caused to the environment during their lifecycle and across their entire supply chain in line with Union law;
52. Given their significant environmental impact, for the purposes of the previous paragraph, the environmental impact of developing, deploying and using artificial intelligence, robotics and related technologies could, where relevant and appropriate, be evaluated throughout their lifetime by sector specific authorities; such evaluation could include an estimate of the impact of the extraction of the materials needed, and the energy consumption and the greenhouse gas emissions caused, by their development, deployment and use;
53. Proposes that for the purpose of developing responsible cutting-edge artificial intelligence solutions, the potential of artificial intelligence, robotics and related technologies should be explored, stimulated and maximised through responsible research and development that requires the mobilisation of resources by the Union and its Member States;
54. Highlights the fact that the development, deployment and use of these technologies provide opportunities for promotion of the Sustainable Development Goals outlined by the United Nations, global energy transition and decarbonisation;
55. Considers that the objectives of social responsibility, gender equality, environmental protection and sustainability should be without prejudice to existing general and sectorial obligations within these fields; believes that non-binding implementation guidelines for developers, deployers and users, especially of high-risk technologies, regarding the methodology for assessing their compliance with this Regulation and the achievement of those objectives should be established;
56. Calls on the Union to promote and fund the development of human-centric artificial

¹ Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (OJ L 151, 7.6.2019, p. 70).

intelligence, robotics and related technologies that address environment and climate challenges and that ensure the respect for fundamental rights through the use of tax, procurement or other incentives;

57. Stresses that, despite the current high carbon footprint of development, deployment and use of artificial intelligence, robotics and related technologies, including automated decisions and machine learning, those technologies can contribute to the reduction of the current environmental footprint of the ICT sector; underlines that these and other properly regulated related technologies should be critical enablers for attaining the goals of the Green Deal, the UN Sustainable Development Goals and the Paris Agreement in many different sectors and should boost the impact of policies delivering environmental protection, for example policies concerning waste reduction and environmental degradation;
58. Calls on the Commission to carry out a study on the impact of AI technology's carbon footprint and the positive and negative impacts of the transition to the use of AI technology by consumers;
59. Notes that, given the increasing development of AI applications, which require computational, storage and energy resources, the environmental impact of AI systems should be considered throughout their lifecycle;
60. Considers that in areas such as health, liability must ultimately lie with a natural or legal person; emphasises the need for traceable and publicly available training data for algorithms;
61. Strongly supports the creation of a European Health Data Space proposed by the Commission in its Communication on a European strategy for data which aims at promoting health-data exchange and at supporting research in full respect of data protection, including processing data with AI technology, and which strengthens and extends the use and re-use of health data; encourages the upscaling of cross-border exchange of health data, the linking and use of such data through secure, federated repositories, specific kinds of health information, such as European Health Records (EHRs), genomic information, and digital health images to facilitate Union-wide interoperable registers or databases in areas such as research, science and health sectors;
62. Highlights the benefits of AI for disease prevention, treatment and control, exemplified by AI predicting the COVID19 epidemic before the WHO; urges the Commission to adequately equip ECDC with the regulatory framework and resources for gathering necessary anonymised real-time global health data independently in conjunction with the Member States, so as, among other purposes, to address issues revealed by the COVID19 crisis;

Privacy and biometric recognition

63. Observes that data production and use, including personal data such as biometric data, resulting from the development, deployment and use of artificial intelligence, robotics and related technologies are rapidly increasing, thereby underlining the need to respect and enforce the rights of citizens to privacy and protection of personal data in line with Union law;
64. Points out that the possibility provided by these technologies for using personal and

non-personal data to categorise and micro-target people, identify vulnerabilities of individuals, or exploit accurate predictive knowledge, has to be counterweighed by effectively enforced data protection and privacy principles such as data minimisation, the right to object to profiling and control the use of one's data, the right to obtain an explanation of a decision based on automated processing and privacy by design, as well as those of proportionality, necessity and limitation based on strictly identified purposes in compliance with GDPR;

65. Emphasises that when remote recognition technologies, such as recognition of biometric features, notably facial recognition, are used by public authorities, for substantial public interest purposes, their use should always be disclosed, proportionate, targeted and limited to specific objectives, restricted in time in accordance with Union law and have due regard for human dignity and autonomy and the fundamental rights set out in the Charter. Criteria for and limits to that use should be subject to judicial review and democratic scrutiny and should take into account its psychological and sociocultural impact on civil society;
66. Points out that while deploying artificial intelligence, robotics and related technologies within the framework of public power decisions has benefits, it can result in grave misuse, such as mass surveillance, predictive policing and breaches of due process rights;
67. Considers that technologies which can produce automated decisions, thus replacing decisions taken by public authorities, should be treated with the utmost precaution, notably in the area of justice and law enforcement;
68. Believes that Member States should have recourse to such technologies only if there is thorough evidence of their trustworthiness and if meaningful human intervention and review is possible or systematic in cases where fundamental liberties are at stake; underlines the importance for national authorities to undertake a strict fundamental rights impact assessment for artificial intelligence systems deployed in these cases, especially following the assessment of those technologies as high-risk;
69. Is of the opinion that any decision taken by artificial intelligence, robotics or related technologies within the framework of prerogatives of public power should be subject to meaningful human intervention and due process, especially following the assessment of those technologies as high-risk;
70. Believes that the technological advancement should not lead to the use of artificial intelligence, robotics and related technologies to autonomously take public sector decisions which have a direct and significant impact on citizen's rights and obligations;
71. Notes that AI, robotics and related technologies in the area of law enforcement and border control could enhance public safety and security, but also needs extensive and rigorous public scrutiny and the highest possible level of transparency both with regards to the risk assessment of individual applications, as well as a general overview of the use of AI, robotics and related technologies in the area of law enforcement and border control; considers that such technologies bear significant ethical risks that must be adequately addressed, considering the possible adverse effects on individuals when it comes, in particular to their rights to privacy, data protection and non-discrimination; stresses that their misuse can become a direct threat to democracy and that their deployment and use must respect the principles of proportionality and necessity, the

Charter of Fundamental Rights, as well as the relevant secondary Union law, such as data protection rules; stresses that AI should never replace humans in issuing judgments; considers that decisions, such as getting bail or probation, that are heard in court, or decisions based solely on automated processing producing a legal effect concerning the individual or which significantly affect them, must always involve meaningful assessment and human judgement;

Good governance

72. Stresses that appropriate governance of the development, deployment and use of artificial intelligence, robotics and related technologies, especially high-risk technologies by having measures in place focusing on accountability and addressing potential risks of bias and discrimination, can increase citizens' safety and trust in those technologies;
73. Considers that a common framework for the governance of these technologies, coordinated by the Commission and/or any relevant institutions, bodies, offices or agencies of the Union that may be designated for this task in this context, to be implemented by national supervisory authorities in each Member State, would ensure a coherent Union approach and prevent a fragmentation of the single market;
74. Observes that data are used in large volumes in the development of artificial intelligence, robotics and related technologies and that the processing, sharing of, access to and use of such data must be governed in accordance with the law and the requirements of quality, integrity, interoperability, transparency, security, privacy and control set out therein;
75. Recalls that access to data is an essential component in the growth of the digital economy; points out in this regard that interoperability of data, by limiting lock-in effects, plays a key role in ensuring fair market conditions and promoting a level playing field in the Digital Single Market;
76. Underlines the need to ensure that personal data are protected adequately, especially data on, or stemming from, vulnerable groups, such as people with disabilities, patients, children, the elderly, minorities, migrants and other groups at risk of exclusion;
77. Notes that the development, deployment and use of artificial intelligence, robotics and related technologies by public authorities are often outsourced to private parties; considers that this should not compromise the protection of public values and fundamental rights in any way; considers that public procurement terms and conditions should reflect the ethical standards imposed on public authorities, when applicable;

Consumers and the internal market

78. Underlines the importance of a regulatory framework for AI being applicable where consumers within the Union are users of, subject to, targeted by, or directed towards an algorithmic system, irrespective of the place of establishment of the entities that develop, sell or employ the system; furthermore, believes that, in the interest of legal certainty, the rules set out in such a framework should apply to all developers and across the value chain, namely the development, deployment and use of the relevant technologies and their components, and should guarantee a high level of consumer protection;
79. Notes the intrinsic link between artificial intelligence, robotics and related technologies,

including software, algorithms and data used or produced by such technologies, and fields such as the internet of things, machine learning, rule-based systems or automated and assisted decision making processes; further notes that standardised icons could be developed to help explain such systems to consumers whenever those systems are characterised by complexity or are enabled to make decisions that impact the lives of consumers significantly;

80. Recalls that the Commission should examine the existing legal framework and its application, including the consumer law *acquis*, product liability legislation, product safety legislation and market surveillance legislation, in order to identify legal gaps, as well as existing regulatory obligations; considers that this is necessary in order to ascertain whether it is able to respond to the new challenges posed by the emergence of artificial intelligence, robotics and related technologies and ensure a high level of consumer protection;
81. Stresses the need to effectively address the challenges created by artificial intelligence, robotics and related technologies and to ensure that consumers are empowered and properly protected; underlines the need to look beyond the traditional principles of information and disclosure on which the consumer law *acquis* has been built, as stronger consumer rights and clear limitations regarding the development, deployment and use of artificial intelligence, robotics and related technologies will be necessary to ensure such technology contributes to making consumers' lives better and evolves in a way that respects fundamental and consumer rights and Union values;
82. Points out that the legislative framework introduced by Decision No 768/2008/EC¹ provides for a harmonised list of obligations for producers, importers and distributors, encourages the use of standards and provides for several levels of control depending on the dangerousness of the product; considers that that framework should also apply to AI embedded products;
83. Notes that for the purpose of analysing the impacts of artificial intelligence, robotics and related technologies on consumers, access to data could, when in full respect of Union law, such as that concerning data protection, privacy and trade secrets, be extended to national competent authorities ; recalls the importance of educating consumers to be more informed and skilled when dealing with artificial intelligence, robotics and related technologies, in order to protect them from potential risks and uphold their rights;
84. Calls on the Commission to propose measures for data traceability, having in mind both the legality of data acquisition and the protection of consumer rights and fundamental rights, while fully respecting Union law such as that concerning data protection, privacy, intellectual property rights and trade secrets;
85. Notes that these technologies should be user-centric and designed in a way that allows everyone to use AI products or services, regardless of their age, gender, abilities or characteristics; notes their accessibility for persons with disabilities is of particular importance; notes that there should not be a one-size-fits-all approach and universal design principles addressing the widest possible range of users and following relevant accessibility standards should be considered; stresses that this will enable individuals to

¹ Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (OJ L 218, 13.8.2008, p. 82).

have equitable access to and to actively participate in existing and emerging computer-mediated human activities and assistive technologies.

