European Parliament
2019-2024

TEXTS ADOPTED

P9_TA(2022)0140

Artificial intelligence in a digital age

European Parliament resolution of 3 May 2022 on artificial intelligence in a digital age (2020/2266(INI))

The European Parliament,

– having regard to Articles 4, 16, 26, 114, 169, 173, 179, 180, 181 and 187 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 the UN Convention on the Rights of the Child and General Comment No 25 of the UN Committee on the Rights of the Child of 2 March 2021 on children's rights in relation to the digital environment,

– having regard to the recommendation of the UN Educational, Scientific and Cultural Organization (UNESCO) on the ethics of artificial intelligence adopted by the UNESCO General Conference at its 41st session on 24 November 2021,

– having regard to the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[1] and the Commission's Better Regulation Guidelines,

– having regard to the Commission communication of 24 March 2021 on the EU strategy on the rights of the child (COM(2021)0142),

– having regard to its resolution of 7 October 2021 on the state of EU cyber defence capabilities[2],

– having regard to its resolution of 15 December 2021 on the challenges and prospects for multilateral weapons of mass destruction arms control and disarmament regimes[3],

– 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 – GDPR)[4],

---

1 OJ L 123, 12.5.2016, p. 1.
2 OJ C 132, 24.3.2022, p. 102.
3 Texts adopted, P9_TA(2021)0504.
4 OJ L 119, 4.5.2016, p. 1.

– having regard to Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240[1],

– having regard to Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013[2],

– having regard to the proposal for a regulation of the European Parliament and of the Council of 21 April 2021 laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206),

– having regard to the proposal for a regulation of the European Parliament and of the Council of 25 November 2020 on European data governance (Data Governance Act) (COM(2020)0767),

– having regard to Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union[3],

– having regard to Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092[4],

– having regard to Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services[5],

– having regard to Council Regulation (EU) 2021/1173 of 13 July 2021 on establishing the European High Performance Computing Joint Undertaking and repealing Regulation (EU) 2018/1488[6],

– having regard to the Commission communication of 25 April 2018 entitled ‘Artificial Intelligence for Europe’ (COM(2018)0237),

– having regard to the Commission communication of 7 December 2018 on a coordinated plan on artificial intelligence (COM(2018)0795),

– having regard to the Commission communication of 8 April 2019 on building trust in human-centric artificial intelligence (COM(2019)0168),

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

---

1 OJ L 166, 11.5.2021, p. 1.
2 OJ L 170, 12.5.2021, p. 1.
3 OJ L 303, 28.11.2018, p. 59.
4 OJ L 170, 12.5.2021, p. 149.
5 OJ L 136, 22.5.2019, p. 1.
6 OJ L 256, 19.7.2021, p. 3.

– having regard to the Commission Green Paper of 27 January 2021 on ageing – fostering solidarity and responsibility between generations (COM(2021)0050),

– having regard to the Commission communication of 19 February 2020 on a European strategy for data (COM(2020)0066),

– having regard to the Commission communication of 19 February 2020 on shaping Europe's digital future (COM(2020)0067),

– having regard to the Commission communications of 10 March 2020 on a new industrial strategy for Europe (COM(2020)0102) and of 5 May 2021 entitled 'Updating the 2020 New Industrial Strategy: Building a stronger Single Market for Europe's recovery' (COM(2021)0350),

– having regard to the Commission communication of 30 September 2020 entitled 'Digital Education Action Plan 2021-2027 – Resetting education and training for the digital age' (COM(2020)0624),

– having regard to the Commission communication of 9 March 2021 entitled '2030 Digital Compass: the European way for the Digital Decade' (COM(2021)0118),

– having regard to the proposal for a decision of the European Parliament and of the Council of 15 September 2021 establishing the 2030 Policy Programme 'Path to the Digital Decade' (COM(2021)0574),

– having regard to the Commission study of 28 July 2020 entitled 'European enterprise survey on the use of technologies based on artificial intelligence',

– having regard to the Commission study of 26 November 2020 entitled 'Energy-efficient cloud computing technologies and policies for an eco-friendly cloud market',

– having regard to the Commission report to the European Parliament, the Council and the European Economic and Social Committee of 19 February 2020 on the safety and liability implications of artificial intelligence, the internet of things and robotics (COM(2020)0064),

– having regard to the Council conclusions of 22 March 2021 on the EU's cybersecurity strategy for the digital decade,

– having regard to the report of the High-Level Expert Group on Artificial Intelligence of 8 April 2019 entitled 'Ethics guidelines for trustworthy AI',

– having regard to the report of the High-Level Expert Group on Artificial Intelligence of 8 April 2019 entitled 'A definition of AI: main capabilities and disciplines',

– having regard to the report of the High-Level Expert Group on Artificial Intelligence of 26 June 2019 entitled 'Policy and investment recommendations for trustworthy AI',

– having regard to the UNESCO publication of March 2019 entitled 'I'd blush if I could: closing gender divides in digital skills through education',

– having regard to the European Union Agency for Fundamental Rights report of 14 December 2020 entitled ‘Getting the future right – Artificial intelligence and fundamental rights’,

– having regard to the recommendation of the Council of the Organisation for Economic Co-operation and Development (OECD) of 22 May 2019 on artificial intelligence,

– having regard to the UN platform for dialogue on artificial intelligence: AI for Good Global Summit,

– having regard to the G20 AI Principles of 9 June 2019,

– having regard to the World Health Organization report of 28 June 2021 on artificial intelligence in health and six guiding principles for its design and use,

– having regard to the European Economic and Social Committee own-initiative opinion of 31 May 2017 entitled ‘Artificial Intelligence – The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society’[1],

– having regard to the report of the Expert Group on Liability and New Technologies – New Technologies Formation of 21 November 2019 entitled ‘Liability for Artificial Intelligence and other emerging digital technologies’,

– having regard to the publication of the Ad hoc Committee on Artificial Intelligence (CAHAI) of the Council of Europe of December 2020 entitled ‘Towards Regulation of AI systems – Global perspectives on the development of a legal framework on Artificial Intelligence systems based on the Council of Europe’s standards on human rights, democracy and the rule of law’,

– having regard to the European University Institute working paper of October 2020 entitled ‘Models of Law and Regulation for AI’,

– having regard to the joint report by Trend Micro Research, the UN Interregional Crime and Justice Research Institute and Europol of 19 November 2020 entitled ‘Malicious Uses and Abuses of Artificial Intelligence’,

– having regard to the Commission’s political guidelines for 2019-2024 entitled ‘A Union that strives for more: my agenda for Europe’,

– having regard to the judgment of the Court of Justice of the European Union of 16 July 2020 in case C-311/18 (*Schrems II*),

– having regard to its resolution of 16 February 2017 with recommendations to the Commission on civil law rules on robotics[2],

– having regard to its resolution of 1 June 2017 on digitising European industry[3],

---

1 OJ C 288, 31.8.2017, p. 1.
2 OJ C 252, 18.7.2018, p. 239.
3 OJ C 307, 30.8.2018, p. 163.

– having regard to its resolution of 6 October 2021 on the EU Road Safety Policy Framework 2021-2030 – Recommendations on next steps towards 'Vision Zero'[1],

– having regard to its resolution of 12 September 2018 on autonomous weapon systems[2],

– having regard to its resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics[3],

– having regard to its resolution of 12 February 2020 entitled 'Automated decision-making processes: ensuring consumer protection and free movement of goods and services'[4],

– having regard to its resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence[5],

– having regard to its resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies[6],

– having regard to its resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies[7],

– having regard to its resolution of 20 January 2021 on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice [8],

– having regard to its resolution of 20 May 2021 entitled 'Shaping the digital future of Europe: removing barriers to the functioning of the digital single market and improving the use of AI for European consumers'[9],

– having regard to its resolution of 25 March 2021 on a European strategy for data[10],

– having regard to its resolution of 19 May 2021 on artificial intelligence in education, culture and the audiovisual sector[11],

– having regard to its resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters[12],

---

1 OJ C 132, 24.3.2022, p. 45.
2 OJ C 433, 23.12.2019, p. 86.
3 OJ C 449, 23.12.2020, p. 37.
4 OJ C 294, 23.7.2021, p. 14.
5 OJ C 404, 6.10.2021, p. 107.
6 OJ C 404, 6.10.2021, p. 129.
7 OJ C 404, 6.10.2021, p. 63.
8 OJ C 456, 10.11.2021, p. 34.
9 OJ C 15, 12.1.2022, p. 204.
10 OJ C 494, 8.12.2021, p. 37.
11 OJ C 15, 12.1.2022, p. 28.
12 OJ C 132, 24.3.2022, p. 17.

– having regard to the study by its Directorate-General for Internal Policies (DG IPOL) of June 2021 entitled ‘Artificial Intelligence diplomacy – Artificial Intelligence governance as a new European Union external policy tool’,

– having regard to the DG IPOL study of May 2021 entitled ‘Challenges and limits of an open source approach to Artificial Intelligence’,

– having regard to the DG IPOL of May 2021 entitled ‘Artificial Intelligence market and capital flows – AI and the financial sector at crossroads’,

– having regard to the DG IPOL study of June 2021 entitled ‘Improving working conditions using Artificial Intelligence’,

– having regard to the DG IPOL study of May 2021 entitled ‘The role of Artificial Intelligence in the European Green Deal’,

– having regard to the DG IPOL study of July 2021 entitled ‘Artificial Intelligence in smart cities and urban mobility’,

– having regard to the DG IPOL study of July 2021 entitled ‘Artificial Intelligence and public services’,

– having regard to the DG IPOL study of July 2021 entitled ‘European Union data challenge’,

– having regard to the DG IPOL study of June 2020 entitled ‘Opportunities of Artificial Intelligence’,

– having regard to the DG IPOL study of October 2021 entitled ‘Europe’s Digital Decade and Autonomy’,

– having regard to the DG IPOL study of January 2022 entitled ‘Identification and assessment of existing and draft EU legislation in the digital field’,

– having regard to the European Parliament Research Service (EPRS) study of September 2020 entitled ‘Civil liability regime for artificial intelligence – European added value assessment’,

– having regard to the EPRS Scientific Foresight Unit study of December 2020 entitled ‘Data subjects, digital surveillance, AI and the future of work’,

– having regard to the EPRS study of September 2020 entitled ‘European framework on ethical aspects of artificial intelligence, robotics and related technologies’,

– having regard to the EPRS study of March 2020 entitled ‘The ethics of artificial intelligence: Issues and initiatives’,

– having regard to the EPRS study of June 2020 entitled ‘Artificial Intelligence: How does it work, why does it matter, and what can we do about it?’,

– having regard to the EPRS study of July 2020 entitled ‘Artificial Intelligence and Law enforcement – Impact on Fundamental Rights’,

– having regard to the EPRS study of June 2020 entitled ‘The impact of the General Data Protection Regulation (GDPR) on artificial intelligence’,

– having regard to the EPRS study of April 2020 entitled ‘The White Paper on Artificial Intelligence’,

– having regard to the EPRS study of September 2021 entitled ‘Regulating facial recognition in the EU’,

– having regard to the EPRS study of February 2021 entitled ‘The future of work: Trends, challenges and potential initiatives’,

– having regard to the EPRS study of June 2021 entitled ‘Robo-advisors: How do they fit in the existing EU regulatory framework, in particular with regard to investor protection?’,

– having regard to the EPRS study of September 2021 entitled ‘China’s ambitions in artificial intelligence’,

– having regard to the EPRS study of June 2021 entitled ‘What if we chose new metaphors for artificial intelligence?’,

– having regard to the EPRS study of January 2018 entitled ‘Understanding artificial intelligence’,

– having regard to the EPRS study of July 2021 entitled ‘Tackling deepfakes in European policy’,

– having regard to the working paper of the Special Committee on Artificial Intelligence in a Digital Age (AIDA) of February 2021 entitled ‘Artificial Intelligence and Health’,

– having regard to the AIDA working paper of March 2021 entitled ‘Artificial Intelligence and the Green Deal’,

– having regard to the AIDA working paper of March 2021 entitled ‘The External Policy Dimensions of AI’,

– having regard to the AIDA working paper of May 2021 entitled ‘AI and Competitiveness’,

– having regard to the AIDA working paper of June 2021 entitled ‘AI and the Future of Democracy’,

– having regard to the AIDA working paper of June 2021 on ‘AI and the Labour Market’,

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

– having regard to the report of the Special Committee on Artificial Intelligence in a Digital Age (A9-0088/2022),

1. Introduction

1. Notes that the world stands on the verge of the fourth industrial revolution; points out that in comparison with the three previous waves, initiated by the introduction of steam,

electricity, and then computers, the fourth wave draws its energy from an abundance of data combined with powerful algorithms and computing capacity; stresses that today's digital revolution is shaped by its global scale, fast convergence, and the enormous impact of emerging technological breakthroughs on states, economies, societies, international relations and the environment; recognises that radical change of this scale has differing impacts on various parts of society depending on their objectives, geographical location or socio-economic context; emphasises that the digital transition must be shaped with full respect for fundamental rights and in such a way that digital technologies serve humanity;

2. Observes that the digital revolution has, at the same time, triggered a global competition as a result of the tremendous economic value and technological capabilities that have accumulated in economies that commit the most resources to the research, development and marketing of artificial intelligence (AI) applications; notes that digital competitiveness and open strategic autonomy have become a central policy objective in several countries; stresses the growing realisation among decision makers that emerging technologies could affect the geopolitical power status of entire countries;

3. Points out that Europe, which for centuries set international standards, dominated technological progress and led in high-end manufacturing and deployment, has therefore fallen behind, developing and investing far less than leading economies like the US or China in the digital market, while remaining relatively competitive in AI thematic research output; recognises the risk of European actors being marginalised in the development of global standards and advancements of technology and of European values being challenged;

4. Highlights, firstly, that digital tools are increasingly becoming an instrument of manipulation and abuse in the hands of some corporate actors as well as in the hands of autocratic governments for the purpose of undermining democratic political systems, thus potentially leading to a clash between political systems; explains that digital espionage, sabotage, low-scale warfare and disinformation campaigns challenge democratic societies;

5. Stresses that the nature of digital business models allows for great degrees of scalability and network effects; points out that many digital markets are characterised by a high degree of market concentration, allowing a small number of tech platforms, most of which are currently US-based, to lead the commercialisation of groundbreaking technological innovations, attract the best ideas, talent and companies and achieve extraordinary profitability; warns that dominant market positions in the data economy are likely to be extended into the emerging AI economy; points out that only eight of today's top 200 digital companies are domiciled in the EU; stresses that the completion of a true digital single market is of the highest importance in that regard;

6. Emphasises that as a result, the global competition for tech leadership has become a priority in the EU; stresses that if the EU does not act swiftly and courageously, it will end up having to follow rules and standards set by others and risks damaging effects on political stability, social security, fundamental rights, individual liberties and economic competitiveness;

7. Argues that AI is one of the key emerging technologies within the fourth industrial revolution; notes that AI fuels the digital economy, as it allows for the introduction of innovative products and services, has the power to increase consumer choice and can

render production processes more efficient; states that by 2030, AI is expected to contribute more than EUR 11 trillion to the global economy; stresses, at the same time, that AI technologies risk reducing human agency; highlights that AI should remain a human-centric, trustworthy technology and should not substitute human autonomy nor assume the loss of individual freedom; stresses the need to ensure that this fourth industrial revolution is inclusive and leaves no one behind;

8. Suggests that there is a global contest for AI leadership; points out that AI technologies promise to deliver immense economic value to those economies which profitably develop, produce and adopt such technologies, as well as to those countries in which such value creation takes place; underlines that AI is not an omnipotent technology, but an efficient set of tools and techniques that can be put to the benefit of society; explains that how technologies function depends on how we design them; points out that the EU has declared its intention to pioneer a regulatory framework on AI; stresses, nonetheless, that it is crucial for the EU to be able to define the regulatory approach, including the protection of fundamental rights and freedoms, and to act as a global standard-setter; stresses, therefore, the importance of European competitiveness in AI and the ability of the EU to shape the regulatory landscape at international level; stresses that certain uses of AI may pose individual and societal risks that can endanger fundamental rights and should therefore be addressed by policymakers, thereby allowing AI to effectively become an instrument that serves people and society, pursuing the common good and general interest;

9. Notes that a clear regulatory framework, political commitment and a more forward-leaning mindset, which are often lacking at present, are needed for European actors to be successful in the digital age and to become technology leaders in AI; concludes that based on such an approach, both EU citizens and businesses can benefit from AI and the great opportunity it offers to boost competitiveness, including with regard to prosperity and well-being; underlines that regulatory frameworks must be shaped in such a way as not to impose unjustified barriers to prevent European actors from being successful in the digital age, in particular for start-ups and small and medium-sized enterprises (SMEs); highlights that private and public investments should be substantially increased to create a climate in which more European success stories emerge and develop on our continent;

10. Highlights that rapid technological progress introduced by AI is increasingly inextricable from most areas of human activity and will also affect the livelihoods of everyone who does not possess the skills they need to adapt fast enough to these new technologies; points out that while achieving digital literacy through upskilling and reskilling can help to address many of the resulting socio-economic concerns, these impacts should also be addressed in the context of social welfare systems, urban and rural infrastructure, and democratic processes;

11. Emphasises the need to reflect the objectives and interests of women and vulnerable groups in the digital transition; highlights, in this context, that women only accounted for 22 % of global AI professionals in 2018, a problem that serves only to perpetuate and entrench stereotypes and bias; recognises the need to preserve the rights to equality before the law, privacy, freedom of expression, and participation in cultural and political life when using AI technologies, especially for minority communities;

2. Potential opportunities, risks and obstacles in the use of AI: six case studies examined by the AIDA Committee

12. Recalls that AI is based on software that uses probabilistic models and algorithmic prediction for a set of specific objectives; points out that the term AI is an umbrella term covering a wide range of old and new technologies, techniques and approaches better understood as 'artificial intelligence systems', which refers to any machine-based systems that often have little more in common than being guided by a given set of human-defined objectives, with varying degrees of autonomy in their actions, and engaging in predictions, recommendations or decision-making based on available data; notes that while some of these technologies are already in widespread use, others are still under development or are even just speculative concepts that may or may not exist in the future;

13. Points out that there is a significant difference between symbolic AI, the main approach to AI from the 1950s to the 1990s, and machine-learning, data-driven AI, which has dominated since the 2000s; clarifies that during the first wave, AI was developed by encoding the knowledge and experience of experts into a set of rules that was then executed by a machine;

14. Notes that in the second wave, the automated learning processes of algorithms based on the processing of large amounts of data, the ability to bring together inputs from multiple different sources and form complex representations of a given environment, and the identification of patterns made AI systems more complex, autonomous and opaque, which can lead to less explainable outcomes; stresses that current AI can therefore be broken down into many different sub-domains and techniques, whereby deep learning is for instance a subfield of machine learning, which itself is a subfield of AI;

15. Notes that although today's AI has become much more effective and powerful than symbolic AI, thanks to the significant increases in computing capacities, it can still only solve clearly defined tasks in domain-specific niches such as chess or image recognition and its programming is not designed to fully recognise the actions that the AI system performs; highlights that AI systems – contrary to what their name suggests – do not have 'intelligence' in a human sense; points out that it is therefore referred to as 'narrow' or 'weak' AI and is still no more than a tool that provides recommendations and predictions; notes, for instance, that self-driving cars operate through a combination of various one-task AI systems that together are able to provide a three-dimensional map of the surroundings of the vehicle so that its operating system can make decisions;

16. Highlights that many fears linked to AI are based on hypothetical concepts such as general AI, artificial superintelligence and singularity which could, in theory, lead to machine intelligence outperforming human intelligence in many areas; stresses that there are doubts as to whether this speculative AI can even be achieved with our technologies and scientific laws; believes, nevertheless, that the risks currently posed by AI-based decision-making need to be addressed by the legislators as it is demonstrably clear that harmful effects such as racial and sex discrimination are already attributable to particular instances where AI has been deployed without safeguards;

17. Underlines that the majority of AI systems currently in use are low-risk; refers, for instance, to automatic translation, 'Eureka machines', gaming machines and robots that carry out repetitive manufacturing processes; concludes that some use cases can be categorised as risky and that such cases require regulatory action and effective safeguards, should these not already be in place;

18. Encourages a public debate on how to explore the enormous potential of AI based on fundamental European values, the principles of transparency, explainability, fairness, accountability, responsibility and trustworthiness, as well as the principle that AI and robotics should be human-centred and developed to complement humans; stresses that in a significant number of areas of human life, from sustainability to healthcare, AI can provide benefits as an auxiliary tool for users and professionals, augmenting the capabilities of humans without impeding their ability to freely act and decide; stresses that the agreed AI ethical principles and requirements should be operationalised in all domains of AI application, building in the necessary safeguards, which will increase citizens' trust, thereby making them embrace the benefits of AI;

19. Underlines that the level of risk of a particular AI application varies significantly depending on the likelihood and severity of harm; highlights, therefore, that legal requirements should be adjusted to this, in line with a risk-based approach and taking into due account, when justified, the precautionary principle; stresses that in such present or future instances where, in a particular use case, AI systems pose high risks to fundamental and human rights, full human oversight and regulatory intervention are needed and that, given the speed of technological development, regulation for high-risk AI systems needs to be flexible and future-proof;

20. Illustrates that the present report addresses six AI case studies in detail, outlining the opportunities offered by AI in the respective sector, the risks to be addressed and the obstacles preventing Europe from fully harnessing the benefits of AI; highlights that the case studies represent some of the most important AI use cases today and, at the same time, reflect some of the main topics of the public hearings held by the AIDA Committee during its mandate, namely health, the Green Deal, external policy and security, competitiveness, the future of democracy and the labour market;

a) AI and health

21. Finds that the methodological analysis of large amounts of data, including through AI, can unlock new solutions or improve existing techniques in the health sector that could speed up scientific research enormously, save human lives and improve patient care by offering innovative treatments and better diagnosis and fostering supportive environments for healthy lifestyles; highlights that AI systems can also contribute to the accessibility, resilience and sustainability of health systems, while at the same time bringing a competitive edge to the European ICT and healthcare sectors if the inherent risks are managed appropriately;

22. Highlights that the use of AI in the health sector should be anchored in strong ethical requirements such as equitable access to healthcare, privacy, liability, transparency, explainability, reliability, inclusiveness and representability of data sets, and constant human oversight; stresses that the design of AI-based systems must address the risk of resources being wrongly allocated to individuals based on faulty or biased categorisation, prioritisation or malfunctioning technology, leading to misdiagnosis, maltreatment or no treatment at all; believes that the highest ethical standards should apply to all healthcare applications and that ethical rules should be established at a very early stage in their development and design, i.e. ethics by design; underlines that automated decision-making in healthcare applications may pose risks to patients' well-being and fundamental rights and stresses that AI must therefore have a supportive role in healthcare, where professional human oversight should always be maintained; calls for AI in medical diagnoses in public health systems to preserve the patient-doctor

relationship and to be consistent with the Hippocratic oath at all times; notes, however, that AI improves the accuracy of screening and is already outperforming doctors' diagnoses in several instances; finds that the existing liability frameworks do not provide sufficient legal certainty and do not uphold the right of patients to legal redress in the event of misdiagnosis and incorrect treatment through AI; welcomes, in this regard, the upcoming legislative proposal on AI liability; notes that it is important to protect health professionals as users of AI systems, as well as patients as end recipients, providing them with sufficient and transparent information;

23. Underlines that AI-based solutions are already being used or tested in clinical settings with the aim of supporting diagnosis, prognosis, treatment and patient engagement, thus speeding up and improving treatment and reducing unnecessary interventions; notes, moreover, that AI can enhance personalised medicine and patient care; notes that AI is currently covering a wide range of health areas, including public health, care services, self-care and health systems; remarks that data plays an important role; finds that there are promising applications for AI in extracting information from images and in other medical devices to inform downstream analysis and notes that it is also expected that deep learning algorithms can deliver a quantitative leap in a variety of clinical tasks;

24. Highlights that AI technologies can be applied to the research, development and mass production of pharmaceuticals and have the potential to speed up the development of new drugs, treatments and vaccines at a lower cost; finds that AI can help predict the outcome of responses to treatments and can allow doctors to adjust therapeutic strategies according to individual genetic or physiological characteristics with increasing levels of accuracy when based on high-quality data and sound assumptions, thereby increasing the effectiveness of preventive care, provided that all ethical requirements are met with regard to professional oversight over AI clinical validation, privacy, data protection and informed consent; notes that big data in health can be analysed with the aid of AI to accelerate its processing; underlines the importance of ensuring that high-performance computing is interoperable with AI, as major economic sectors including manufacturing, health and pharmaceuticals rely on high-performance computing;