86. Stresses that where money originating from public sources significantly contributes to the development, deployment or use of artificial intelligence, robotics and related technologies, in addition to open procurement and open contracting standards, consideration could be given to the possibility of having the code, the generated data -as far as they are non-personal- and the trained model made public by default upon agreement with the developer, in order to guarantee transparency, enhance cybersecurity and enable the reuse thereof so as to foster innovation; stresses that, in this way, the full potential of the single market can be unlocked, avoiding market fragmentation;
87. Considers that AI, robotics and related technologies have enormous potential to deliver opportunities for consumers to have access to several amenities in many aspects of their lives alongside better products and services, as well as to benefit from better market surveillance, as long as all applicable principles, conditions, including transparency and auditability, and regulations continue to apply;

Security and defence

88. Highlights that the security and defence policies of the European Union and its Member States are guided by the principles enshrined in the Charter and by those of the United Nations Charter, and by a common understanding of the universal values of respect for the inviolable and inalienable rights of the human person, human dignity, of freedom, of democracy, of equality and of the rule of law; stresses that all defence-related efforts within the Union framework must respect those universal values whilst promoting peace, security and progress in Europe and in the world;
89. Welcomes the endorsement, by the 2019 Meeting of High Contracting Parties to the United Nations Convention on Certain Conventional Weapons (CCW), of 11 Guiding Principles for the development and use of autonomous weapons systems; regrets however the failure to agree on a legally binding instrument regulating lethal autonomous weapons (LAWS), with an effective enforcement mechanism; welcomes and supports the report by the Commission's High-Level Expert Group on Artificial Intelligence entitled 'Ethics Guidelines for Trustworthy AI' published on 9 April 2019 and its position on lethal autonomous weapon systems (LAWS); urges Member States to develop national strategies for the definition and status of lethal autonomous weapons (LAWS) towards a comprehensive strategy at Union level and to promote, together with the Union's High Representative/Vice-President of the Commission ('HR/VP') and the Council, the discussion on LAWS in the UN CCW framework and other relevant fora and the establishment of international norms regarding the ethical and legal parameters for the development and use of fully autonomous, semi-autonomous and remotely operated lethal weapons systems; recalls in this respect its resolution on autonomous weapon systems of 12 September 2018 and calls once again for the urgent development and adoption of a common position on lethal autonomous weapon systems, for an international ban on the development, production and use of lethal autonomous weapon systems enabling strikes to be carried out without meaningful human control and without respect for the human-in-the-loop principle, in line with the statement of the world's most prominent AI researchers in their open letter from 2015; welcomes the agreement of 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; believes that ethical aspects of other AI-applications in defence, such as intelligence, surveillance and reconnaissance (ISR) or cyber operations must not be overlooked, and special attention must be paid to the development and deployment of drones in military operations;

90. Underlines that emerging technologies in the defence and security sector not covered by international law should be judged taking account of the principle of respect for humanity and the dictates of public conscience;
91. Recommends that any European framework regulating the use of AI-enabled systems in defence, both in combat and non-combat situations, must respect all applicable legal regimes, in particular international humanitarian law and international human rights law, and it must be in compliance with Union law, principles and values, keeping in mind the disparities in terms of technical and security infrastructure throughout the Union;
92. Recognises that unlike defence industrial bases, critical AI innovations could come from small Member States, thus a CSDP-standardised approach should ensure that smaller Member States and SMEs are not crowded out; stresses that a set of common EU AI capabilities matched to Member States operating concepts can bridge the technical gaps that could leave out States lacking the relevant technology, industry expertise or the ability to implement AI systems in their defence ministries;
93. Considers that current and future security and defence-related activities within the Union framework will draw on AI, on robotics and autonomy, and on related technologies and that reliable, robust and trustworthy AI could contribute to a modern and effective military; the Union must therefore assume a leading role in research and development of AI systems in the security and defence field; believes that the use of AI-enabled applications in security and defence could offer a number of direct benefits to the operation commander, such as higher quality collected data, greater situational awareness, increased speed for decision-making, reduced risk of collateral damage thanks to better cabling, protection of forces on the ground, as well as greater reliability of military equipment and hence reduced risk for humans and of human casualties; stresses that the development of reliable AI in the field of defence is essential for ensuring European strategic autonomy in capability and operational areas; recalls that AI systems are also becoming key elements in countering emerging security threats, such as cyber and hybrid warfare both in the online and offline spheres; underlines at the same time all the risks and challenges of unregulated use of AI; notes that AI could be exposed to manipulation, to errors and inaccuracies;
94. Stresses that AI technologies are, in essence, of dual use, and the development of AI in defence-related activities benefits from exchanges between military and civil technologies; highlights that AI in defence-related activities is a transverse disruptive technology, the development of which may provide opportunities for the competitiveness and the strategic autonomy of the Union;
95. Recognises, in the hybrid and advanced warfare context of today, that the volume and velocity of information during the early phases of a crisis might be overwhelming for human analysts and that an AI system could process the information to ensure that human decision-makers are tracking the full spectrum of information within an appropriate timeframe for a speedy response;

96. Underlines the importance of investing in the development of human capital for artificial intelligence, fostering the necessary skills and education in the field of security and defence AI technologies with particular focus on ethics of semi-autonomous and autonomous operational systems based on human accountability in an AI-enabled world; stresses in particular the importance of ensuring that ethicists in this field have appropriate skills and receive proper training ; calls on the Commission to present as soon as possible its 'Reinforcement of the Skills Agenda', announced in the White Paper on Artificial Intelligence on 19 February 2020;
97. Stresses that quantum computing could represent the most revolutionary change in conflict since the advent of atomic weaponry and thus urges that the further development of quantum computing technologies be a priority for the Union and Member States; recognises that acts of aggression, including attacks on critical infrastructure, aided by quantum computing will create a conflict environment in which the time available to make decisions will be compressed dramatically from days and hours to minutes and seconds, forcing Member States to develop capabilities that protect themselves and train both its decision makers and military personnel to respond effectively within such timeframes;
98. Calls for increased investment in European AI for defence and in the critical infrastructure that sustains it;
99. Recalls that most of the current military powers worldwide have already engaged in significant R&D efforts related to the military dimension of artificial intelligence; considers that the Union must ensure that it does not lag behind in this regard;
100. Calls on the Commission to embed cybersecurity capacity-building in its industrial policy in order to ensure the development and deployment of safe, resilient and robust AI-enabled and robotic systems; calls on the Commission to explore the use of blockchain-based cybersecurity protocols and applications to improve the resilience, trustworthiness and robustness of AI infrastructures through disintermediated models of data encryption; encourages European stakeholders to research and engineer advanced features that would facilitate the detection of corrupt and malicious AI-enabled & robotics systems which could undermine the security of the Union and of citizens;
101. Stresses that all AI-systems in defence must have a concrete and well-defined mission framework, whereby humans retain the agency to detect and disengage or deactivate deployed systems should they move beyond the mission framework defined and assigned by a human commander, or should they engage in any escalatory or unintended action; considers that AI-enabled systems, products and technology intended for military use should be equipped with a 'black box' to record every data transaction carried out by the machine;
102. Underlines that the entire responsibility and accountability for the decision to design, develop, deploy and use AI-systems must rest on human operators, as there must be meaningful human monitoring and control over any weapon system and human intent in the decision to use force in the execution of any decision of AI-enabled weapons systems that might have lethal consequences; underlines that human control should remain effective for the command and control of AI-enabled systems, following the human-in-the-loop, human-on-the-loop and human-in-command principles at the military leadership level; stresses that AI-enabled systems must allow the military leadership of armies to assume its full responsibility and accountability for the use of

lethal force and exercise the necessary level of judgment, which machines cannot be endowed with as such judgment must be based on distinction, proportionality and precaution, for taking lethal or large-scale destructive action by means of such systems; stresses the need to establish clear and traceable authorisation and accountability frameworks for the deployment of smart weapons and other AI-enabled systems, using unique user characteristics like biometric specifications to enable deployment exclusively by authorised personnel;

Transport

103. Highlights the potential of using artificial intelligence, robotics and related technologies for all autonomous means of road, rail, waterborne and air transport, and also for boosting the modal shift and intermodality, as such technologies can contribute to finding the optimal combination of modes of transport for the transport of goods and passengers; furthermore, stresses their potential to make transport, logistics and traffic flows more efficient and to make all modes of transport safer, smarter, and more environmentally friendly; points out that an ethical approach to AI can also be seen as an early warning system, in particular as regards the safety and efficiency of transport;
104. Highlights the fact that the global competition between companies and economic regions means that the Union needs to promote investments and strengthen the international competitiveness of companies operating in the transport sector, by establishing an environment favourable for the development and application of AI solutions and further innovations, in which Union-based undertakings can become world leaders in the development of AI technologies;
105. Stresses that the Union's transport sector needs an update of the regulatory framework concerning such emerging technologies and their use in the transport sector and a clear ethical framework for achieving trustworthy AI, including safety, security, the respect of human autonomy, oversight and liability aspects, which will increase benefits that are shared by all and will be key to boosting investment in research and innovation, development of skills and the uptake of AI by public services, SMEs, start-ups and businesses and at the same time ensuring data protection as well as interoperability, without imposing an unnecessary administrative burden on businesses and consumers;
106. Notes that the development and implementation of AI in the transport sector will not be possible without modern infrastructure, which is an essential part of intelligent transport systems; stresses that the persistent divergences in the level of development between Member States create the risk of depriving the least developed regions and their inhabitants of the benefits brought by the development of autonomous mobility; calls for the modernisation of transport infrastructure in the Union, including its integration into the 5G network, to be adequately funded;
107. Recommends the development of Union-wide trustworthy AI standards for all modes of transport, including the automotive industry, and for testing of AI-enabled vehicles and related products and services;
108. Notes that AI systems could help to reduce the number of road fatalities significantly, for instance through better reaction times and better compliance with rules; considers, however, that it will be impossible for use of autonomous vehicles to result in the elimination of all accidents and underlines that this makes the explainability of AI decisions increasingly important in order to justify shortcomings and unintended

consequences of AI decisions;