25. Underlines that AI-based solutions have the potential to tailor treatments and drug development to patients' specific needs and enhance engagement with stakeholders and participants in the healthcare system; finds that AI and access to relevant, updated and high-quality anonymised and representative data sets, in line with the EU rules on personal data protection, supports healthcare professionals to help them provide better care for their patients and more personalised feedback, guidance and support, promoting patient safety and making therapy more effective; highlights that this may be particularly helpful in selecting and reviewing the growing body of scientific knowledge for the purposes of extracting relevant insights for health professionals; highlights that citizens from all Member States should be able to share their health data with healthcare providers and authorities of their choice; underlines, in this regard, the need to create incentives for upskilling, reskilling and outskilling for workers in health careers;

26. Finds that the fight against COVID-19 has both accelerated research into and the deployment of new technologies, notably AI applications, in the quest for improved case detection, clinical care and therapeutics research, and highlighted the usefulness of AI as well as the importance of funding and high-quality data for the purpose of the efficient monitoring and modelling of the spread of infectious disease outbreaks, in accordance with data protection law; notes, however, that experiences with AI

applications during COVID-19 have revealed some of the limitations in the use of AI in medical diagnostics[1];

27. Highlights the potential of AI systems to alleviate the burden on health systems and health professionals in particular and to contribute to solutions to provide care to rapidly ageing populations in Europe and the world and protect them from dangerous diseases;

28. Highlights that the use of safe and efficient AI applications for administrative tasks that do not require human action can save a lot of time for healthcare workers that can be devoted to patient visits instead;

29. Stresses that consumer health applications based on AI can help track an individual's health status through everyday devices such as smartphones, allowing users to voluntarily provide data which can be the basis for early warnings and alerts regarding life-threatening illnesses such as strokes or cardiac arrests; stresses that health applications based on AI may also encourage healthy behaviour and empower responsible self-care for individuals by equipping patients with additional means to monitor their own health and lifestyle and by improving the accuracy of screening by healthcare professionals; points out, however, the particular sensitivity of personal health data and the risk of data breaches or misuses in this regard, and underlines the need to apply strong cybersecurity standards for any health application;

30. Stresses that AI in the health sector is particularly dependent on large amounts of personal data, data sharing, high data quality, data accessibility and data interoperability to realise the full potential of AI and health; stresses the need to facilitate the linking of electronic health records with e-prescribing systems in order to allow health professionals involved in patient care to access the necessary information on the patient, subject to his or her consent;

31. Welcomes the creation of a European health data space in order to build in data of very high quality for use in the health sector; considers that the interconnection and interoperability of high-performance computing infrastructure with the European health data space would ensure the availability of large, high-quality health data sets, which are important for researching and treating pathologies, especially rare diseases and paediatric conditions;

32. Stresses the need to build trust by promoting interoperability and more collaboration between different healthcare professionals serving the same patients; stresses the need to offer training to healthcare professionals on AI techniques and approaches; stresses the need to combat mistrust, such as by tapping into the full potential of data anonymisation and pseudonymisation, and to better inform citizens, health professionals and decision makers about the uses, benefits and risks of AI in the field of health, as well as AI developers about the challenges and risks of processing sensitive data in this domain;

33. Believes, moreover, that binding and robust ethical and legal standards and enforceable rights of redress are necessary to promote an ecosystem of trust among citizens and to

---

1 Roberts, M., Driggs, D., Thorpe, M. et al., 'Common pitfalls and recommendations for using machine learning to detect and prognosticate for COVID-19 using chest radiographs and CT scans', *Nature Machine Intelligence*, 3, pp. 199-217, 15 March 2021.

adequately protect health data from potential misuse and unlawful access; agrees with the Commission that citizens should have secure access to a comprehensive electronic record of data concerning their health and should retain control over personal data concerning their health and be able to share it securely, with effective protection for personal data and strong cybersecurity, with authorised third parties; highlights that unauthorised access and dissemination should be prohibited and that the protection of patients' personal data must be guaranteed in compliance with data protection legislation;

34. Underlines, in this regard, the risk of biased decisions leading to discrimination and violations of human rights; stresses the need, therefore, for impartial checks on the algorithms and data sets used, and for the promotion of further research on the methods and bias embedded in trained AI systems in order to prevent unethical and discriminatory conclusions in the field of human health data;

35. Stresses that an efficient and uniform application of the GDPR across the EU is needed in order to overcome challenges such as legal uncertainty and a lack of cooperation in the health sector; stresses that such challenges lead in some cases to delays in scientific discoveries and a bureaucratic burden in health research; stresses that the creation of a European health data space that guarantees patients' rights and data portability could increase cooperation and stimulate data sharing for research and innovation in the European health sector;

36. Notes that AI can contribute to the rapid progress of new technologies, such as brain imaging, which already have important applications in medicine but also entail substantial risks to human agency and the expression of fundamental rights without requiring consent; is concerned about the lack of legislation concerning neurological data and believes that the EU should strive to become a world leader in the development of safe neurological technologies;

b) AI and the Green Deal

37. Highlights that the Commission's two key priorities for the years to come are a Europe fit for the digital age and the Green Deal; underlines the need to ensure that the digital transition contributes to the achievement of sustainable development and promotes the green transition; finds that this requires an acceleration of innovation compatible with the EU's climate targets and environmental standards; highlights that AI applications may be able to bring environmental and economic benefits and strengthen predictive capabilities that can contribute to the fight against climate change and to achieving the objectives of the European Green Deal and the EU's target of becoming the first climate-neutral continent by 2050; finds that the use of AI has the potential to reduce global greenhouse gas emissions by up to 4 % by 2030[1]; finds that according to some estimates, ICT technologies may reduce 10 times more greenhouse gas emissions than their own footprint[2], but recognises that this requires conscious design choices and regulatory action; warns, at the same time, that the increasing energy consumption in storing the large data sets needed to train AI systems can also have a negative effect; recalls that data traffic and ICT infrastructure consume about 7 % of the world's electricity today, a figure which, without the right safeguards, is projected to increase to 13 % by 2030; adds that the intensive use of raw materials to build microprocessors and

---

1 DG IPOL study, *Opportunities of Artificial Intelligence,* June 2020.

2 AIDA working paper, *Artificial Intelligence and the Green Deal*, March 2021.

high-tech devices using AI can also contribute to this negative impact; underlines that in order to guarantee the 'large handprint but small footprint' of AI on the environment and climate, these direct and indirect negative environmental impacts need to be considered and AI systems need to be designed to promote sustainable consumption, limit resource usage and energy consumption, avoid unnecessary processing operations and prevent damage to the environment; emphasises that addressing the environmental impact of the ICT sector requires relevant information and data;

38. Is concerned that only six Member States have included a strong focus on AI applications in their efforts to meet the Green Deal objectives; finds that AI can be used to collect and organise information relevant to environmental planning, decision-making and the management and monitoring of the progress of environmental policies, for instance for cleaner air, where AI applications can monitor pollution and warn of hazards; highlights that such AI and digital solutions could be used across several sectors to scale up resource-efficient solutions;

39. Emphasises the importance of AI-based systems in developing smart cities and villages by optimising resource use and increasing the resilience of infrastructure, including through traffic prediction and reduction, smart energy management, emergency assistance and waste, as is already the case in several cities and municipalities across the EU; stresses that AI-based solutions can further assist in urban planning, architecture, construction and engineering processes to reduce emissions, construction time, costs and waste;

40. Stresses that the energy transition will not take place without digitalisation; highlights that AI can monitor, optimise and reduce energy consumption and production, as well as support the integration of renewable energies into existing electricity grids; underlines that smart meters, efficient lighting, cloud computing and distributed software together with an AI component have the potential to transform energy use patterns and promote responsible usage;

41. Highlights that the growing complexity of an energy transition system, with increased volatile renewable generation and changes in load management, makes increasing automated control necessary for energy supply security; stresses that AI has the potential to benefit security of supply, especially in the operation, monitoring, maintenance and control of water, gas and electricity networks; notes, however, that AI-enhanced grid technologies will introduce millions of intelligent components with common vulnerabilities, adding a large number of potential attack points to the energy networks and increasing the vulnerabilities of critical infrastructure, if the appropriate cybersecurity provisions are not in place; finds that smart grids require further investment and research;

42. Finds that AI and other digital applications for mobility and transport have the potential to optimise traffic flows and enhance road safety, including by increasing the efficiency of transport systems; points out that AI can inform the design and energy management of energy-efficient vehicles; highlights that the options for app-based ride services, ride pooling and car sharing have considerably increased and that AI is often used in such mobility services through efficient route planning and pick-up point selection;

43. Believes that AI can have a transformative role in the agricultural sector, supporting the emergence of new harvesting methods, including harvest prediction and agricultural resource management; stresses that agriculture is a key sector in which AI can help cut

emissions and the use of pesticides, fertilisers, chemicals and water by focusing their use on the exact amount and in a narrower area; further stresses that AI can contribute to the restoration of biodiversity by monitoring endangered species or tracking deforestation activities; highlights the need to develop deployment guidelines and standardised assessment methodologies to support 'green AI' in areas such as smart grids, precision farming, and smart and sustainable cities as well as communities; is of the opinion that AI in the form of precision farming has the potential to optimise the on-farm production of food as well as broader land management by improving land use planning, predicting land use change and monitoring crop health, as well as the potential to transform predictions of extreme weather events;

44. Stresses that AI can contribute to the circular economy by rendering production, consumption and recycling processes and behaviour more resource-efficient and increasing the transparency of material use, for example with regard to the ethical sourcing of raw materials and reduced waste; highlights that AI has the potential to increase businesses' understanding of their emissions, including in value chains, thus helping them to adjust and achieve individual emissions targets; underlines that digital tools can help businesses to implement the necessary steps towards more sustainable conduct, especially SMEs which otherwise may not have the resources to do so;

45. Highlights that it is not currently possible to use AI to fully measure environmental impacts; finds that there is a need for more studies on the role of AI in reducing environmental impacts; stresses that more environmental data is needed in order to gain more insight and induce more progress through AI solutions; underlines that using AI to systematically connect data on CO_2 emissions with data on production and consumption patterns, supply chains and logistics routes could ensure that activities that have a positive or negative impact are detected;

c) External policy and the security dimension of AI

46. Reiterates that the EU is pushing for a global agreement on common standards for the responsible use of AI, which is of paramount importance; believes, as a matter of principle however, in the potential of like-minded democracies to work together to jointly shape the international debate on an AI framework that is respectful of human rights and the rule of law, to work together towards certain common norms and principles, technical and ethical standards, and guidelines for responsible state behaviour, especially under the umbrella of intergovernmental organisations such as the UN and OECD, thereby promoting multilateralism, sustainable development, interoperability and data sharing on the international stage; supports the work of the UN Open-Ended Working Group on ICT and international security; underlines that confidence-building measures are essential to increase the level of dialogue and trust; calls, therefore, for more transparency in the use of AI in order to ensure better accountability;

47. Welcomes the recent multilateral initiatives to develop guidelines and standards for an ethically responsible use of AI such as the OECD principles on AI, the Global Partnership on AI, the UNESCO recommendation on the ethics of AI, the AI for Good Global Summit, the Council of Europe's recommendations for a possible legal framework on AI, and UNICEF's policy guidance on AI for children; welcomes the work ongoing at international level on AI standards and the progress made with the International Organization for Standardization standards on the governance implications of AI;

48. Welcomes, furthermore, the establishment and operationalisation of the EU-US Trade and Technology Council (TTC); salutes the outcome of the TTC's first meeting in Pittsburgh; sees the TTC as a potential forum for global coordination between the European Union and the United States for setting global rules for AI and global technological standards that safeguard our common values, for boosting joint investment, research and development, and for closer political coordination in international institutions on issues related to technology and AI;

49. Highlights the key role the EU can play in setting global standards, as the first bloc in the world to introduce legislation on AI; stresses that the Union's legal framework on AI could make Europe a world leader in the sector and should therefore be promoted worldwide by cooperating with all international partners while continuing the critical and ethics-based dialogue with third countries that have alternative governance models and standards on AI;

50. Observes that the Chinese Government has signed standards and cooperation agreements with 52 countries through its Belt and Road Initiative; warns that since several of these standards, including on AI technologies and in particular in relation to government surveillance and individual liberties, are not in line with human rights and EU values, China's standards activism poses a challenge for the EU;

51. Stresses that AI technologies, especially those that have not been designed and developed with the explicit control procedures in place and are used improperly and without oversight in military command centres or in missile launch facilities, entail particularly significant risks and could escalate an automated reciprocal conflict;

52. Notes that the use of AI systems in defence-related developments is considered a game changer in military operations through the analysis of data, the ability to reflect greater situational complexity, the potential to improve target accuracy, optimise logistics and engage in armed conflicts with a reduced risk of physical harm to civilian populations and one's own military personnel, as well as using data for the development of modes of action such as wargaming; cautions, however, that this could lead to a lower threshold for the use of force and therefore more conflicts; affirms that machines cannot make human-like decisions involving the legal principles of distinction, proportionality and precaution; affirms that humans should be kept in control of the decision to deploy and use weapons and remain accountable for the use of lethal force and for decisions over life and death; is of the opinion that AI-based weapons systems should be subject to global standards and an international ethical code of conduct to underpin the deployment of AI technologies in military operations, with full respect for international humanitarian law and human rights law and in compliance with Union law and values;

53. Is concerned about the military research and technological developments being pursued in some countries with regard to lethal autonomous weapons systems without meaningful human control; observes that lethal autonomous weapons systems are already used in military conflicts; recalls that Parliament has repeatedly called for an international ban on the development, production and use of lethal autonomous weapons systems and for effective negotiations to begin on their prohibition; stresses that AI-enabled systems can under no circumstances be allowed to replace human decision-making involving the legal principles of distinction, proportionality and precaution;

54. Notes, in particular, that AI technology may entail potential risks as a means of pursuing various forms of hybrid warfare and foreign interference; specifies that it could for instance be mobilised to trigger disinformation, by using bots or fake social media accounts, to weaponise interdependence, by gathering valuable information or denying network access to adversaries, to create disturbances in the economic and financial systems of other countries, to pollute the political debate and favour extremist groups, or to manipulate elections to destabilise democracies;

55. Highlights that AI technologies could also include AI-powered malware, identity theft, data poisoning or other forms of adversarial machine learning that cause other AI systems to misinterpret input; points, in particular, to the rise in deepfakes, which are not necessarily cyberattacks but lead to doubts over the authenticity of all digital content, including videos, and therefore require particular attention in terms of transparency requirements; warns that deepfakes could contribute to a broad climate of public mistrust in AI, as well as a deeper socio-political polarisation within our societies;

56. Elaborates that the use of AI systems in a significant amount of key critical infrastructure such as energy and transport grids, the space sector, the food chain, banking and financial infrastructure, and hospital facilities has created new vulnerabilities that require robust cybersecurity measures to prevent threats; points out, in this regard, the importance of cooperation and information sharing and action both at EU level as well as among Member States; underlines the importance of fostering the resilience of critical entities to hybrid threats;

57. Warns that the capabilities of AI may also pose security risks, as they may lead humans to place such confidence in AI that they trust it more than their own judgement; notes that using a human-in-the-loop approach as a corrective mechanism is not feasible in all cases; notes that experiments have shown that this can elevate the level of autonomy of AI beyond the supporting role for which it was originally designed and means that humans miss opportunities to gain experience and refine their skills and knowledge of AI systems; stresses, therefore, that safety by design and meaningful human oversight based on appropriate training as well as appropriate security and privacy safeguards are required in high-risk AI systems in order to overcome such automation bias;

58. Highlights, however, that AI can be used to predict power failures and identify maintenance needs with great accuracy; specifies, in addition, that it can be used to synthesise large amounts of data via automated information extraction or automated information classification, and to detect specific patterns; stresses that these elements would allow for better prediction and assessment of the threat level and system vulnerabilities, faster decision-making processes, improved reactivity and securing endpoint devices more effectively;

59. Underlines, in particular, the inherent potential in enabling law enforcement agencies to identify and counter criminal activity, which is aided by AI technology; underlines that such AI-related law enforcement activities do, however, require full respect for fundamental rights, strict democratic oversight, clear transparency rules, a powerful IT infrastructure, human oversight, highly skilled employees and access to relevant and high-quality data;

d) AI and competitiveness

60. Notes that more and more products and services along the value chain will be interconnected in the near future, with AI and automation playing an important role in many manufacturing processes, operations and business models; underlines the paramount importance of basic research for the development of AI industrial ecosystems as well as substantial investment to promote digital public administration and upgrade digital infrastructure;

61. Observes that despite the significant increase in venture capital and other early-stage funding in the last two years, many European industries are lagging behind and the current funding levels in the EU are still insufficient and should be substantially ramped up in order to match the dynamism of leading AI ecosystems like Silicon Valley and elsewhere; highlights the peculiar cluster-network structure of the EU innovation ecosystem, as opposed to centralised (and state-supported) innovation ecosystems;

62. Underlines that AI can be a game changer for the competitiveness of EU industry and has the potential to increase productivity, accelerate innovation, improve manufacturing processes and help to monitor the resilience of European supply chains;

63. Points to the risk of supply chains being disrupted due to economic decoupling or catastrophic events such as pandemics or climate change-related phenomena; stresses that using AI can help to detect patterns of disruption in supply chains and inform predictive maintenance, which could support the diversification of suppliers;

64. Notes that companies that have initiated digital disruption have often been rewarded with significant gains in market share; notes that recent studies indicate that this pattern is likely to repeat itself with even more intensity as companies that adopt AI often collect large amounts of data, which tends to enhance their competitive position; is concerned about the resulting risks of market concentration to the detriment of SMEs and start-ups;

65. Emphasises that this outlook is particularly concerning since the largest incumbent tech companies that will likely also dominate AI technologies are gatekeepers to markets, while capturing most of the value that is generated; stresses that because the data that drives the AI sector is overwhelmingly collected from the very same large tech companies, which offer users access to services in exchange for data and exposure to targeted advertisements, their existing market dominance is likely to, in itself, become a driver of further market dominance; points out that many of these tech companies are headquartered outside the EU yet manage to capture the value generated by data on European customers, thus gaining a competitive advantage;

66. Welcomes the recent Commission communication calling for competition rules to be updated to make them fit for the digital age[1] and stresses the key role of *ex ante* measures, including the future Digital Markets Act, in counterbalancing concentration before it arises; underlines, moreover, the role that standardisation and regulatory cooperation can play in addressing this issue, by facilitating the global development of products and services irrespective of their physical location;

67. Underlines that SMEs and start-ups are playing a central role in the introduction of AI technologies within the EU as they represent the bulk of all companies and are a critical

---

[1] Commission communication of 18 November 2021 on a competition policy fit for new challenges (COM(2021)0713).

source of innovation; observes, however, that promising AI start-ups face significant barriers to expanding across Europe due to the incomplete digital single market and regulatory divergence in many Member States, or, when they do scale up, are acquired by large tech companies; regrets that SMEs often face a lack of funding, complex administrative procedures and a lack of adequate skills and access to information; notes that EU competition authorities have in the past allowed most foreign takeovers of European AI and robotics companies;

68. Stresses that the intensive use of algorithms, e.g. for price-setting, could also create completely new AI-specific problems within the single market; notes that antitrust authorities might, for instance, find it difficult to prove price collusion between AI-driven price-setting systems; adds, moreover, that the few AI providers that are already participating in stock trading could present a systemic risk to the financial markets, including through collusion; stresses that algorithmic collusion can be very hard to identify, since AI-based systems do not need to communicate with each other in the way that humans do for collusive practices, which can make it impossible to prove collusive intent; underlines the risk that this poses for market stability and the need for EU and national competition authorities to develop appropriate strategies and tools; highlights, in addition, the systemic risk to financial markets from the widespread use of algorithmic trading models and systems without any human interaction, which have in the past greatly amplified market movements, and are likely to do so again in the future;

69. Observes that many AI companies within the EU currently face legal uncertainty regarding how they can develop their products and services in an assured manner as a result of bureaucratic hurdles, an overlap between existing sector-specific legislation and the absence of established AI standards and norms;

70. Highlights the challenge for AI companies in terms of quality control and consumer protection; concludes that transparency and trustworthiness are essential to ensure that EU companies have a competitive advantage, as such considerations will decide in the future whether a product or service is eventually accepted by the market;

71. Notes that although 26 % of high-value research publications on AI come from Europe, only four out of the top 30 applicants (13 %) and 7 % of businesses engaged in AI patenting worldwide are European;

72. Considers that the EU's intellectual property laws require harmonisation and clear and transparent enforcement, and a balanced, enforceable and predictable framework to allow European businesses, and in particular SMEs and start-ups, to secure intellectual property protection;

73. Is concerned that SME use of IP protection remains low, as SMEs often do not use IP protection as they are not fully aware of their rights nor do they have enough resources to uphold them; highlights the importance of information and statistics on IP protection among SMEs active in knowledge-intensive sectors and welcomes efforts, including simplified registration procedures and lower administrative fees, to provide SMEs and start-ups with better knowledge and to facilitate their access to IP protection; notes that in order to help EU companies protect their AI IP rights, the EU's position as a global standard-setter should be strengthened; stresses that international competitiveness and attractiveness is rooted in a strong and resilient single market, including in IP protection and enforcement;

74. States that data analytics, as well as access to, sharing and re-use of non-personal data, are already essential for many data-driven products and services today, but will be important for the development and deployment of upcoming AI systems; stresses, however, that most of the non-personal data generated in the EU so far goes unused, while a single market for data is still in the making;

75. Points out the importance of facilitating access to data and data sharing, and open standards and open source technology as a way to enhance investments and boost innovation in AI technologies in the EU; specifies that better harmonisation on the interpretations by national data protection authorities as well as on guidance on mixed data and on depersonalisation techniques would be useful for AI developers;

76. Highlights the role AI can play in assisting enforcement action by European and national authorities, particularly in the fields of customs and market surveillance; is of the opinion that trade and customs procedures can be made more efficient and more cost-effective through AI, by increasing compliance and ensuring that only safe products enter the single market; points to the example of the Canada Border Services Agency Assessment and Revenue Management (CARM) system, which greatly simplifies import and export procedures using qualified AI risk assessment and streamlined digitalised information management to reduce the need for lengthy inspections;

e) AI and the labour market

77. Notes that AI is increasingly influencing the labour market, the workplace and the social domain and that the impacts of technological change on work and employment are multifaceted; emphasises that the use of AI in this area gives rise to a number of ethical, legal and employment related challenges; is concerned that in terms of the labour market, digitalisation could lead to workforce reorganisation and the potential disappearance of certain sectors of employment; believes that the adoption of AI, if combined with the necessary support infrastructure, education and training, could increase capital and labour productivity, innovation, sustainable growth and job creation;

78. Stresses that although AI may replace some tasks, including repetitive, heavy, labour-intensive or dangerous ones, it could also help to improve skills, raise the quality of work and create new, higher value-added employment, leaving more time for stimulating tasks and career development; stresses that AI is currently already substituting or complementing humans in a subset of tasks but that it is not yet having detectable significant aggregate labour market consequences[1]; stresses, however, the potential for an increase in income inequality if AI increases high-skill occupations and replaces low-skill occupations; adds that any resulting economic and social implications need to be mitigated by appropriate measures, research and foresight and prepared for by investing in reskilling and upskilling of the workforce with a focus on underrepresented groups such as women and minorities, who are likely to be most affected by this transition, and by promoting diversity in all phases of development of AI systems; is concerned that AI could produce processes of deskilling and create and embed low-paid, low-autonomy work and extend atypical, flexible (or ‘gig’) work;

---

1 Acemoglu, D., et al., *AI and Jobs: Evidence from Online Vacancies,* National Bureau of Economic Research, December 2020.

underlines that algorithmic management could lead to power imbalances between management and employees and obscurity about decision-making;