Employment, workers' rights, digital skills and the workplace

109. Notes that the application of artificial intelligence, robotics and related technologies in the workplace can contribute to inclusive labour markets and impact occupational health and safety, while it can also be used to monitor, evaluate, predict and guide the performance of workers with direct and indirect consequences for their careers; whereas AI should have a positive impact on working conditions and be guided by respect for human rights as well as the fundamental rights and values of the Union; whereas AI should be human centric, enhance the well-being of people and society and contribute to a fair and just transition; such technologies should therefore have a positive impact on working conditions guided by respect for human rights as well as the fundamental rights and values of the Union;
110. Highlights the need for competence development through training and education for workers and their representatives with regard to AI in the workplace to better understand the implications of AI solutions; stresses that applicants and workers should be duly informed in writing when AI is used in the course of recruitment procedures and other human resource decisions and how in this case a human review can be requested in order to have an automated decision reversed;
111. Stresses the need to ensure that productivity gains due to the development and use of AI and robotics do not only benefit company owners and shareholders, but also profit companies and the workforce, through better working and employment conditions, including wages, economic growth and development, and also serve society at large, especially where such gains come at the expense of jobs; calls on the Member States to carefully study the potential impact of AI on the labour market and social security systems and to develop strategies as to how to ensure long-term stability by reforming taxes and contributions as well as other measures in the event of smaller public revenues;
112. Underlines the importance of corporate investment in formal and informal training and life-long learning in order to support the just transition towards the digital economy; stresses in this context that companies deploying AI have the responsibility of providing adequate re-skilling and up-skilling for all employees concerned, in order for them to learn how to use digital tools and to work with co-bots and other new technologies, thereby adapting to changing needs of the labour market and staying in employment;
113. Considers that special attention should be paid to new forms of work, such as gig and platform work, resulting from the application of new technologies in this context; stresses that regulating telework conditions across the Union and ensuring decent working and employment conditions in the digital economy must likewise take the impact of AI into account; calls on the Commission to consult with social partners, AI-developers, researchers and other stakeholders in this regard;
114. Underlines that artificial intelligence, robotics and related technologies must not in any way affect the exercise of fundamental rights as recognised in the Member States and at Union level, including the right or freedom to strike or to take other action covered by the specific industrial relations systems in Member States, in accordance with national law and/or practice, or affect the right to negotiate, to conclude and enforce collective agreements, or to take collective action in accordance with national law and/or practice;

115. Reiterates the importance of education and continuous learning to develop the qualifications necessary in the digital age and to tackle digital exclusion; calls on the Member States to invest in high quality, responsive and inclusive education, vocational training and life-long learning systems as well as re-skilling and up-skilling policies for workers in sectors that are potentially severely affected by AI; highlights the need to provide the current and future workforce with the necessary literacy, numeracy and digital skills as well as competences in science, technology, engineering and mathematics (STEM) and cross-cutting soft skills, such as critical thinking, creativity and entrepreneurship; underlines that special attention must be paid to the inclusion of disadvantaged groups in this regard;
116. Recalls that artificial intelligence, robotics and related technologies used at the workplace must be accessible for all, based on the design for all principle;

Education and culture

117. Stresses the need to develop criteria for the development, the deployment and the use of AI bearing in mind their impact on education, media, youth, research, sports and the cultural and creative sectors, by developing benchmarks for and defining principles of ethically responsible and accepted uses of AI technologies that can be appropriately applied in these areas, including a clear liability regime for products resulting from AI use;
118. Notes that every child enjoys the right to public education of quality at all levels; therefore, calls for the development, the deployment and the use of quality AI systems that facilitate and provide quality educational tools for all at all levels and stresses that the deployment of new AI systems in schools should not lead to a wider digital gap being created in society; recognises the enormous potential contribution that AI and robotics can make to education; notes that AI personalised learning systems should not replace educational relationships involving teachers and that traditional forms of education should not be left behind, while at the same time pointing out that financial, technological and educational support, including specialised training in information and communications technology must be provided for teachers seeking to acquire appropriate skills so as to adapt to technological changes and not only harness the potential of AI but also understand its limitations; calls for a strategy to be developed at Union level in order to help transform and update our educational systems, prepare our educational institutions at all levels and equip teachers and pupils with the necessary skills and abilities;
119. Emphasises that educational institutions should aim to use AI systems for educational purposes that have received a European certificate of ethical compliance;
120. Emphasises that opportunities provided by digitisation and new technologies must not result in an overall loss of jobs in the cultural and creative sectors, the neglect of the conservation of originals or in the downplaying of traditional access to cultural heritage, which should equally be encouraged; notes that AI systems developed, deployed and used in the Union should reflect its cultural diversity and its multilingualism;
121. Acknowledges the growing potential of AI in the areas of information, media and online platforms, including as a tool to fight disinformation in accordance with Union law; underlines that, if not regulated, it might also have ethically adverse effects by exploiting biases in data and algorithms that may lead to disseminating disinformation

and creating information bubbles; emphasises the importance of transparency and accountability of algorithms used by video-sharing platforms (VSP) as well as streaming platforms, in order to ensure access to culturally and linguistically diverse content;

National supervisory authorities

122. Notes the added value of having designated national supervisory authorities in each Member State, responsible for ensuring, assessing and monitoring compliance with legal obligations and ethical principles for the development, deployment and use of high-risk artificial intelligence, robotics and related technologies, thus contributing to the legal and ethical compliance of these technologies;
123. Believes that these authorities must be required to, without duplicating their tasks, cooperate with the authorities responsible for implementing sectorial legislation in order to identify technologies which are high-risk from an ethical perspective and in order to supervise the implementation of required and appropriate measures where such technologies are identified;
124. Indicates that such authorities should liaise not only among themselves but also with the European Commission and other relevant institutions, bodies, offices and agencies of the Union in order to guarantee coherent cross-border action;
125. Suggests that, in the context of such cooperation, common criteria and an application process be developed for the granting of a European certificate of ethical compliance, including following a request by any developer, deployer or user of technologies not considered as high-risk seeking to certify the positive assessment of compliance carried out by the respective national supervisory authority;
126. Calls for such authorities to be tasked with promoting regular exchanges with civil society and innovation within the Union by providing assistance to researchers, developers, and other relevant stakeholders, as well as to less digitally-mature companies, in particular small and medium-sized enterprises or start-ups; in particular regarding awareness-raising and support for development, deployment, training and talent acquisition to ensure efficient technology transfer and access to technologies, projects, results and networks;
127. Calls for sufficient funding by each Member State of their designated national supervisory authorities and stresses the need for national market surveillance authorities to be reinforced in terms of capacity, skills and competences, as well as knowledge about the specific risks of artificial intelligence, robotics and related technologies;

Coordination at Union level

128. Underlines the importance of coordination at Union level as carried out by the Commission and/or any relevant institutions, bodies, offices and agencies of the Union that may be designated in this context, in order to avoid fragmentation, and of ensuring a harmonised approach across the Union; considers that coordination should focus on the mandates and actions of the national supervisory authorities in each Member State as referred to in the previous sub-section, as well as on sharing of best practices among those authorities and contributing to the cooperation as regards research and development in the field throughout the Union; calls on the Commission to assess and

find the most appropriate solution to structure such coordination; examples of relevant existing institutions, bodies, offices and agencies of the Union are ENISA, the EDPS and the European Ombudsman;

129. Believes that such coordination, as well as a European certification of ethical compliance, would not only benefit the development of Union industry and innovation in that context but also increase the awareness of citizens regarding the opportunities and risks inherent to these technologies;
130. Suggests a centre of expertise be created, bringing together academia, research, industry, and individual experts at Union level, to foster exchange of knowledge and technical expertise, and to facilitate collaboration throughout the Union and beyond; further calls for this centre of expertise to involve stakeholder organisations, such as consumer protection organisations, in order to ensure wide consumer representation; considers that due to the possible disproportionate impact of algorithmic systems on women and minorities, the decision levels of such a structure should be diverse and ensure gender equality; emphasises that Member States must develop risk-management strategies for AI in the context of their national market surveillance strategies;
131. Proposes that the Commission and/or any relevant institutions, bodies, offices and agencies of the Union that may be designated in this context provide any necessary assistance to national supervisory authorities concerning their role as first points of contact in cases of suspected breaches of the legal obligations and ethical principles set out in the Union's regulatory framework for AI, including the principle of non-discrimination; it should also provide any necessary assistance to national supervisory authorities in cases where the latter carry out compliance assessments in view of supporting the right of citizens to contest and redress, namely by supporting, when applicable, the consultation of other competent authorities in the Union, in particular the Consumer Protection Cooperation Network and national consumer protection bodies, civil society organisations and social partners located in other Member States;
132. Acknowledges the valuable output of the High-Level Expert Group on Artificial Intelligence, comprising representatives from academia, civil society and industry, as well as the European AI Alliance, particularly 'The Ethics Guidelines for Trustworthy Artificial Intelligence', and suggests that it might provide expertise to the Commission and/or any relevant institutions, bodies, offices and agencies of the Union that may be designated in this context;
133. Notes the inclusion of AI-related projects under the European Industrial Development Programme (EDIDP); believes that the future European Defence Fund (EDF) and the Permanent structured cooperation (PESCO) may also offer frameworks for future AI-related projects that could help to better streamline Union efforts in this field, and promote at the same time the Union's objective of strengthening human rights, international law, and multilateral solutions; stresses that AI-related projects should be synchronised with the wider Union civilian programmes devoted to AI; notes that, in line with the European Commission's White Paper of 19 February 2020 on Artificial Intelligence, excellence and testing centres concentrating on research and development of AI in the field of security and defence should be established with rigorous specifications underpinning the participation of and investment from private stakeholders;
134. Takes note of the Commission's White Paper of 19 February 2020 on Artificial

Intelligence and regrets that military aspects were not taken into account; calls on the Commission and on the HR/VP to present, also as part of an overall approach, a sectorial AI strategy for defence-related activities within the Union framework, that ensures both respect for citizens' rights and the Union's strategic interests, and that is based on a consistent approach spanning from the inception of AI-enabled systems to their military uses, and to establish a working Group on security and defence within the High-Level Expert Group on Artificial Intelligence that should specifically deal with policy and investment questions as well as ethical aspects of AI in the field of security and defence; calls on the Council, the Commission and on the VP/HR to enter into a structured dialogue with Parliament to that end;

European certification of ethical compliance

135. Suggests that common criteria and an application process relating to the granting of a European certificate of ethical compliance be developed in the context of coordination at Union level, including following a request by any developer, deployer or user of technologies not considered as high-risk seeking to certify the positive assessment of compliance carried out by the respective national supervisory authority;
136. Believes that such European certificate of ethical compliance would foster ethics by design throughout the supply chain of artificial intelligence ecosystems; suggests, therefore, that this certification could be, in the case of high-risk technologies, a mandatory prerequisite for eligibility for public procurement procedures on artificial intelligence, robotics and related technologies;