79. Highlights that AI uptake offers an opportunity to foster significant cultural change within organisations, including through improved workplace safety, better work-life balance, and offering the right to disconnect and more effective training opportunities and guidance to employees; points, in this regard, to the recommendations of the OECD stressing that automation could also give rise to a reduction of working time, thus improving workers' living conditions and health; is of the opinion that human-empowering AI applications could also create new job opportunities, in particular for those who, because of restrictions such as disabilities or living circumstances, have until now been bound to less qualified jobs; stresses the need to use AI assistance in the workplace to provide time for humans to improve the quality of their output instead of just increasing the workload;

80. Condemns the increased recourse to AI-fuelled surveillance in the workplace, often occurring without the workers' knowledge, let alone their consent, particularly also in the context of teleworking; sustains that this practice should not be allowed, as it is extremely abusive of the fundamental right to privacy, data protection and the human dignity of the worker and to social and labour rights, and also has negative effects on the mental health of workers due to the degree of intrusion, its blanket or indiscriminate effect, and lack of safeguards for affected individuals;

81. Is concerned that a similar risk of surveillance is present also in the school environment, with the increasing adoption of AI systems in schools, undermining the fundamental rights of children; notes that the implications AI has for children's privacy, safety and security fall across a wide spectrum, from benefits related to the ability to understand threats facing children with greater specificity and accuracy, to risks around unintended privacy infringements; underlines that both the positive and negative implications for children's privacy, safety and security call for close examination and corresponding safeguards; further stresses that special consideration and protection need to be given to children when developing AI systems because of their particularly sensitive nature and specific vulnerabilities;

82. Stresses that it is paramount to provide individuals with comprehensive skills development programmes in all stages of life, in order to enable them to remain productive in a continuously evolving workplace and avoid their exclusion from the labour market; considers that the adaptation of the workforce in terms of AI education, lifelong learning and reskilling is of vital importance; highlights that current concepts of learning and working are still overly defined by the pre-digital world, which is contributing to a growing skills gap and a new digital divide for citizens who do not have access to a secure digital space; stresses that enhancing digital literacy contributes to achieving the UN Sustainable Development Goals, in particular those on education, human capital and infrastructure; highlights the gain in knowledge of new forms of working and learning due to the COVID-19 crisis which could further be explored;

83. Underlines that to reap the full benefits of digitalisation, the Union must address digital literacy and skills for all; believes that digital literacy is a precondition for citizens' trust in and public awareness of the impacts of AI; highlights the importance of including basic training in digital skills and AI in national education systems; believes that the implementation and development of AI technology in the field of minority languages might lead to a boost in their knowledge and use; stresses that more than 70 % of

businesses report a lack of staff with adequate digital and AI skills as an obstacle to investment; is concerned that as of 2019, there were 7.8 million ICT specialists in the EU, with a prior annual growth rate of 4.2 %, which is far short of the 20 million experts that are needed for key areas such as data analysis as projected by the Commission;

84. Is concerned about the extensive gender gap in this area, with only one in six ICT specialists and one in three science, technology, engineering and mathematics (STEM) graduates being women[1]; notes with concern that the gender divide is persisting, especially in the area of start-ups, where in 2019, USD 92 of every USD 100 invested in European tech companies went to founding teams that were entirely comprised of men; recommends targeted initiatives to support women in STEM in order to close the overall skills gap in this sector; stresses that this gap inevitably results in biased algorithms; emphasises the importance of empowering and motivating girls towards STEM careers and eradicating the gender gap in this area;

f) AI and the future of democracy

85. States that AI has, on the one hand, the potential to assist in building a more transparent and efficient public sector, but on the other hand, that the technical developments in the field of AI, often driven by a logic of growth and profits, are very rapid and dynamic, making it difficult for policymakers to have a sufficient understanding of how new AI applications work and what kind of outcomes those applications can produce, although they have a duty to provide a framework to ensure that AI complies with fundamental rights and can be used for the benefit of society; highlights that expert forecasts on the future impact of AI also vary, suggesting it might be difficult even for them to predict the outcomes of deploying new AI technologies; argues, therefore, that this uncertainty makes it necessary for legislators to take due account of the precautionary principle in regulating AI; believes it is crucial to consult experts with different expertise and backgrounds in order to create solid, workable and future-proof legislation; cautions that legal uncertainty can be one of the biggest impediments to innovation; notes, in this regard, the importance of promoting AI literacy among citizens, including elected representatives and national authorities;

86. Warns that legislative cycles are therefore often out of sync with the pace of technological progress, forcing policymakers to play catch up and favour the regulation of use cases already in the market; points out that a sound regulatory approach to AI must be preceded by an exhaustive analysis of proportionality and necessity, to avoid hampering innovation and the competitiveness of EU companies;

87. Stresses that using AI to acquire biometric data could be both intrusive and damaging or beneficial for the individual, as well as for the general public;

88. Notes with concern that such AI technologies pose crucial ethical and legal questions; notes that certain AI technologies enable the automation of information processing to an unprecedented scale, which paves the way for mass surveillance and other unlawful interference and poses a threat to fundamental rights, in particular the rights to privacy and data protection;

---

1 Commission communication of 9 March 2021 entitled ‘2030 Digital Compass: the European way for the Digital Decade’ (COM(2021)0118).

89. Stresses that many authoritarian regimes use AI systems to control, exert mass surveillance over, spy on, monitor and rank their citizens or restrict freedom of movement; stresses that any form of normative citizen scoring by public authorities, especially within the field of law enforcement, border control and the judiciary, as well as its use by private companies or individuals, leads to loss of autonomy and privacy, brings risks of discrimination and is not in line with European values; recalls that technologies such as cyber-surveillance and biometric recognition, which can be used to these ends, are subject to the EU Export Control Regulation; is highly concerned about and condemns cases of EU companies selling biometric systems which would be illegal to use within the EU to authoritarian regimes in non-EU countries;

90. Notes that dominant tech platforms nowadays not only have significant control over access to information and its distribution, but they also use AI technologies to obtain more information on a person's identity, behaviour and knowledge of decisional history; believes that such profiling poses risks to democratic systems as well as to the safeguarding of fundamental rights and the autonomy of citizens; stresses that this creates an imbalance of power and poses systemic risks that could affect democracy;

91. Points out that digital platforms can, including through AI-driven marketing applications, be used for foreign interference and to spread disinformation and deepfakes, acting as networks for propaganda, trolling and harassment with the aim of undermining electoral processes; stresses that machine learning enables, in particular, the targeted use of personal data to manipulate unaware voters by creating personalised and convincing messages; stresses the importance of strong transparency obligations that are effectively enforced;

92. Underlines that AI could, however, also be used to reduce anti-democratic and unethical activities on platforms, and as a means to limit the distribution of fake news and hate speech, even though tests of its abilities to understand context-specific content have so far shown poor results; is concerned that divisive language may lead to greater user engagement, which is why removal of such language would be in direct conflict with such platforms' business model which is based on maximising user engagement; is of the opinion that AI-powered solutions must be based on full respect for freedom of expression and opinion, and on strong evidence in their favour, before their eventual use;

93. Stresses that bias in AI systems, especially when it comes to deep learning systems, often occurs due to a lack of diverse and high-quality training and testing data, for instance where data sets are used which are not sufficiently representative of vulnerable groups, or where the task definition or requirement settings themselves are biased; notes that bias can also arise due to a possible lack of diversity in developer teams, reiterating intrinsic biases, due to a limited volume of training and testing data, or where a biased AI developer has compromised the algorithm; points out that reasoned differentiation is also intentionally created in order to improve the AI's learning performance under certain circumstances;

94. Stresses that structural biases present in our society should not be repeated or even increased through low quality datasets; specifies, in this regard, that algorithms learn to be as discriminatory as the data they are working with, and, as a result of low quality training data or biases and discrimination observed in society, might suggest decisions that are inherently discriminatory, which exacerbates discrimination within society; notes, however, that AI biases can sometimes be corrected; concludes that it is therefore

necessary to apply technical means and establish different control layers on AI systems, including the software, algorithms and data used and produced by them, in order to minimise this risk; argues that AI can and should be used to reduce biases and discrimination and promote equal rights and positive social change in our societies, including through normative requirements on data sets used to train AI systems; stresses that one of the most efficient ways of reducing bias in AI systems is to ensure, to the extent possible under Union law, that the maximum amount of non-personal data is available for training purposes and machine learning;

g) Recurring findings in all six case studies

95. Notes that there are clear societal benefits and opportunities associated with adopting AI technologies, which can only be reaped if transversal obstacles are addressed in the EU, in accordance with fundamental rights, values and legislation; states that overlap of legislation, market fragmentation, bureaucratic hurdles, a lack of accessible digital infrastructure and digital skills in the broader society, and insufficient investment in research and development can be observed in particular as barriers to the successful application of trusted AI in all fields analysed;

96. Concludes from the case studies examined, furthermore, that there are certain use cases that are risky or harmful, but that it is not necessarily specific AI technologies themselves but their areas of application; recognises that future regulation needs to address legitimate concerns related to these risks in order for AI technologies to find broad application in the EU;

97. States that while it is important to examine and categorise potential risks posed by AI, the case studies illustrated that AI technologies can provide us with effective countermeasures that are able to mitigate or eliminate these risks; underlines that as AI is still in its early stages of development within a wider context of emerging technologies, its full potential as well as its risks are not certain; points out that there is a need to look not only at risks to individuals, but also at the broader societal and non-material individual harms; highlights the significant imbalances of market power present in data markets and the adjacent AI economy; stresses that fair competition and removing obstacles to competition for start-ups and SMEs are essential to fairly distribute the potential benefits of AI in economic and societal terms, which appear to be significant both in the EU and globally;

3. The EU's place in global AI competition

98. Observes fierce global AI competition, where the EU has not yet met its aspirations; examines in the following sections the EU's global competitiveness with regard to AI by comparing it with that of China and the US, focusing on three core elements: regulatory approach, market position and investments; recognises, however, that transnational markets and corporations cannot easily be delineated across national borders, as most tech companies have customers, shareholders, employees and suppliers in many different countries;

a) Regulatory approach

99. Notes that the US has not yet introduced horizontal legislation in the digital field, and has so far focused on sector-specific laws and facilitating investments, including through tax measures on private sector innovation, in particular among its tech giants

and leading universities; observes that, despite recent developments showing a more active policymaking role, the US approach has so far mostly reflected a focus on providing legal guidance to businesses, investing in research projects and removing perceived barriers to innovation;

100. Stresses that the 2019 American AI Initiative Act ushered in a slight realignment, as besides redirecting funding, retraining workers and strengthening digital infrastructure, the US Government announced the development of common standards for trustworthy AI; notes, however, that the resulting 10 principles were very broadly formulated in order to allow each government agency to create sector-specific regulations; expects that although the current US administration plans to bring forward a new bill of rights to limit AI harms in 2022, the US approach will remain market-driven;

101. Highlights that the Chinese President Xi Jinping underlined in as early as 2013 the importance of technologies in geopolitics, the role of public policies in defining long-term objectives and the fact that AI technologies offer an opportunity to relaunch its military power; stresses further that the Chinese Government subsequently put forward the Made in China 2025 plan in 2015 and the Next Generation AI Development Plan in 2017, both of which had the clear targets of making China the global leader in AI by 2030; notes that the 2018 Chinese AI standardisation white paper further outlined how the socialist market economy can develop international standards and strategically engage in international standardisation organisations; notes the introduction of rules on recommender systems as well as an ethics code on AI in China;

102. Observes that on the global stage, China actively promotes international AI partnerships as a way to export its own AI-based surveillance practices, social scoring system and censorship strategies; emphasises that heavy investment abroad under the Digital Silk Road initiative is also used as a means to spread Chinese influence and its AI technology globally, which could have far-reaching implications beyond imposing technological standards or maintaining technological competitiveness; concludes that the Chinese Government's approach is therefore built upon deploying AI domestically as well as exporting AI technologies based on predetermined standards that are in line with the ideology of the Chinese Government;

103. Notes that the Commission started its work on regulating AI in 2018 by publishing the European AI strategy, setting up a High-Level Expert Group and introducing a coordinated plan[1] to foster 'AI made in Europe'; notes that the 2020 white paper on AI proposed numerous measures and policy options for future AI regulation and eventually resulted in the horizontal AI Act[2], which was presented along with a revised coordinated plan on AI[3] in May 2021; points out that as of June 2021, 20 Member States have published national AI strategies, while seven more are in the final preparatory stages of adopting theirs;

---

1 European Commission, Coordinated Plan on Artificial Intelligence (COM(2018)0795).

2 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206).

3 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions – Fostering a European approach to Artificial Intelligence (COM(2021)0205).

104. Emphasises that central to the EU regulatory approach is a strong attention to the development of a European digital single market as well as ethical considerations in line with core human rights values and democratic principles; acknowledges that establishing the world's first regulatory framework for AI could give the EU leverage and a first-mover advantage in setting international AI standards based on fundamental rights as well as successfully exporting human-centric, 'trustworthy AI' around the world; underlines that this approach needs to be supported by regulatory coordination and convergence with international partners;

b) Market situation

105. Notes that many of the 100 leading AI companies globally are headquartered in the US, whereas only few are in the EU; notes that the US also leads in the total number of AI start-ups;

106. Points out that in recent years, several European digital companies have been acquired by US tech giants; welcomes the Commission's ambition of tackling acquisitions that may have a significant impact on effective competition in the digital market and of limiting killer acquisitions; points out, however, that in some cases, acquisition may be a primary objective of start-up creators and their funders, as one legitimate method to derive benefits from their ideas;

107. Stresses that while the US and China are trying to accelerate the use of AI technologies in the public and private sectors, the adoption of AI within the EU lags behind; states that in 2020, only 7 % of EU companies with at least 10 employees were using AI technologies, with significant differences among Member States as well as among different business sectors;

108. Is concerned that while the US and China each have a unified digital market with a coherent set of rules, the EU's digital single market is still not complete and unjustified barriers remain; stresses that the development of AI products and services could be further slowed down by the ongoing work on 27 different national AI strategies;

109. Points also to the fact that inconsistencies in EU law, overlap of different legislative initiatives, contradictions between EU and national laws, different legal interpretations and a lack of enforcement among Member States all prevent a level playing field and risk creating legal uncertainty for European companies as they may find it difficult to determine whether their AI innovations are compliant with EU law;

110. Notes that the market fragmentation for AI companies is further exacerbated by a lack of common standards and norms in some sectors, including on data interoperability;regrets the regulatory risk resulting from the delay of legislation, such as the ePrivacy Regulation; highlights as an example the fact that EU AI developers face a data challenge that neither their US nor Chinese counterparts do due to the incomplete European digital single market; observes that they often do not have enough high-quality data to train and test their algorithms, and struggle with a lack of sectoral data spaces and cross-sectoral interoperability, as well as constraints on cross-border data flows;

c) Investments

111. Observes that European companies and governments invest far less in AI technologies than the US or China; points out that although private investments in the EU AI industry are rising significantly, the EU is still substantially underinvesting in AI compared to other leading regions, as the US and China account for more than 80 % of the EUR 25 billion annual equity investments in AI and blockchain, while the EU's share only amounts to 7 % or about EUR 1.75 billion; stresses that the liquidity of EU financing markets for tech companies still lacks the scale of comparable markets in the US; notes that the US is also leading in venture capital and private equity funding, which is particularly important for AI start-ups, with EUR 12.6 billion in 2019, against EUR 4.9 billion for China and EUR 2.8 billion for the EU; notes that as a consequence, European AI entrepreneurs are crossing the Atlantic to scale up their businesses in the US;

112. States that together with national initiatives, the estimated annual public investment of the EU in AI of EUR 1 billion[1] is much lower than the EUR 5.1 billion invested annually in the US and up to EUR 6.8 billion in China[2]; states, however, that between 2017 and 2020, EU public funding for AI research and innovation increased by 70 % compared to the previous period, and in 2019, the EU invested between EUR 7.9 and 9 billion in AI, which was 39 % more than in the previous year; acknowledges and welcomes the Commission's plans to increase investment further through the digital Europe programme, Horizon Europe, InvestEU, the European Structural and Investment Funds, the European Investment Fund, the Connecting Europe Facility in Telecom and various cohesion policy programmes, which will be further complemented and leveraged by the 20 % minimum expenditure target for digital transition in the national recovery and resilience plans, as agreed by the Commission and the Member States under the Recovery and Resilience Facility; underlines, however, the recent report by the European Investment Bank which quantifies the EU investment gap in AI and blockchain technologies at EUR 5-10 billion per year;

113. Stresses that AI companies within the EU face strong competition for qualified employees, which is made worse by 42 % of the EU population lacking basic digital skills; stresses the need to train and attract a substantially higher number of well-educated graduates, including women, to work in the digital sector;

114. Observes that although the EU has an excellent community of researchers on AI, the brain drain of EU researchers remains an issue; stresses that measures are needed to appeal to leading researchers; notes that the EU only spent 2.32 % of its GDP on research and development in 2020, while the US spent 3.08 %; recalls that the Member States must uphold their commitment to invest 3 % of their GDP in research and development in order to ensure the Union's strategic autonomy in the digital field;

115. Notes that the EU's digital infrastructure needs substantial updating, with just 25 % of people in the EU being able to connect to a 5G network, compared to 76 % of people in the US; observes that the EU lacks sufficient high-performance digital infrastructure with interoperable data spaces, high transmission rates and volumes, reliability and short delays; stresses the need to support European AI ecosystems with excellence clusters;

---

1 Data from 2018.

2 Koerner, K., *(How) will the EU become an AI superstar?*, Deutsche Bank, March 2020.

d) Conclusion

116. Concludes that the US is the overall leader in AI as it is ahead in many categories, with US-headquartered companies leading technology development in areas such as cloud computing and high-performance computing capabilities, and also when it comes to investment, attracting AI talent, research and infrastructure; highlights, however, that China, which a few years ago was still significantly lagging behind the US in all indicators, is quickly catching up; recognises that both countries have the advantage of a unified single market and stronger commitment to remaining a leader in AI;

117. Stresses that despite the EU's strong position on industrial software and robotics, EU actors are still behind their US and Chinese peers in many categories; underlines that the EU should develop an ambitious plan for human-centric European AI; notes that the EU is, however, ahead on regulatory approaches; points out that a viable EU strategy for becoming more competitive on AI involves focusing on research and innovation, skills, infrastructure and investment, while at the same time trying to establish a future-oriented, horizontal and innovation-friendly regulatory framework for AI development and use, and simultaneously ensuring that fundamental rights of EU citizens and the rule of law are safeguarded;

118. Underlines that Brexit had a negative impact on the EU's efforts to strengthen its global AI footprint, as the UK was one of the leading EU countries in AI; stresses, however, that the UK should remain a valued partner of the EU, bolstering the competitiveness of both partners and the promotion of shared regulatory outlooks in global standard setting;

119. Concludes that the EU is currently still far from fulfilling its aspiration of becoming competitive in AI on a global level, and could risk falling further behind in some categories; maintains that swift action on the EU Roadmap for AI outlined below poses an opportunity to change this situation;

120. Specifies that as the EU does not have the legislative power to address all the points listed in the EU Roadmap for AI, the special committee recommends pursuing further high-level discussions and political processes among EU institutions and Member States in order to push for a more harmonised approach to AI and help Member States to coordinate their efforts; refers, in this regard, to the EU 2000 Lisbon agenda, which, despite the criticism, played an important part in guiding the EU's policy orientation over 20 years and in keeping up the pressure on Member States to reform;

4. 'Europe fit for the digital age' – Roadmap for becoming a global leader

a) Favourable regulatory environment

i. LAW-MAKING

121. Calls on the Commission to only propose legislative acts in the form of regulations for new digital laws in areas such as AI, as the digital single market needs to undergo a process of genuine harmonisation; is convinced that due to rapid technological development, digital legislation should always be flexible, principle-based, technology-neutral, future-proof and proportionate, while adopting a risk-based approach where appropriate, based on respect for fundamental rights and preventing unnecessary additional administrative burden for SMEs, start-ups, academia and research; stresses,

furthermore, the importance of a high degree of legal certainty and, consequently, the need for robust, practical and unambiguous applicability criteria, definitions and obligations in all legal texts regarding the sale, use or development of AI technologies;

122. Believes that the better regulation agenda is key to making the EU AI strategy a success; stresses the need to focus on the review, adaptation, implementation and enforcement mechanisms of already existing laws before proposing new legislative acts;

123. Urges the Commission to perform in-depth *ex ante* impact assessments with adequate foresight and risk analysis prior to issuing new digital proposals in areas such as AI; emphasises that impact assessments should systematically map and evaluate relevant existing legislation, preventing any overlaps or conflicts;

124. Suggests that new laws in areas such as AI should be complemented with the promotion of stakeholder-developed European standards; is of the opinion that the EU should strive to avoid fragmentation and that international standards can serve as a useful reference, but that the EU should prioritise developing its own standards; highlights that such standards should result from fair competition for the best standards within the EU, which should be responded to by the EU and standardisation organisations; notes that technical standards and design instructions could then be combined with labelling schemes as a way to build consumer trust by providing trustworthy services and products; stresses the role of EU standardisation organisations in developing state-of-the-art technical standards; calls on the Commission to accelerate issuing standardisation mandates to the European standardisation organisations according to Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation[1];

125. Explains that an open certification platform could establish an ecosystem of trust that involves governments, civil society, businesses and other stakeholders;

126. Calls for Parliament, the Commission and the Council to improve their abilities to deal with internal competence conflicts when it comes to overarching topics such as AI, as such conflicts risk delaying the legislative procedure, with knock-on effects in terms of the entry into force of the legislation;

ii. GOVERNANCE AND ENFORCEMENT

127. Calls for consistent EU-wide coordination, implementation and enforcement of AI-related legislation;

128. Explains that stakeholder-based consultation forums such as the Data Innovation Board, to be established by the Data Governance Act, or the European AI Alliance, which includes private-public partnerships, such as the European Alliance for Industrial Data, Edge and Cloud, are a promising governance approach; elaborates that this approach enables the EU's AI ecosystem to operationalise its principles, values, objectives and reflect societal interests at the level of software code;

129. Highlights that the 'pacing problem' requires special focus on effective *ex post* enforcement by courts and regulatory agencies as well as *ex ante* approaches to deal with legal challenges posed by emerging technologies; supports, therefore, the use of

---

1 OJ L 316, 14.11.2012, p. 12.

regulatory sandboxes, which would give AI developers the unique chance to experiment in a fast, agile and controlled manner under the supervision of competent authorities; notes that these regulatory sandboxes would be experimental spaces in which to test AI systems and new business models under real world conditions in a controlled environment before they enter the market;

iii. LEGAL FRAMEWORK FOR AI

130. Highlights that an underlying objective of the EU's digital strategy, as well as that of the AI strategy, is creating a 'European Way' in a digitalised world; clarifies that this approach should be human-centric, trustworthy, guided by ethical principles and based on the concept of the social market economy; underlines that the individual and the protection of their fundamental rights should always remain at the centre of all political and legislative considerations;

131. Agrees with the conclusion drawn by the Commission in its 2020 White Paper on artificial intelligence that there is a need to establish a risk-based legal framework for AI, notably covering high-level ethical standards based on transparency, auditability and accountability, combined with product safety provisions, appropriate liability rules and sector-specific provisions, while at the same time providing businesses and users with enough flexibility and legal certainty and a level playing field to foster AI uptake and innovation;

132. Points out the guiding added value of taking the concepts, terminology and standards developed by the OECD as inspiration for the definition of AI in legislation; stresses that doing so would give the EU an advantage in shaping a future international AI governance system;

133. Is convinced that it is not always AI as a technology that should be regulated, but that the level of regulatory intervention should be proportionate to the type of individual and/or societal risk incurred by the use of an AI system; underlines, in this regard, the importance of distinguishing between 'high-risk' and 'low-risk' AI use cases; concludes that the former category needs strict additional legislative safeguards while 'low-risk' use cases may, in many cases, require transparency requirements for end users and consumers;

134. Specifies that the classification of AI systems as 'high-risk' should be based on their concrete use and the context, nature, probability, severity and potential irreversibility of the harm that can be expected to occur in breach of fundamental rights and health and safety rules as laid down in Union law; stresses that this classification should be accompanied by guidance and the promotion of the exchange of best practices for AI developers; stresses that the right to privacy must always be respected and that AI developers should guarantee full compliance with the rules on data protection;

135. Underlines that AI systems that are likely to interact with or otherwise affect children must take their rights and vulnerabilities into account and meet the highest available standards of safety, security and privacy by design and default;