International cooperation

137. Is of the opinion that effective cross-border cooperation and ethical standards can be achieved only if all stakeholders commit to ensure human agency and oversight, technical robustness and safety, transparency and accountability, diversity, non-discrimination and fairness, societal and environmental well-being, and respect the established principles of privacy, data governance and data protection, specifically those enshrined in Regulation (EU) 2016/679;
138. Stresses that the Union's legal obligations and ethical principles for the development, deployment and use of these technologies could make Europe a world leader in the artificial intelligence sector and should therefore be promoted worldwide by cooperating with international partners while continuing the critical and ethics-based dialogue with third countries that have alternative models of artificial intelligence regulation, development and deployment models;
139. Recalls that the opportunities and risks inherent to these technologies have a global dimension, as the software and data they use are frequently imported into and exported out of the Union, and therefore there is a need for a consistent cooperation approach at international level; calls on the Commission to take the initiative to assess which bilateral and multilateral treaties and agreements should be adjusted to ensure a consistent approach and promote the European model of ethical compliance globally;
140. Points out the added value of coordination at Union level as referred to above in this context as well;
141. Calls for synergies and networks to be established between the various European research centres on AI as well as other multilateral fora, such as the Council of Europe,

the United Nations Educational Scientific and Cultural Organization (UNESCO), the Organisation for Economic Co-operation and Development's (OECD), the World Trade Organisation and the International Telecommunications Union (ITU), in order to align their efforts and to better coordinate the development of artificial intelligence, robotics and related technologies;

142. Underlines that the Union must be at the forefront of supporting multilateral efforts to discuss, in the framework of the UN CCW Governmental Expert Group and other relevant fora, an effective international regulatory framework that ensures meaningful human control over autonomous weapon systems in order to master those technologies by establishing well defined, benchmark-based processes and adopting legislation for their ethical use, in consultation with military, industry, law enforcement, academic and civil society stakeholders, to understand the related ethical aspects and to mitigate the inherent risks of such technologies and prevent use for malicious purposes;
143. Recognises the role of NATO in promoting Euro-Atlantic security and calls for cooperation within NATO for the establishment of common standards and interoperability of AI systems in defence; stresses that the transatlantic relationship is important for the preservation of shared values and for countering future and emerging threats;
144. Stresses the importance of the creation of an ethical code of conduct underpinning the deployment of weaponised AI-enabled systems in military operations, similar to the existing regulatory framework prohibiting the deployment of chemical and biological weapons; is of the opinion that the Commission should initiate the creation of standards on the use of AI-enabled weapons systems in warfare in accordance with international humanitarian law, and that the Union should pursue the international adoption of such standards; considers that the Union should engage in AI diplomacy in international fora with like-minded partners like the G7, the G20 and the OECD;

Final aspects

145. Concludes, following the above reflections on aspects related to the ethical dimension of artificial intelligence, robotics and related technologies, that the legal and ethical dimensions should be enshrined in an effective, forward-looking and comprehensive regulatory framework at Union level, supported by national competent authorities, coordinated and enhanced by the Commission and/or any relevant institutions, bodies, offices and agencies of the Union that may be designated in this context, regularly supported by the aforementioned centre of expertise and duly respected and certified within the internal market;
146. In accordance with the procedure laid down in Article 225 of the Treaty on the Functioning of the European Union, requests the Commission to submit a proposal for a Regulation on ethical principles for the development, deployment and use of artificial intelligence, robotics and related technologies on the basis of Article 114 of the Treaty on the Functioning of the European Union and based on the detailed recommendations set out in the annex hereto; points out that the proposal should not undermine sector-specific legislation but should only cover identified loopholes;
147. Recommends that the European Commission, after consulting with all the relevant stakeholders, review, if necessary, existing Union law applicable to artificial intelligence, robotics and related technologies in order to address the rapidity of their

development in line with the recommendations set out in the annex hereto, avoiding over-regulation, including for SMEs;

148. Believes that a periodical assessment and review, when necessary, of the Union regulatory framework related to artificial intelligence, robotics and related technologies will be essential to ensure that the applicable legislation is up to date with the rapid pace of technological progress;
149. Considers that the legislative proposal requested would have financial implications if any European body were entrusted with the above-mentioned coordination functions and the necessary technical means and human resources to fulfil its newly attributed tasks were provided;

o

o o

150. Instructs its President to forward this resolution and the accompanying detailed recommendations to the Commission and the Council.

**ANNEX TO THE RESOLUTION:
DETAILED RECOMMENDATIONS AS TO THE CONTENT OF THE PROPOSAL
REQUESTED**

A. PRINCIPLES AND AIMS OF THE PROPOSAL REQUESTED

I. The main principles and aims of the proposal are:

- to build trust at all levels of involved stakeholders and of society in artificial intelligence, robotics and related technologies, especially when they are considered high-risk;
- to support the development of artificial intelligence, robotics and related technologies in the Union, including by helping businesses, start-ups and small and medium-sized enterprises to assess and address with certainty current and future regulatory requirements and risks during the innovation and business development process, and, during the subsequent phase of use by professionals and private individuals, by minimising burdens and red tape;
- to support deployment of artificial intelligence, robotics and related technologies in the Union by providing the appropriate and proportionate regulatory framework which should apply without prejudice to existing or future sectorial legislation, with the aim of encouraging regulatory certainty and innovation while guaranteeing fundamental rights and consumer protection;
- to support use of artificial intelligence, robotics and related technologies in the Union by ensuring that they are developed, deployed and used in a manner that is compliant with ethical principles;
- to require transparency and better information flows among citizens and within organisations developing, deploying or using artificial intelligence, robotics and related technologies, as a means of ensuring that these technologies are compliant with Union law, fundamental rights and values, and with the ethical principles of the proposal for Regulation requested.

II. The proposal consists of the following elements:

- a ‘Regulation on ethical principles for the development, deployment and use of artificial intelligence, robotics and related technologies’;
- the coordination role at Union level by the Commission and/or any relevant institutions, bodies, offices and agencies of the Union that may be designated in this context and a European certification of ethical compliance;
- the support role of the European Commission;
- the role of the ‘Supervisory Authority’ in each Member State to ensure that ethical principles are applied to artificial intelligence, robotics and related technologies;

- the involvement and consultation of, as well as provision of support to, relevant research and development projects and concerned stakeholders, including start-ups, small and medium-sized enterprises, businesses, social partners, and other representatives of civil society;
- an annex establishing an exhaustive and cumulative list of high-risk sectors and high-risk uses and purposes;

III. The ‘Regulation on ethical principles for the development, deployment and use of artificial intelligence, robotics and related technologies’ builds on the following principles:

- human-centric, human-made and human-controlled artificial intelligence, robotics and related technologies;
- mandatory compliance assessment of high-risk artificial intelligence, robotics and related technologies;
- safety, transparency and accountability;
- safeguards and remedies against bias and discrimination;
- right to redress;
- social responsibility and gender equality in artificial intelligence, robotics and related technologies;
- environmentally sustainable artificial intelligence, robotics and related technologies;
- respect for privacy and limitations on the use of biometric recognition;
- good governance relating to artificial intelligence, robotics and related technologies, including the data used or produced by such technologies.

IV. For the purposes of coordination at Union level, the Commission and/or any relevant institutions, bodies, offices and agencies of the Union that may be designated in this context should carry out the following main tasks:

- cooperating in monitoring the implementation of the proposal for a Regulation requested and relevant sectorial Union law;
- cooperating regarding the issuing of guidance concerning the consistent application of the proposal for a Regulation requested, namely the application of the criteria for artificial intelligence, robotics and related technologies to be considered high-risk and the list of high-risk sectors and high-risk uses and purposes set out in the annex to the Regulation;
- cooperating with the ‘Supervisory Authority’ in each Member State regarding the development of a European certificate of compliance with ethical principles and legal obligations as laid down in the proposal for a Regulation requested and relevant Union law, as well as the development of an application process

for any developer, deployer or user of technologies not considered as high-risk seeking to certify their compliance with the proposal for a Regulation requested;

- cooperating regarding the supporting of cross-sector and cross-border cooperation through regular exchanges with concerned stakeholders and civil society, in the EU and in the world, notably with businesses, social partners, researchers and competent authorities, including as regards the development of technical standards at international level;
- cooperating with the ‘Supervisory Authority’ in each Member State regarding the establishing of binding guidelines on the methodology to be followed for the compliance assessment to be carried out by each ‘Supervisory Authority’;
- cooperating regarding the liaising with the ‘Supervisory Authority’ in each Member State and the coordinating of their mandate and tasks;
- cooperating on raising awareness, providing information and engaging in exchanges with developers, deployers and users throughout the Union;
- cooperating on raising awareness, providing information, promoting digital literacy, training and skills and engaging in exchanges with designers, developers, deployers, citizens, users and institutional bodies throughout the Union and internationally;
- cooperating regarding the coordination of a common framework for the governance of the development, deployment and use of artificial intelligence, robotics and related technologies to be implemented by the ‘Supervisory Authority’ in each Member State;
- cooperating regarding serving as a centre for expertise by promoting the exchange of information and supporting the development of a common understanding in the Single Market;
- cooperating regarding the hosting of a Working Group on Security and Defence.

V. Additionally, the Commission should carry out the following tasks:

- drawing up and subsequently updating, by means of delegated acts, a common list of high-risk technologies identified within the Union in cooperation with the ‘Supervisory Authority’ in each Member State;
- updating, by means of delegated acts, the list provided for in the Annex to the Regulation.

VI. The ‘Supervisory Authority’ in each Member State should carry out the following main tasks:

- contributing to the consistent application of the regulatory framework established in the proposal for a Regulation requested in cooperation with the ‘Supervisory Authority’ in the other Member States, as well as other authorities

responsible for implementing sectorial legislation, the Commission and/or any relevant institutions, bodies, offices and agencies of the Union that may be designated in this context, namely regarding the application of the risk assessment criteria provided for in the proposal for a Regulation requested and of the list of high-risk sectors and of high-risk uses or purposes set out in its annex, and the following supervision of the implementation of required and appropriate measures where high-risk technologies are identified as a result of such application;

- assessing whether artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced by such technologies, developed, deployed and used in the Union are to be considered high-risk technologies in accordance with the risk assessment criteria provided for in the proposal for a Regulation requested and in the list set out in its annex;
- issuing a European certificate of compliance with ethical principles and legal obligations as laid down in the proposal for Regulation requested and relevant Union law, including when resulting from an application process for any developer, deployer or user of technologies not considered as high-risk seeking to certify their compliance with the proposal for a Regulation requested, as developed by the Commission and/or any relevant institutions, bodies, offices and agencies of the Union that may be designated in this context;
- assessing and monitoring their compliance with ethical principles and legal obligations as laid down in the proposal for a Regulation requested and relevant Union law;
- being responsible for establishing and implementing standards for the governance of artificial intelligence, robotics and related technologies, including by liaising and sustaining a regular dialogue with all relevant stakeholders and civil society representatives; to that end, cooperating with the Commission and/or any relevant institutions, bodies, offices and agencies of the Union that may be designated in this context regarding the coordination of a common framework at Union level;
- raising awareness, providing information on artificial intelligence, robotics and related technologies to the public, and supporting the training of relevant professions, including in the judiciary, thereby empowering citizens and workers with the digital literacy, skills and tools necessary for a fair transition;
- serving as a first point of contact in cases of a suspected breach of the legal obligations and ethical principles set out in the proposal for a Regulation requested and carrying out a compliance assessment in such cases; in the context of this compliance assessment, it may consult and/or inform other competent authorities in the Union, notably the Consumer Protection Cooperation Network, national consumer protection bodies, civil society organisations and social partners.

VII. The key role of stakeholders should be to engage with the Commission and/or any relevant institutions, bodies, offices and agencies of the Union that may be designated in this context and the ‘Supervisory Authority’ in each Member State.

B. TEXT OF THE LEGISLATIVE PROPOSAL REQUESTED

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on ethical principles for the development, deployment and use of artificial intelligence, robotics and related technologies

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee,

Acting in accordance with the ordinary legislative procedure,

Whereas:

- (1) The development, deployment and use of artificial intelligence, robotics and related technologies, including the software, algorithms and data used or produced by such technologies, should be based on a desire to serve society. Such technologies can entail opportunities and risks, which should be addressed and regulated by a comprehensive regulatory framework at Union level, reflecting ethical principles, to be complied with from the moment of the development and deployment of such technologies to their use.
- (2) Compliance with such a regulatory framework regarding the development, deployment and use of artificial intelligence, robotics and related technologies, including the software, algorithms and data used or produced by such technologies, in the Union should be of a level that is equivalent in all Member States, in order to efficiently seize the opportunities and consistently address the risks of such technologies, as well as avoid regulatory fragmentation. It should be ensured that the application of the rules set out in this Regulation throughout the Union is homogenous.
- (3) In this context, the current diversity of the rules and practices to be followed across the Union poses a significant risk of fragmentation of the Single Market and to the protection of the well-being and prosperity of individuals and society alike, as well

as to the coherent exploration of the full potential that artificial intelligence, robotics and related technologies have for promoting innovation and preserving that well-being and prosperity. Differences in the degree of consideration on the part of developers, deployers and users of the ethical dimension inherent to these technologies can prevent them from being freely developed, deployed or used within the Union and such differences can constitute an obstacle to a level playing field and to the pursuit of technological progress and economic activities at Union level, distort competition and impede authorities in the fulfilment of their obligations under Union law. In addition, the absence of a common regulatory framework, reflecting ethical principles, for the development, deployment and use of artificial intelligence, robotics and related technologies results in legal uncertainty for all those involved, namely developers, deployers and users.

- (4) Nevertheless, while contributing to a coherent approach at Union level and within the limits set by it, this Regulation should provide a margin for implementation by Member States, including with regard to how the mandate of their respective national supervisory authority is to be carried out, in view of the objective it is to achieve as set out herein.
- (5) This Regulation is without prejudice to existing or future sectorial legislation. It should be proportionate with regard to its objective so as not to unduly hamper innovation in the Union and be in accordance with a risk-based approach.
- (6) The geographical scope of application of such a framework should cover all the components of artificial intelligence, robotics and related technologies throughout their development, deployment and use in the Union, including in cases where part of the technologies might be located outside the Union or not have a specific or single location, such as in the case of cloud computing services.
- (7) A common understanding in the Union of notions such as artificial intelligence, robotics, related technologies and biometric recognition is required in order to allow for a unified regulatory approach and thus legal certainty for citizens and companies alike. They should be technologically neutral and subject to review whenever necessary.
- (8) In addition, the fact that there are technologies related to artificial intelligence and robotics that enable software to control physical or virtual processes, at a varying degree of autonomy¹, needs to be considered. For example, for automated driving of vehicles, six levels of driving automation have been proposed by SAE international

¹ For automated driving of vehicles, six levels of driving automation have been proposed by SAE International standard J3016, last updated in 2018 to J3016_201806. https://www.sae.org/standards/content/j3016_201806/

standard J3016.

- (9) The development, deployment and use of artificial intelligence, robotics and related technologies, including the software, algorithms and data used or produced by such technologies, should complement human capabilities, not substitute them and ensure that their execution does not run against the best interests of citizens and that it complies with Union law, fundamental rights as set out in the Charter of Fundamental Rights of the European Union (the ‘Charter’), settled case-law of the Court of Justice of the European Union, and other European and international instruments which apply in the Union.
- (10) Decisions made or informed by artificial intelligence, robotics and related technologies should remain subject to meaningful human review, judgment, intervention and control. The technical and operational complexity of such technologies should never prevent their deployer or user from being able to, at the very least, trigger a fail-safe shutdown, alter or halt their operation, or revert to a previous state restoring safe functionalities in cases where the compliance with Union law and the ethical principles and legal obligations laid down in this Regulation is at risk.
- (11) Artificial intelligence, robotics and related technologies whose development, deployment and use entail a significant risk of causing injury or harm to individuals or society in breach of fundamental rights and safety rules as laid down in Union law, should be considered as high-risk technologies. For the purposes of assessing them as such, the sector where they are developed, deployed or used, their specific use or purpose and the severity of the injury or harm that can be expected to occur should be considered. The degree of severity should be determined based on the extent of the potential injury or harm, the number of affected persons, the total value of damage caused and the harm to society as a whole. Severe types of injury and harm are, for instance, violations of children’s, consumers’ or workers’ rights that, due to their extent, the number of children, consumers or workers affected or their impact on society as a whole entail a significant risk to breach fundamental rights and safety rules as laid down in Union law. This Regulation should provide an exhaustive and cumulative list of high-risk sectors, and high-risk uses and purposes.
- (12) The obligations laid down in this Regulation, specifically those regarding high-risk technologies, should only apply to artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced by such technologies, developed, deployed or used in the Union, which, following the risk assessment provided for in this Regulation, are considered as high-risk. Such obligations are to be complied with without prejudice to the general obligation that any artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced by such technologies, should be developed,

deployed and used in the Union in a human-centric manner and based on the principles of human autonomy and human safety in accordance with Union law and in full respect of fundamental rights such as human dignity, right to liberty and security and right to the integrity of the person.

- (13) High-risk technologies should respect the principles of safety, transparency, accountability, non-bias or non-discrimination, social responsibility and gender equality, right to redress, environmental sustainability, privacy and good governance, following an impartial, objective and external risk assessment by the national supervisory authority in accordance with the criteria provided for in this Regulation and in the list set out in its annex. This assessment should take into account the views and any self-assessment made by the developer or deployer.
- (14) The Commission and/or any relevant institutions, bodies, offices and agencies of the Union that may be designated for this purpose should prepare non-binding implementation guidelines for developers, deployers and users on the methodology for compliance with this Regulation. In doing so, they should consult relevant stakeholders.
- (15) There should be coherence within the Union when it comes to the risk assessment of these technologies, especially in the event they are assessed both in light of this Regulation and in accordance with any applicable sector-specific legislation. Accordingly, national supervisory authorities should inform other authorities carrying out risk assessments in accordance with any sector-specific legislation when these technologies are assessed as high-risk following the risk assessment provided for in this Regulation.
- (16) To be trustworthy high-risk artificial intelligence, robotics and related technologies, including the software, algorithms and data used or produced by such technologies should be developed, deployed and used in a safe, transparent and accountable manner in accordance with the safety features of robustness, resilience, security, accuracy and error identification, explainability, interpretability, auditability, transparency and identifiability, and in a manner that makes it possible to disable the functionalities concerned or to revert to a previous state restoring safe functionalities, in cases of non-compliance with those features. Transparency should be ensured by allowing access to public authorities, when strictly necessary, to technology, data and computing systems underlying such technologies.
- (17) Developers, deployers and users of artificial intelligence, robotics and related technologies, especially high-risk technologies, are responsible to varying degrees for the compliance with safety, transparency and accountability principles to the extent of their involvement with the technologies concerned, including the software, algorithms and data used or produced by such technologies. Developers should

ensure that the technologies concerned are designed and built in line with the safety features set out in this Regulation, whereas deployers and users should deploy and use the concerned technologies in full observance of those features. To this end, developers of high-risk technologies should evaluate and anticipate the risks of misuse that can reasonably be expected regarding of the technologies they develop. They must also ensure that the systems they develop indicate to the extent possible and through appropriate means, such as disclaimer messages, the likelihood of errors or inaccuracies.

- (18) Developers and deployers should make available to users any subsequent updates of the technologies concerned, namely in terms of software as stipulated by contract or laid down in Union or national law. In addition where a risk assessment so indicates, developers and deployers should provide public authorities with the relevant documentation on the use of the technologies concerned and safety instructions in that regard, including, when strictly necessary and in full respect of Union law on data protection, privacy and intellectual property rights and trade secrets, the source code, development tools and data used by the system.
- (19) Individuals have a right to expect the technology they use to perform in a reasonable manner and to respect their trust. The trust placed by citizens in artificial intelligence, robotics and related technologies, including the software, algorithms and data used or produced by such technologies, depends on the understanding and comprehension of the technical processes. The degree of explainability of such processes should depend on the context of those technical processes, and on the severity of the consequences of an erroneous or inaccurate output, and needs to be sufficient for challenging them and for seeking redress. Auditability, traceability, and transparency should address any possible unintelligibility of such technologies.
- (20) Society's trust in artificial intelligence, robotics and related technologies, including the software, algorithms and data used or produced by such technologies, depends on the degree to which their assessment, auditability and traceability are enabled in the technologies concerned. Where the extent of their involvement so requires, developers should ensure that such technologies are designed and built in a manner that enables such an assessment, auditing and traceability. Within the limits of what is technically possible, developers, deployers and users should ensure that artificial intelligence, robotics and related technologies are deployed and used in full respect of transparency requirements, and allowing auditing and traceability.
- (21) In order to ensure transparency and accountability, citizens should be informed when a system uses artificial intelligence, when artificial intelligence systems personalise a product or service for its users, whether they can switch off or limit the personalisation and when they are faced with an automated decision making technology. Furthermore, transparency measures should be accompanied, as far as

this is technically possible, by clear and understandable explanations of the data used and of the algorithm, its purpose, its outcomes and its potential dangers.

- (22) Bias in and discrimination by software, algorithms and data is unlawful and should be addressed by regulating the processes through which they are designed and deployed. Bias can originate both from decisions informed or made by an automated system as well as from data sets on which such decision making is based or with which the system is trained.
- (23) Software, algorithms and data used or produced by artificial intelligence, robotics and related technologies should be considered biased where, for example, they display suboptimal results in relation to any person or group of persons, on the basis of a prejudiced personal or social perception and subsequent processing of data relating to their traits.
- (24) In line with Union law, software, algorithms and data used or produced by artificial intelligence, robotics and related technologies should be considered discriminatory where they produce outcomes that have disproportionate negative effects and result in different treatment of a person or group of persons, including by putting them at a disadvantage when compared to others, based on grounds such as their personal traits, without objective or reasonable justification and regardless of any claims of neutrality of the technologies.
- (25) In line with Union law, legitimate aims that could under this Regulation be considered to objectively justify any differential treatment between persons or group of persons are the protection of public safety, security and health, the prevention of criminal offences, the protection of fundamental rights and freedoms, fair representation and objective requirements for holding a professional occupation.
- (26) Artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced by such technologies, should contribute to sustainable progress. Such technologies should not run counter to the cause of preservation of the environment or the green transition. They could play an important role in achieving the Sustainable Development Goals outlined by the United Nations with a view to enabling future generations to flourish. Such technologies can support the monitoring of adequate progress on the basis of sustainability and social cohesion indicators, and by using responsible research and innovation tools requiring the mobilisation of resources by the Union and its Member States to support and invest in projects addressing those goals.
- (27) The development, deployment and use of artificial intelligence, robotics and related technologies, including the software, algorithms and data used or produced by such technologies, should in no way purposefully cause or accept by design injury or harm of any kind to individuals or society. Accordingly, high-risk technologies in

particular should be developed, deployed and used in a socially responsible manner.