136. Notes that the environments in which AI systems operate may differ in a business-to-business (B2B) environment compared to a business-to-consumer (B2C) environment; points out that consumer rights need to be legally protected through consumer protection legislation; stresses that while companies can solve liability and other legal

challenges quickly and cost-effectively by contractual means with business partners directly, legislation may be necessary to protect smaller businesses from market power abuse by dominant actors through commercial or technological lock-in, barriers to market entry or asymmetric information problems; highlights that there is also a necessity to take into account the needs of SMEs and start-ups with complex requirements, to avoid putting them at a disadvantage compared to larger companies, which have the resources to maintain sizeable legal and compliance departments;

137. Underlines the need to apply a principles-based approach to open ethical questions raised by new technological possibilities resulting from the sale and use of AI applications, including through the use of fundamental, mandatory principles such as the non-maleficence principle, the principle of respecting human dignity and fundamental rights, and the protection of the democratic process; notes that good practices in AI development such as human-centric AI, responsible governance and the principles of transparency and explainability, as well as principles of sustainable AI that are fully aligned with the UN 2030 Agenda for Sustainable Development, are other important components in shaping the AI economy;

138. Acknowledges that it is not always possible to completely 'de-bias' AI algorithms as the ideal objective of error-free data is very difficult or near impossible to achieve; notes that even an AI system that has been tested will inevitably encounter real world scenarios that might produce biased results when deployed in a setting that differs from the composition of its training and testing data; stresses that the EU should strive to improve the transparency of data sets and algorithms, cooperate very closely with AI developers to counterbalance and reduce structural societal biases and consider mandatory human rights due diligence rules at an early stage of development;

139. Elaborates that meaningful transparency or explainability obligations for AI systems, while helpful in many cases, may not be possible to implement in every instance; notes that intellectual property rights and trade secrets must be protected from illegal practices such as industrial espionage;

140. States that the legislative framework on intellectual property must continue to incentivise and protect AI innovators by granting them patents as a reward for developing and publishing their creations; finds that existing laws are mostly future-proof, but proposes certain adjustments, including the integration of open source elements, as well as the use of public procurement to mandate, where appropriate, open source software for AI solutions; proposes new forms of patent licensing to ensure that tools are available to regions and initiatives that could not otherwise afford them;

141. Considers that obligatory *ex ante* risk self-assessments based on clear rules and standards, as well as data protection impact assessments, complemented by third-party conformity assessments with relevant and appropriate CE marking, combined with *ex post* enforcement by market surveillance, could be useful to ensure that AI systems on the market are safe and trustworthy; believes that in order to prevent SMEs from being pushed out of the market, standards and guidance on complying with AI legislation should be developed with the close involvement of small businesses, internationally aligned to the greatest extent possible and available free of charge;

142. Notes that in order to increase product safety and improve the identification of faults, the developers of high-risk AI should ensure that accessible logs of algorithmic activity are maintained securely; considers that, where relevant, developers should design high-

risk AI systems with embedded mechanisms – ‘stop buttons’ – for human intervention to safely and efficiently halt automated activities at any moment and ensure a human-in-the-loop approach; considers that the AI system’s output and reasoning should always be comprehensible by humans;

143. Recognises the legal challenges caused by AI systems, and that there is a need to consider a revision of specific parts of the existing liability rules; looks forward, in this regard, to the presentation of the Commission’s legislative proposal on AI liability; stresses that the Product Liability Directive[1] and the national fault-based liability regimes can, in principle, remain the centrepiece legislation for countering most harm caused by AI; underlines that in some cases there could be inappropriate outcomes, but warns that any revision should take the existing product safety legislation into account and should be based on clearly identified gaps, while being future-proof and capable of being effectively implemented and of ensuring the protection of individuals in the EU;

144. Underlines that the legal framework should not subject children to the same level of personal responsibility as adults for understanding risk;

145. Notes that certain changes to the legal definitions of ‘product’, including integrated software applications, digital services and inter-product dependency, and ‘producer’, including backend operator, service provider and data supplier, may be considered to ensure that compensation is available for harm caused by these technologies; stresses, however, that an overly broad or excessively narrow approach to the definition of ‘product’ should be avoided;

146. Points out that, due to the characteristics of AI systems, such as their complexity, connectivity, opacity, vulnerability, capacity of being modified through updates, capacity for self-learning and potential autonomy, as well as the multitude of actors involved in their development, deployment and use, there are significant challenges to the effectiveness of Union and national liability framework provisions; considers, therefore, that although there is no need for a complete revision of well-functioning liability regimes, specific and coordinated adjustments to European and national liability regimes are necessary to avoid a situation in which persons who suffer harm or whose property is damaged end up without compensation; specifies that while high-risk AI systems should fall under strict liability laws, combined with mandatory insurance cover, any other activities, devices or processes driven by AI systems that cause harm or damage should remain subject to fault-based liability; believes that the affected person should nevertheless benefit from a presumption of fault on the part of the operator, unless the latter is able to prove that it has abided by its duty of care;

iv. EU DATA CHALLENGE

147. Takes note of the conclusions drawn by the Commission in its 2020 communication entitled ‘A European strategy for data’ and by Parliament in its resolution of 25 March 2021 on the same topic, which state that the creation of a single European data space accompanied by the development of sectoral data spaces and a focus on common standards is key to ensuring fast scalability of AI solutions in the EU and beyond, as well as to ensure the EU’s open strategic autonomy and economic

---

[1] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, 7.8.1985, p. 29).

prosperity; recalls the essential link between the availability of high-quality data and the development of AI applications; stresses, in this regard, the need to deploy robust, reliable and interoperable cloud services within the EU, as well as solutions that leverage decentralised data analytics and edge architecture; calls on the Commission to clarify rights to access, use and share data by holders of co-created non-personal data; stresses that data access must be made technically possible, including through interoperable standardised interfaces and interoperable software; stresses that barriers to data sharing lead to less innovation, diminished competition and the furthering of oligopolistic market structures, which face a strong risk of perpetuating themselves into the adjacent market for AI applications;

148. Stresses the key importance of opening data silos and fostering access to data for AI researchers and companies as outlined in Parliament's resolution on the European data strategy; stresses that market imbalances deriving from increased data restriction by private companies increase market entry barriers and diminish wider data access and use, making it especially difficult for start-ups and researchers to acquire or licence the data they need to train their algorithms; underlines the need to establish the required legal certainty and interoperable technical infrastructure, while also motivating data holders in Europe to make their large amounts of unutilised data available; considers that voluntary data sharing between businesses based on fair contractual arrangements contributes to achieving this goal; acknowledges, however, that B2B contractual agreements do not necessarily guarantee adequate access to data for SMEs owing to disparities in negotiation power or expertise; highlights that open data marketplaces facilitate data sharing by helping AI companies and researchers to acquire or licence data from those who wish to make data available on such marketplaces, which include data catalogues, and allow data holders and users to negotiate data sharing transactions; welcomes in this context the rules on data intermediation services in the Data Governance Act;

149. Welcomes the initiatives of the European cloud federation, such as the European Alliance for Industrial Data, Edge and Cloud, as well as the GAIA-X project, which aim to develop a federated data infrastructure and create an ecosystem that allows scalability, interoperability and self-determination of data providers; notes that an EU cloud rulebook that compiles existing legislation and self-regulatory initiatives would also help to translate common EU principles and values into actionable processes and checks for technical practitioners;

150. Recommends that data interoperability be further strengthened and that common standards be established in order to facilitate the flow of data between different machines and entities, to enhance the sharing of data across countries and sectors and to enable the large-scale creation of high-quality datasets; notes that encouraging open standards, open source software, creative commons licences, and open application programming interfaces (APIs) could also play a key role in accelerating data sharing; highlights the role of common European data spaces in facilitating the free movement of data in the European data economy;

151. Calls on the Commission and the Member States to guarantee that fair contractual conditions are more strongly enforced within the scope of competition rules, with the aim of addressing imbalances in market power without unjustifiably interfering with contractual freedom, and that antitrust authorities are equipped and resourced to counter data concentration tendencies; underlines that European data spaces would allow companies to cooperate more closely with each other, and therefore considers that more

guidance and legal clarity for businesses on competition law and cooperation on data sharing and pooling is needed; stresses that data cooperation, including for the training of AI applications or in the internet of things (IoT) industry, should under no circumstances facilitate the forming of cartels or create barriers to new entrants into a market; emphasises the importance of clarifying the contractual rights of AI developers and companies which contribute to the creation of data through the use of algorithms or IoT machines, and in particular the rights to access data, to data portability, to urge another party to stop using data, and to correct or delete data;

152. Calls on Member States, with regard to government-held data, to quickly implement the Open Data Directive[1] and to properly apply the Data Governance Act, making high-value datasets available ideally free of charge and supplying them in machine readable formats and APIs; stresses that this initiative would reduce the costs for public bodies to disseminate and re-use their data and would help EU researchers and companies enormously in improving their digital technologies in areas such as AI;

153. Calls for a uniform implementation of the GDPR across the EU by effectively and swiftly applying the consistency mechanism and by aligning the diverse national interpretations of the law; finds that there is also a need to better equip data protection authorities, including with technical expertise;

154. Takes note of the Commission's 2019 practical guidance on how to process mixed data sets; points out that not sharing data sets continues to often be the best option for AI researchers and companies due to uncertainty as to whether data is sufficiently anonymised;

155. Considers that Opinion 05/2014 of the Article 29 Data Protection Working Party of 10 April 2014 on anonymisation techniques offers a useful overview, which could be further developed; calls on the European Data Protection Board (EDPB) to adopt guidelines based on specific use cases and relevant situations for different types of data controllers and processors and different processing situations, including a checklist with all the requirements that have to be fulfilled to make data sufficiently anonymous; notes, however, that anonymisation techniques are currently not able to guarantee full and complete protection of privacy, as experiments have shown that modern AI systems nevertheless manage to re-identify a person;

156. Asks the EDPB to issue more guidance for researchers and companies in areas such as AI on how to effectively process personal data outside the EU in a GDPR-compliant way;

157. Suggests the funding of more research on standardising 'privacy by design' approaches, as well as promoting cryptographic solutions and privacy-preserving machine learning, as it is crucial to ensure that high-quality data can be used to train algorithms and perform AI tasks without breaching privacy; notes that data trusts, certifications for high-risk AI applications, personal information management systems and the use of synthetic data also show promise;

---

[1] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (OJ L 172, 26.6.2019, p. 56).

158. Encourages the EU and its Member States to leverage the recently established OECD project on trusted government access to personal data held by the private sector as a reference point for policymakers globally to work towards an international solution and regulatory convergence of best practices in this area; stresses, in this regard, that the free flow of data and metadata across international borders, while fully respecting the EU data protection *acquis*, is a crucial enabler for digital innovation in Europe; calls on the Commission to therefore refrain from imposing data localisation requirements, except where required to protect fundamental rights, including data protection, or in limited, proportionate and justified cases where such a policy is in the interest of the EU or necessary to uphold European standards;

159. Calls on the Commission to respond to the ruling of the Court of Justice of the European Union (CJEU) that the EU-US Privacy Shield is invalid by taking all the measures necessary to ensure that any new adequacy decision with regard to the US fully complies with the GDPR, with the Charter of Fundamental Rights of the European Union, and every aspect of the CJEU judgment, while also simplifying transatlantic data flows; calls on the Commission to continue pursuing data adequacy talks with other non-EU countries, as this is the best way to promote the EU's data protection policies and allow the international exchange of data;

b) Completing the digital single market

i. NATIONAL AI STRATEGIES

160. Calls on the Member States to review their national AI strategies, as the several of them still remain vague and lack clear goals, including regarding digital education for society as a whole as well as advanced qualifications for specialists; recommends that the Member States formulate concrete, quantifiable and specific actions, while trying to create synergies between them;

161. Calls on the Commission to help Member States to set priorities and align their national AI strategies and regulatory environments as much as possible in order to ensure coherence and consistency across the EU; points out that, while a diversity of national approaches is a good way to establish best practices, AI developers and researchers would face major obstacles if they were subject to different operating parameters and regulatory obligations in each of the 27 Member States;

ii. MARKET BARRIERS

162. Urges the Commission to continue its work on removing unjustified barriers to the full completion of the digital single market, including undue country-based discrimination, incomplete mutual recognition of professional qualifications, overly burdensome market access procedures, unnecessarily high regulatory compliance costs and diverging conformity assessment procedures, and to address the frequent use of derogations which results in diverging rules among different Member State jurisdictions; highlights that for companies operating in a cross-border environment, EU-wide rules on AI, in contrast to a fragmented country-by-country approach, are a welcome development that will help foster European leadership on AI development and deployment;