- (28) Therefore, developers, deployers and users should be held responsible, to the extent of their involvement in the artificial intelligence, robotics and related technologies concerned, and in accordance with Union and national liability rules, for any injury or harm inflicted upon individuals and society.
- (29) In particular, the developers who take decisions that determine and control the course or manner of the development of artificial intelligence, robotics and related technologies, as well as the deployers who are involved in their deployment by taking decisions regarding such deployment and by exercising control over the associated risks or benefiting from such deployment, with a controlling or managing function, should be generally considered responsible for avoiding the occurrence of any such injury or harm, by putting adequate measures in place during the development process and thoroughly respecting such measures during the deployment phase, respectively.
- (30) Socially responsible artificial intelligence, robotics and related technologies, including the software, algorithms and data used or produced by such technologies, can be defined as technologies which contribute to find solutions that safeguard and promote different aims regarding society, most notably democracy, health and economic prosperity, equality of opportunity, workers' and social rights, diverse and independent media and objective and freely available information, allowing for public debate, quality education, cultural and linguistic diversity, gender balance, digital literacy, innovation and creativity. They are also those that are developed, deployed and used having due regard for their ultimate impact on the physical and mental well-being of citizens and that do not promote hate speech or violence. Such aims should be achieved in particular by means of high-risk technologies.
- (31) Artificial intelligence, robotics and related technologies should also be developed, deployed and used with a view to supporting social inclusion, democracy, plurality, solidarity, fairness, equality and cooperation and their potential in that context should be maximised and explored through research and innovation projects. The Union and its Member States should therefore mobilise their communication, administrative and financial resources for the purpose of supporting and investing in such projects.
- (32) Projects relating to the potential of artificial intelligence, robotics and related technologies to deal with the question of social well-being should be carried out on the basis of responsible research and innovation tools so as to guarantee the compliance with ethical principles of those projects from the outset.
- (33) The development, deployment and use of artificial intelligence, robotics and related technologies, including the software, algorithms and data used or produced by such technologies, should take into consideration their environmental footprint. In line

with obligations laid down in applicable Union law, such technologies should not cause harm to the environment during their lifecycle and across their entire supply chain and should be developed, deployed and used in a manner that preserves the environment, mitigates and remedies their environmental footprint, contributes to the green transition and supports the achievement of climate neutrality and circular economy goals.

- (34) For the purposes of this Regulation, developers, deployers and users should be held responsible, to the extent of their respective involvement in the development, deployment or use of any artificial intelligence, robotics and related technologies considered as high-risk, for any harm caused to the environment in accordance with the applicable environmental liability rules.
- (35) These technologies should also be developed, deployed and used with a view to supporting the achievement of environmental goals in line with the obligations laid down in applicable Union law, such as reducing waste production, diminishing the carbon footprint, combating climate change and preserving the environment, and their potential in that context should be maximised and explored through research and innovation projects. The Union and the Member States should therefore mobilise their communication, administrative and financial resources for the purpose of supporting and investing in such projects.
- (36) Projects relating to the potential of artificial intelligence, robotics and related technologies in addressing environmental concerns should be carried out on the basis of responsible research and innovation tools so as to guarantee from the outset the compliance of those projects with ethical principles.
- (37) Any artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced by such technologies, developed, deployed and used in the Union should fully respect Union citizens' rights to privacy and protection of personal data. In particular, their development, deployment and use should be in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council¹ and Directive 2002/58/EC of the European Parliament and of the Council².
- (38) In particular, the ethical boundaries of the use of artificial intelligence, robotics and

¹ 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) (OJ L 119, 4.5.2016, p. 1).

² Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

related technologies, including software, algorithms and data used or produced by such technologies, should be duly considered when using remote recognition technologies, such as recognition of biometric features, notably facial recognition, to automatically identify individuals. When these technologies are used by public authorities for reasons of substantial public interest, namely to guarantee the security of individuals and to address national emergencies, and not to guarantee the security of properties, the use should always be disclosed, proportionate, targeted and limited to specific objectives and restricted in time in accordance with Union law and having due regard to human dignity and autonomy and the fundamental rights set out in the Charter. Criteria for and limits to that use should be subject to judicial review and submitted to democratic scrutiny and debate involving civil society.

- (39) Governance that is based on relevant standards enhances safety and promotes the increase of citizens' trust in the development, deployment and use of artificial intelligence, robotics and related technologies including software, algorithms and data used or produced by such technologies.
- (40) Public authorities should conduct impact assessments regarding fundamental rights before deploying high-risk technologies which provide support for decisions that are taken in the public sector and that have a direct and significant impact on citizens' rights and obligations.
- (41) Among the existing relevant governance standards are, for example, the 'Ethics Guidelines for Trustworthy AI' drafted by the High-Level Expert Group on Artificial Intelligence set up by the European Commission, and any other technical standards such as those adopted by the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC), and the European Telecommunications Standards Institute (ETSI), at European level, the International Organization for Standardization (ISO) and the Institute of Electrical and Electronics Engineers (IEEE), at international level.
- (42) Sharing and use of data by multiple participants is sensitive and therefore the development, deployment and use of artificial intelligence, robotics and related technologies should be governed by relevant rules, standards and protocols reflecting the requirements of quality, integrity, security, reliability, privacy and control. The data governance strategy should focus on the processing, sharing of and access to such data, including its proper management, auditability and traceability, and guarantee the adequate protection of data belonging to vulnerable groups, including people with disabilities, patients, children, minorities and migrants or other groups at risk of exclusion. In addition, developers, deployers and users should be able, where relevant, to rely on key performance indicators in the assessment of the datasets they use for the purposes of enhancing the trustworthiness of the technologies they develop, deploy and use.

- (43) Member States should appoint an independent administrative authority to act as a supervisory authority. In particular, each national supervisory authority should be responsible for identifying artificial intelligence, robotics and related technologies considered as high-risk in the light of the risk assessment criteria provided for in this Regulation and for assessing and monitoring the compliance of these technologies with the obligations laid down in this Regulation.
- (44) Each national supervisory authority should also carry the responsibility of the good governance of these technologies under the coordination of the Commission and/or any relevant institutions, bodies, offices or agencies of the Union that may be designated for this purpose. They therefore have an important role to play in promoting the trust and safety of Union citizens, as well as in enabling a democratic, pluralistic and equitable society.
- (45) For the purposes of assessing technologies which are high-risk in accordance with this Regulation and monitoring their compliance with it, national supervisory authorities should, where applicable, cooperate with the authorities responsible for assessing and monitoring these technologies and enforcing their compliance with sectorial legislation.
- (46) National supervisory authorities should engage in substantial and regular cooperation with each other, as well as with the European Commission and other relevant institutions, bodies, offices and agencies of the Union, in order to guarantee a coherent cross-border action, and allow for consistent development, deployment and use of these technologies within the Union in compliance with the ethical principles and legal obligations laid down in this Regulation.
- (47) In the context of such cooperation and in view of achieving full harmonisation at Union level, national supervisory authorities should assist the Commission regarding drawing up a common and exhaustive list of high-risk artificial intelligence, robotics and related technologies in line with the criteria provided for in this Regulation and its Annex. Furthermore a granting process should be developed for the issuing of a European certificate of ethical compliance, including a voluntary application process for any developer, deployer or user of technologies not considered as high-risk seeking to certify their compliance with this Regulation.
- (48) National supervisory authorities should ensure the gathering of a maximum number of stakeholders such as industry, businesses, social partners, researchers, consumers and civil society organisations, and provide a pluralistic forum for reflection and exchange of views so as to achieve comprehensible and accurate conclusions for the purpose of guiding how governance is regulated.
- (49) National supervisory authorities should ensure the gathering of a maximum number of stakeholders such as industry, businesses, social partners, researchers, consumers

and civil society organisations, and provide a pluralistic forum for reflection and exchange of views, to facilitate cooperation with and collaboration between stakeholders, in particular from academia, research, industry, civil society and individual experts, so as to achieve comprehensible and accurate conclusions for the purpose of guiding how governance is regulated.

- (50) Additionally, these national supervisory authorities should provide professional administrative guidance and support to developers, deployers and users, particularly small and medium-sized enterprises or start-ups, encountering challenges as regards complying with the ethical principles and legal obligations laid down in this Regulation.
- (51) The Commission and/or any relevant institutions, bodies, offices and agencies of the Union that may be designated for this purpose should establish binding guidelines on the methodology to be used by the national supervisory authorities when conducting their compliance assessment.
- (52) Whistle-blowing brings potential and actual breaches of Union law to the attention of authorities with a view to preventing injury, harm or damage that would otherwise occur. In addition, reporting procedures ameliorate the information flow within companies and organisations, thus mitigating the risk of flawed or erroneous products or services being developed. Companies and organisations developing, deploying or using artificial intelligence, robotics and related technologies, including data used or produced by those technologies, should set up reporting channels and persons reporting breaches should be protected from retaliation.
- (53) The rapid development of artificial intelligence, robotics and related technologies, including the software, algorithms and data used or produced by such technologies, as well as of the technical machine learning, reasoning processes and other technologies underlying that development are unpredictable. As such, it is both appropriate and necessary to establish a review mechanism in accordance with which, in addition to its reporting on the application of the Regulation, the Commission is to regularly submit a report concerning the possible modification of the scope of application of this Regulation.
- (54) Since the objective of this Regulation, namely to establish a common regulatory framework of ethical principles and legal obligations for the development, deployment and use of artificial intelligence, robotics and related technologies in the Union, cannot be sufficiently achieved by the Member States, but can rather, by reason of its scale and effects, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is

necessary in order to achieve that objective.

- (55) Coordination at Union level as set out in this Regulation would be best achieved by the Commission and/or any relevant institutions, bodies, offices and agencies of the Union that may be designated in this context in order to avoid fragmentation and ensure the consistent application of this Regulation. The Commission should therefore be tasked with finding an appropriate solution to structure such coordination at Union level in view of coordinating the mandates and actions of the national supervisory authorities in each Member State, namely regarding the risk assessment of artificial intelligence, robotics and related technologies, the establishment of a common framework for the governance of the development, deployment and use of these technologies, the developing and issuing of a certification of compliance with the ethical principles and legal obligations laid down in this Regulation, supporting regular exchanges with concerned stakeholders and civil society and creating a centre of expertise, bringing together academia, research, industry, and individual experts at Union level to foster exchange of knowledge and technical expertise, and promoting the Union's approach through international cooperation and ensuring a consistent reply worldwide to the opportunities and risks inherent in these technologies.

HAVE ADOPTED THIS REGULATION:

Chapter I
General provisions

Article 1
Purpose

The purpose of this Regulation is to establish a comprehensive and future-proof Union regulatory framework of ethical principles and legal obligations for the development, deployment and use of artificial intelligence, robotics and related technologies in the Union.

Article 2
Scope

This Regulation applies to artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced by such technologies, developed, deployed or used in the Union.

Article 3
Geographical scope

This Regulation applies to artificial intelligence, robotics and related technologies where any part thereof is developed, deployed or used in the Union, regardless of whether the software, algorithms or data used or produced by such technologies are located outside of the Union or do not have a specific geographical location.

Article 4
Definitions

For the purposes of this Regulation, the following definitions apply:

- (a) ‘artificial intelligence’ means a system that is either software-based or embedded in hardware devices, and that displays intelligent behaviour by, inter alia, collecting, processing, analysing, and interpreting its environment, and by taking action, with some degree of autonomy, to achieve specific goals¹;
- (b) ‘autonomy’ means an AI-system that operates by interpreting certain input and using a set of pre-determined instructions, without being limited to such instructions, despite the system’s behaviour being constrained by and targeted at

¹ Definition as in the European Commission Communication COM(2018)0237, 25.04.2018, page 1, adapted.

fulfilling the goal it was given and other relevant design choices made by its developer;

- (c) ‘robotics’ means technologies that enable automatically controlled, reprogrammable, multi-purpose machines¹ to perform actions in the physical world traditionally performed or initiated by human beings, including by way of artificial intelligence or related technologies;
- (d) ‘related technologies’ means technologies that enable software to control with a partial or full degree of autonomy a physical or virtual process, technologies capable of detecting biometric, genetic or other data, and technologies that copy or otherwise make use of human traits;
- (e) ‘high risk’ means a significant risk entailed by the development, deployment and use of artificial intelligence, robotics and related technologies to cause injury or harm to individuals or society in breach of fundamental rights and safety rules as laid down in Union law, considering their specific use or purpose, the sector where they are developed, deployed or used and the severity of injury or harm that can be expected to occur;
- (f) ‘development’ means the construction and design of algorithms, the writing and design of software or the collection, storing and management of data for the purpose of creating or training artificial intelligence, robotics and related technologies or for the purpose of creating a new application for existing artificial intelligence, robotics and related technologies;
- (g) ‘developer’ means any natural or legal person who takes decisions that determine and control the course or manner of the development of artificial intelligence, robotics and related technologies;
- (h) ‘deployment’ means the operation and management of artificial intelligence, robotics and related technologies, as well as their placement on the market or otherwise making them available to users;
- (i) ‘deployer’ means any natural or legal person who is involved in the specific deployment of artificial intelligence, robotics and related technologies with a controlling or managing function by taking decisions, exercising control over the risk and benefiting from such deployment;
- (j) ‘use’ means any action relating to artificial intelligence, robotics and related technologies other than development or deployment;

¹ From the definition for industrial robots in ISO 8373.

- (k) ‘user’ means any natural or legal person who uses artificial intelligence, robotics and related technologies other than for the purposes of development or deployment;
- (l) ‘bias’ means any prejudiced personal or social perception of a person or group of persons on the basis of their personal traits;
- (m) ‘discrimination’ means any differential treatment of a person or group of persons based on a ground which has no objective or reasonable justification and is therefore prohibited by Union law;
- (n) ‘injury or harm’ means, including where caused by hate speech, bias, discrimination or stigmatisation, physical or mental injury, material or immaterial harm such as financial or economic loss, loss of employment or educational opportunity, undue restriction of freedom of choice or expression or loss of privacy, and any infringement of Union law that is detrimental to a person;
- (o) ‘good governance’ means the manner of ensuring that the appropriate and reasonable standards and protocols of behaviour are adopted and observed by developers, deployers and users, based on a formal set of rules, procedures and values, and which allows them to deal appropriately with ethical matters as or before they arise.

Article 5

Ethical principles of artificial intelligence, robotics and related technologies

1. Any artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced by such technologies, shall be developed, deployed and used in the Union in accordance with Union law and in full respect of human dignity, autonomy and safety and other fundamental rights set out in the Charter.
2. Any processing of personal data carried out in the development, deployment and use of artificial intelligence, robotics and related technologies, including personal data derived from non-personal data and biometric data, shall be carried out in accordance with Regulation (EU) 2016/679 and Directive 2002/58/EC.
3. The Union and its Member States shall encourage research projects intended to provide solutions, based on artificial intelligence, robotics and related technologies, that seek to promote social inclusion, democracy, plurality, solidarity, fairness, equality and cooperation.

Chapter II

Obligations for high-risk technologies

Article 6

Obligations for high-risk technologies

1. The provisions in this Chapter shall only apply to artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced by such technologies, developed, deployed or used in the Union which are considered high-risk.
2. Any high-risk artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced by such technologies, shall be developed, deployed and used in a manner that ensures that they do not breach the ethical principles set out in this Regulation.

Article 7

Human-centric and human-made artificial intelligence

1. Any artificial high-risk technologies, including software, algorithms and data used or produced by such technologies, shall be developed, deployed and used in a manner that guarantees full human oversight at any time.
2. The technologies referred to paragraph 1 shall be developed, deployed and used in a manner that allows full human control to be regained when needed, including through the altering or halting of those technologies.

Article 8

Safety, transparency and accountability

1. Any high-risk artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced by such technologies, shall be developed, deployed and used in a manner that ensures that they are:
 - (a) developed, deployed and used in a resilient manner so that they ensure an adequate level of security by adhering to minimum cybersecurity baselines proportionate to identified risk, and one that prevents any technical vulnerabilities from being exploited for malicious or unlawful purposes;
 - (b) developed, deployed and used in a secure manner that ensures there are safeguards that include a fall-back plan and action in case of a safety or security risk;
 - (c) developed, deployed and used in a manner that ensures a reliable performance as reasonably expected by the user regarding reaching the aims and carrying out the activities they have been conceived for, including by ensuring that all operations are reproducible;

- (d) developed, deployed and used in a manner that ensures that the performance of the aims and activities of the particular technologies is accurate; if occasional inaccuracies cannot be avoided, the system shall indicate, to the extent possible, the likeliness of errors and inaccuracies to deployers and users through appropriate means;
 - (e) developed, deployed and used in an easily explainable manner so as to ensure that there can be a review of the technical processes of the technologies;
 - (f) developed, deployed and used in a manner such that they inform users that they are interacting with artificial intelligence systems, duly and comprehensively disclosing their capabilities, accuracy and limitations to artificial intelligence developers, deployers and users;
 - (g) in accordance with Article 6, developed, deployed and used in a manner that makes it possible, in the event of non-compliance with the safety features set out in subparagraphs (a) to (g), for the functionalities concerned to be temporarily disabled and to revert to a previous state restoring safe functionalities.
2. In accordance with Article 6(1), the technologies mentioned in paragraph 1 of this Article, including software, algorithms and data used or produced by such technologies, shall be developed, deployed and used in transparent and traceable manner so that their elements, processes and phases are documented to the highest possible and applicable standards, and that it is possible for the national supervisory authorities referred to in Article 18 to assess the compliance of such technologies with the obligations laid down in this Regulation. In particular, the developer, deployer or user of those technologies shall be responsible for, and be able to demonstrate, compliance with the safety features set out in paragraph 1.
3. The developer, deployer or user of the technologies mentioned in paragraph 1 shall ensure that the measures taken to ensure compliance with the safety features set out in paragraph 1 can be audited by the national supervisory authorities referred to in Article 18 or, where applicable, other national or European sectorial supervisory bodies.

Article 9

Non-bias and non-discrimination

1. Any software, algorithm or data used or produced by high-risk artificial intelligence, robotics and related technologies developed, deployed or used in the Union shall be unbiased and, without prejudice to paragraph 2, shall not discriminate on grounds such as race, gender, sexual orientation, pregnancy, disability, physical or genetic

features, age, national minority, ethnicity or social origin, language, religion or belief, political views or civic participation, citizenship, civil or economic status, education, or criminal record.

2. By way of derogation from paragraph 1, and without prejudice to Union law governing unlawful discrimination, any differential treatment between persons or groups of persons may be justified only where there is an objective, reasonable and legitimate aim that is both proportionate and necessary insofar as no alternative exists which would cause less interference with the principle of equal treatment.

Article 10

Social responsibility and gender equality

Any high-risk artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced by such technologies, developed, deployed and used in the Union shall be developed, deployed and used in compliance with relevant Union law, principles and values, in a manner that does not interfere in elections or contribute to the dissemination of disinformation, respects worker's rights, promotes quality education and digital literacy, does not increase the gender gap by preventing equal opportunities for all and does not disrespect intellectual property rights and any limitations or exceptions thereto.

Article 11

Environmental sustainability

Any high-risk artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced by such technologies, shall be assessed as to their environmental sustainability by the national supervisory authorities referred to in Article 18 or, where applicable, other national or European sectorial supervisory bodies, ensuring that measures are put in place to mitigate and remedy their general impact as regards natural resources, energy consumption, waste production, the carbon footprint, climate change emergency and environmental degradation in order to ensure compliance with the applicable Union or national law, as well as any other international environmental commitments the Union has undertaken.

Article 12

Respect for privacy and protection of personal data

The use and gathering of biometric data for remote identification purposes in public areas, as biometric or facial recognition, carries specific risks for fundamental rights and shall be deployed or used only by Member States' public authorities for substantial public interest purposes. Those authorities shall ensure that such deployment or use is disclosed to the public, proportionate, targeted and limited to specific objectives and location and restricted in time, in accordance with Union and national law, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC, and with due regard for human dignity and autonomy and the

fundamental rights set out in the Charter, namely the rights to respect for privacy and protection of personal data.

Article 13

Right to redress

Any natural or legal person shall have the right to seek redress for injury or harm caused by the development, deployment and use of high-risk artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced by such technologies, in breach of Union law and the obligations set out in this Regulation

Article 14

Risk assessment

1. For the purposes of this Regulation, artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced by such technologies, shall be considered high-risk technologies when, following a risk assessment based on objective criteria such as their specific use or purpose, the sector where they are developed, deployed or used and the severity of the possible injury or harm caused, their development, deployment or use entail a significant risk to cause injury or harm that can be expected to occur to individuals or society in breach of fundamental rights and safety rules as laid down in Union law.
2. Without prejudice to applicable sectorial legislation, the risk assessment of artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced by such technologies, shall be carried out, in accordance with the objective criteria provided for in paragraph 1 of this Article and in the exhaustive and cumulative list set out in the Annex to this Regulation, by the national supervisory authorities referred to in Article 18 under the coordination of the Commission and/or any other relevant institutions, bodies, offices and agencies of the Union that may be designated for this purpose in the context of their cooperation.
3. In cooperation with the national supervisory authorities referred to in paragraph 2, the Commission shall, by means of delegated acts in accordance with Article 20, draw up and subsequently update a common list of high-risk technologies identified within the Union.
4. The Commission shall also, by means of delegated acts in accordance with Article 20, regularly update the list provided for in the Annex to this Regulation.

Article 15

Compliance assessment

1. High-risk artificial intelligence, robotics and related technologies shall be subject to an assessment of compliance with the obligations set out in Articles 6 to 12 of this Regulation, as well as to subsequent monitoring, both of which shall be carried out by

the national supervisory authorities referred to in Article 18 under the coordination of the Commission and/or any other relevant institutions, bodies, offices and agencies of the Union that may be designated for this purpose.

2. The software, algorithms and data used or produced by high-risk technologies which have been assessed as compliant with the obligations set out in this Regulation pursuant to paragraph 1 shall also be considered to comply with those obligations, unless the relevant national supervisory authority decides to conduct an assessment on its own initiative or at the request of the developer, the deployer or the user.
3. Without prejudice to sectorial legislation, the Commission and/or any relevant institutions, bodies, offices and agencies of the Union that may be specifically designated for this purpose shall prepare binding guidelines on the methodology to be used by the national supervisory authorities for the compliance assessment referred to in paragraph 1 by the date of the entry into force of this Regulation.

Article 16

European certificate of ethical compliance

1. Where there has been a positive assessment of compliance of high-risk artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced by such technologies, carried out in line with Article 15, the respective national supervisory authority shall issue a European certificate of ethical compliance.
2. Any developer, deployer or user of artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced by such technologies, that are not considered as high-risk and that are therefore not subject to the obligations laid down in Articles 6 to 12 and to the risk assessment and compliance assessment provided for in Articles 14 and 15, may also seek to certify the compliance with the obligations laid down in this Regulation, or part of them where so justified by the nature of the technology in question as decided by the national supervisory authorities. A certificate shall only be issued if an assessment of compliance has been carried out by the relevant national supervisory authority and that assessment is positive.
3. For the purposes of issuing the certificate referred to in paragraph 2, an application process shall be developed by the Commission and/or any other relevant institutions, bodies, offices and agencies of the Union that may be designated for this purpose.

Chapter III

Institutional oversight

Article 17

Governance standards and implementation guidance

1. Artificial intelligence, robotics and related technologies developed, deployed or used in the Union shall comply with relevant governance standards established in accordance with Union law, principles and values by the national supervisory authorities referred to in Article 18 in accordance with Union law, principles and values, under the coordination of the Commission and/or any relevant institutions, bodies, offices and agencies of the Union that may be designated for this purpose and in consultation with relevant stakeholders.
2. The standards referred to in paragraph 1 shall include non-binding implementation guidelines on the methodology for compliance with this Regulation by developers, deployers and users and shall be published by the date of entry into force of this Regulation.
3. Data used or produced by artificial intelligence, robotics and related technologies developed, deployed or used in the Union shall be managed by developers, deployers and users in accordance with relevant national, Union, other European organisations' and international rules and standards, as well as with relevant industry and business protocols. In particular, developers and deployers shall carry out, where feasible, quality checks of the external sources of data used by artificial intelligence, robotics and related technologies, and shall put oversight mechanisms in place regarding their collection, storage, processing and use.
4. Without prejudice to portability rights and rights of persons whose usage of artificial intelligence, robotics and related technologies has generated data, the collection, storage, processing, sharing of and access to data used or produced by artificial intelligence, robotics and related technologies developed, deployed or used in the Union shall comply with the relevant national, Union, other European organisations' and international rules and standards, as well as with relevant industry and business protocols. In particular, developers and deployers shall ensure those protocols are applied during the development and deployment of artificial intelligence, robotics and related technologies, by clearly defining the requirements for processing and granting access to data used or produced by these technologies, as well as the purpose, scope and addressees of the processing and the granting of access to such data, all of which shall at all times be auditable and traceable.

Article 18

Supervisory authorities

1. Each Member State shall designate an independent public authority to be responsible for monitoring the application of this Regulation ('supervisory authority'), and for

carrying out the risk and compliance assessments and the certification provided for in Articles 14, 15 and 16, without prejudice to sectorial legislation.

2. Each national supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities in each Member State shall cooperate with each other, the Commission and/or other relevant institutions, bodies, offices and agencies of the Union that may be designated for this purpose.
3. Each national supervisory authority shall serve as a first point of contact in cases of suspected breach of the ethical principles and legal obligations laid down in this Regulation, including discriminatory treatment or violation of other rights, as a result of the development, deployment or use of artificial intelligence, robotics and related technologies. In such cases, the respective national supervisory authority shall carry out a compliance assessment in view of supporting the right of citizens to contest and redress.
4. Each national supervisory authority shall be responsible for supervising the application of the relevant national, European and international governance rules and standards referred to in Article 17 to artificial intelligence, robotics and related technologies, including by liaising with the maximum possible number of relevant stakeholders. For that purpose, the supervisory authorities in each Member State shall provide a forum for regular exchange with and among stakeholders from academia, research, industry and civil society.
5. Each national supervisory authority shall provide professional and administrative guidance and support concerning the general implementation of Union law applicable to artificial intelligence, robotics and related technologies and the ethical principles set out in this Regulation, especially to relevant research and development organisations and small and medium-sized enterprises or start-ups.
6. Each Member State shall notify to the European Commission the legal provisions which it adopts pursuant to this Article by ... [OJ: please enter the date one year after entry into force] and, without delay, any subsequent amendment affecting them.
7. Member States shall take all measures necessary to ensure the implementation of the ethical principles and legal obligations laid down in this Regulation. Member States shall support relevant stakeholders and civil society, at both Union and national level, in their efforts to ensure a timely, ethical and well-informed response to the new opportunities and challenges, in particular those of a cross-border nature, arising from technological developments relating to artificial intelligence, robotics and related technologies.

Article 19

Reporting of breaches and protection of reporting persons

Directive (EU) 2019/1937 of the European Parliament and of the Council¹ shall apply to the reporting of breaches of this Regulation and the protection of persons reporting such breaches.

Article 20

Coordination at Union level

1. The Commission and/or any relevant institutions, bodies, offices and agencies of the Union that may be designated in this context shall have the following tasks:
 - ensuring a consistent risk assessment of artificial intelligence, robotics and related technologies referred to in Article 14 to be carried out by the national supervisory authorities referred to in Article 18 on the basis of the common objective criteria provided for in Article 8(1) and in the list of high-risk sectors and of high-risk uses or purposes set out in the Annex to this Regulation;
 - taking note of the compliance assessment and subsequent monitoring of high-risk artificial intelligence, robotics and related technologies referred to in Article 15 to be carried out by the national supervisory authorities referred to in Article 18;
 - developing the application process for the certificate referred to in Article 16 to be issued by the national supervisory authorities referred to in Article 18;
 - without prejudice to sectorial legislation, preparing the binding guidelines referred to in Article 17(4) on the methodology to be used by the national supervisory authorities referred to in Article 18;
 - coordinating the establishment of the relevant governance standards referred to in Article 17 by the national supervisory authorities referred to in Article 18, including non-binding implementation guidelines for developers, deployers and users on the methodology for compliance with this Regulation;
 - cooperating with the national supervisory authorities referred to in Article 18 regarding their contribution to the consistent application of this Regulation throughout the Union pursuant to Article 18(2);
 - serving as a centre for expertise by promoting the exchange of information related to artificial intelligence, robotics and related technologies and supporting the development of a common understanding in the Single Market, issuing additional guidance, opinions and expertise to the national supervisory authorities referred to in Article 18, monitoring the implementation of relevant Union law, identifying standards for best practice and, where appropriate, making recommendations for

¹ Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (OJ L 305, 26.11.2019, p. 17).

regulatory measures; in doing so, it should liaise with the maximum possible number of relevant stakeholders and ensure that the composition of its decision levels is diverse and ensures gender equality;

- hosting a Working Group on Security and Defence aimed at looking into policy and investment questions specifically related to the ethical use of artificial intelligence, robotics and related technologies in the field of security and defence.

Article 21

Exercise of delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The power to adopt delegated acts referred to in Article 14(3) and (4) shall be conferred on the Commission for a period of 5 years from (date of entry into force of this Regulation).
3. The delegation of power referred to in Article 14(3) and (4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or a later date specified therein. It shall not affect the validity of any delegated act already in force.
4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law Making.
5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
6. A delegated act adopted pursuant to Article 14(3) and (4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or, if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 22

Amendment to Directive (EU) 2019/1937

Directive (EU) 2019/1937 is amended as follows:

(1) In Article 2(1), the following point is added:

‘(xi) development, deployment and use of artificial intelligence, robotics and related technologies.’

(2) In Part I of the Annex, the following point is added:

‘K. Point (a)(xi) of Article 2(1) - development, deployment and use of artificial intelligence, robotics and related technologies.

“(xxi) Regulation [XXX] of the European Parliament and of the Council on ethical principles for the development, deployment and use artificial intelligence, robotics and related technologies”.’

Article 23

Review

The Commission shall keep under regular review the development of artificial intelligence, robotics and related technologies, including the software, algorithms and data used or produced by such technologies, and shall by ... [OJ: please enter the date three years after entry into force], and every three years thereafter, submit to the European Parliament, the Council and the European Economic and Social Committee a report on the application of this Regulation, including an assessment of the possible modification of the scope of application of this Regulation.

Article 24

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from XX.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at ...,

For the European Parliament

The President

For the Council

The President

ANNEX

Exhaustive and cumulative list of high-risk sectors and of high-risk uses or purposes that entail a risk of breach of fundamental rights and safety rules.

High-risk sectors	<ul style="list-style-type: none">• Employment• Education• Healthcare• Transport• Energy• Public sector (asylum, migration, border controls, judiciary and social security services)• Defence and security• Finance, banking, insurance
High-risk uses or purposes	<ul style="list-style-type: none">• Recruitment• Grading and assessment of students• Allocation of public funds• Granting loans• Trading, brokering, taxation, etc.• Medical treatments and procedures• Electoral processes and political campaigns• Public sector decisions that have a significant and direct impact on the rights and obligations of natural or legal persons• Automated driving• Traffic management• Autonomous military systems• Energy production and distribution• Waste management• Emissions control