163. Calls on the Commission to accelerate the establishment of a real capital markets union; stresses the need to improve access to financial resources, especially for SMEs, start-ups and scale-ups;

164. Underlines the need to swiftly conclude the negotiations on pending legislative files aimed at the completion of the digital single market;

165. Calls on the Commission to ensure consistent enforcement of the rules of the single market;

166. Notes that the new legislative framework should be carefully updated and aligned with digital products and services; proposes that the focus be placed on modernising and simplifying compliance procedures by introducing digital alternatives to existing analogue and paper-based means allowing companies, for instance by using digital CE marking, electronic labelling or digitalised safety instructions;

167. Encourages the Commission to support offline businesses wishing to go online; encourages further information campaigns targeting SMEs and start-ups in anticipation of new and future EU legislation in this regard, as well as increased enforcement of market surveillance rules as a means to increase the trust of European consumers;

iii. LEVEL PLAYING FIELD

168. Is convinced that the current national and European competition and antitrust frameworks need to be reformed in order to better target abuses of market power and algorithmic collusion in the digital economy, and issues related to data accumulation, as well as to better address the risks of new emerging monopolies without compromising innovation; welcomes the upcoming approval of the Digital Markets Act; calls for specific consideration of potential competition issues in the field of AI;

169. Notes that such a reform should strengthen an evidence-based approach and take the value of data and the implications of network effects more into account, introducing clear rules for market-dominant platforms and increasing legal certainty for cooperation in the digital economy;

170. States, in this regard, that the Commission should adapt its market definition practices to define markets more accurately and in line with modern market realities in the digital sector, carrying out dynamic analysis and adopting a long-term view to assess the existence of competitive pressures;

171. Calls on the Commission and national competition authorities to increase their efforts to monitor digital markets on an ongoing basis, and thus identify competitive constraints and competition bottlenecks, and subsequently impose correctives more frequently on companies that abuse their dominant position or that engage in anti-competitive behaviour;

172. Calls on the Member States to substantially increase funding for and the technical capacity of competition authorities in order to ensure the effective and swift enforcement of competition rules in the fast-paced and complex digital economy; underlines that competition authorities should speed up abuse proceedings and, where necessary, apply interim measures to preserve and promote fair competition, while at the same time guaranteeing the procedural defence rights of companies;

c) Digital green infrastructure

i. CONNECTIVITY AND COMPUTING POWER

173. Calls on the Commission to follow up on its ambition of incentivising 75 % of European enterprises to take up cloud computing services, big data and AI by 2030 in order to remain globally competitive and accelerate its climate neutrality targets to ensure they are achieved by 2050; finds that the allocation of EUR 2.07 billion in funding for digital infrastructure under the Connecting Europe Facility is insufficient;

174. Stresses that the shift in the volume and processing of data for AI also requires the development and deployment of new data processing technologies encompassing the edge, thereby moving away from centralised cloud-based infrastructure models towards an increased decentralisation of data processing capabilities; urges the strengthening of investment and research in distributed computing clusters, edge nodes and digital microcontroller initiatives; notes that moving to a wide use of edge solutions may be more resource intensive, as benefits of pooling optimisation are lost and stresses that the environmental cost/benefit of edge infrastructures should be looked into at a systemic level in a European cloud strategy, including to optimise energy consumption of AI;

175. Stresses that AI requires powerful hardware to make sophisticated algorithms useable, including high-performance and quantum computing and the IoT; calls for continued increases in targeted public and private funding for innovative solutions that reduce energy consumption, including software eco-design; calls for the development of standards on measuring the use of resources by digital infrastructure at EU level, based on best practices; is concerned about the global microprocessor crisis and welcomes, in this regard, the Commission's proposal for a Chips Act to reduce the EU's current dependence on external suppliers; warns, however, of the future risks of overcapacity in the market and cautions careful consideration of the investment cycle;

176. Highlights that a functioning and fast infrastructure for AI must be based on fair and safe digital high-speed connectivity, which requires 5G roll-out in all urban areas by 2030, as well as wide access to ultra-fast broadband networks and spectrum policy with licence conditions that ensure predictability, foster long-term investment and do not distort competition; urges the Member States to continue to implement the 5G toolbox; calls for the Broadband Cost Reduction Directive[1] to be put into practice to facilitate network deployment; calls on the Commission to conduct environmental impact assessments on 5G; stresses the importance of counteracting the spread of disinformation related to 5G networks with an EU communication strategy; points out, in this regard, that a broad and inclusive debate will ultimately contribute to creating trust among citizens regarding the actions towards continuous development of mobile networks;

177. Calls on the Commission to establish timetables for the Member States, cities, regions and industry and improve the administrative approval processes for 5G; requests that in regions where roll-out is carried out by the public sector, more funds be made available to bring high-speed connectivity to remote communities and contribute to bridging the digital gap; calls for support for broadband and connectivity projects under the multiannual financial framework, with easier access for local authorities to avoid the underutilisation of public funds;

---

[1] Directive 2014/61/EU of the European Parliament and of the Council of 15 May 2014 on measures to reduce the cost of deploying high-speed electronic communications networks (OJ L 155, 23.5.2014, p. 1).

178. Calls on the Commission to assess the interplay between AI and the next wave of digital infrastructure, enabling Europe to take the lead in next generation networks, including 6G;

179. Calls for a clear strategy on fibre-optic network deployment and broadband roll-out in rural areas, which is also key for data-intensive technologies such as AI; calls, in this regard, for increased support by the European Investment Bank for connectivity projects in rural areas;

180. Stresses that the significant investment required for network deployment and a swift roll-out in order to achieve the targets set by the Digital Compass requires infrastructure-sharing agreements, which are also key to promoting sustainability and reducing energy consumption; stresses that these efforts are still at their beginning and need to be further expanded;

ii. SUSTAINABILITY

181. Urges the EU to take the lead in making green digital infrastructure climate neutral and energy efficient by 2030 in line with the Paris Agreement targets and integrated with the European Green Deal policy programme; including by assessing the environmental impact of large-scale deployments of AI-based systems, taking into account the increased energy needs of AI development and use; calls for coordinated global multilateral action to utilise AI in the fight against climate change and environmental and ecological degradation, as well as biodiversity loss;

182. Urges the use of AI to monitor energy consumption in municipalities and develop energy efficiency measures;

183. Recognises the data- and resource-intensive character of some large-scale AI applications and their respective impacts on the environment; recalls that for European AI to be sustainable and environmentally responsible, AI systems should be designed, developed and deployed with achieving the green transition, climate neutrality and a circular economy in mind;

184. Calls on the Commission to incentivise the use of energy-efficient data centres that can support carbon neutrality;

185. Highlights that data centres' current lack of information sharing hinders the possibility of taking adequate public action and having a comparative overview of the environmental performance of data centres; calls for a significant increase in the number of environmental impact assessments carried out on AI development; calls for requirements to be developed to ensure that appropriate evidence is available to measure the environmental footprint of large-scale AI applications; points to the need for clear rules and guidelines for environmental impact assessments on AI, including multi-criteria life cycle assessments; calls for open access to data centres' environmental key performance indicators, the development of EU standards and the creation of EU green cloud computing labels;

186. Calls for a circular economy plan for digital technologies and AI and emphasises that the EU should secure a strong ICT recycling chain;

187. Recommends fostering the use of AI-based solutions, in line with the green and digital twin transitions in all sectors, to coordinate sustainable standards for businesses and

enable the monitoring of energy efficiency and the collection of information on emissions and product lifecycles;

188. Calls on the Commission to launch competitions and missions for AI solutions tackling specific environmental problems and to strengthen this component in Horizon Europe and the digital Europe programme; recalls that projects relating to AI's potential for addressing environmental concerns should be carried out on the basis of responsible and ethical research and innovation;

189. Calls on the Commission to develop environmental criteria and tie the allocation of the EU budget, funding and public procurement procedures for AI to their environmental performance;

190. Calls on the Commission to foster smart cities, covering smart buildings, smart grids, connected cars, mobility platforms, public services and logistics; supports the development of a common collection of best practices for projects and applications; stresses that smart cities require good cooperation between state and local governments, as well as among their agencies and private parties;

191. Stresses the need to define principles to ensure that relevant climate and sustainability data can be integrated when setting up new sustainability data spaces;

192. Calls on the Commission to cooperate with the Member States and the private sector in setting up and support testing facilities where AI applications can be tested on their sustainability performance and to offer guidance on how to improve the environmental footprint of these application; encourages adapting existing testing facilities to focus on use cases in circular production;

193. Calls on the Commission to promote sustainable transport infrastructure that uses AI to increase efficiency, decrease pollution and promote adaptability to user needs;

d) Ecosystem of excellence

i. TALENT

194. Calls on the Commission to create an AI skills framework for individuals, building on the digital competence framework, to provide citizens, workers and businesses with relevant AI training and learning opportunities and improve the sharing of knowledge, best practices, and media and data literacy between organisations and companies at both EU and national level; asks the Commission to move quickly in creating such a competence framework by building on existing AI education schemes; recommends the establishment of a European AI skills data space to support European skills training on sectoral and regional levels in all Member States; stresses that the acquisition and teaching of digital and AI skills needs to be accessible to all, in particular to women and vulnerable groups; urges the Commission and the Member States to support free online courses that enhance basic training in AI;

195. Urges investment in research to better understand the structural AI-related trends in the labour market, including which skills are in higher demand or at risk of shortage in the future to inform employee transition schemes;

196. Notes with concern the lack of targeted and systematic measures in professional training for adults; calls on the Commission and the Member States, to develop policies

including appropriate investment in the reskilling and upskilling of the workforce, including informing citizens on how algorithms operate and their impact on daily life; calls for special attention to be paid to those who have lost their jobs or are at risk of losing them due to the digital transition, with the aim of preparing them to work with AI- and ICT-related technologies; calls on the Commission to incentivise and invest in multi-stakeholder skills partnerships to test best practices; recommends monitoring the creation of quality jobs linked to AI in the EU;

197. Stresses that existing digital gaps can only be closed with targeted and inclusive measures towards both women and the elderly and therefore calls for substantial investments in targeted upskilling and educational measures to close such digital gaps; calls on the Commission and the Member States to foster a gender-equal culture and working conditions in this regard;

198. Calls for the Commission to promote gender equality in companies working on AI- and ICT-related activities, including through financing women-led projects in the digital sector and promoting a minimum number of women researchers participating in AI- and ICT-related research funding calls;

199. Stresses the need to address the talent shortage by ensuring the growth, attraction and retention of top talent; urges the Commission to follow up on its goal of having 20 million ICT specialists employed in the EU; stresses that in order to retain top AI talent and prevent brain drain, the EU needs to enable competitive salaries, better working conditions, cross-border cooperation and competitive infrastructure;

200. Emphasises the added value of having a simplified and streamlined Union framework for attracting international talent in the technology sector in order to enable talent flow and mobility within the EU and from abroad, improve international talent's access to the Union's labour market and attract workers and students on demand; highlights that new innovative tools and legislation are needed to help match employers with prospective ICT workers, address labour market shortages and facilitate the recognition of international qualifications and skills; recommends creating an EU talent pool and matching platform to serve as a one-stop shop for international talent who wish to apply for work in the EU, as well as for employers who search for potential employees abroad; calls on the Commission to expand the scope of the application of the EU Blue Card to ensure that Europe remains open to global talent;

201. Calls on the Commission to address the increased demand for remote work across Member State borders to allow EU and international employees to work remotely in a different Member State than the one they are residing in; recommends, in this context, a comprehensive review of legislative and other hurdles to remote work and addressing these in subsequent legislative proposals;

202. Emphasises the need to strengthen innovation cohesion among EU regions and across Member States, as talent can be unevenly distributed;

203. Calls on the Commission and Member States to ensure appropriate protection of workers' rights and well-being, such as non-discrimination, privacy, autonomy and human dignity in the use of AI and algorithmic management, including as regards undue surveillance practices; stresses that when AI is used at work, employers must be transparent about the way it is used and its influence on working conditions and stresses that workers should always be informed and consulted prior to the use of AI-based

devices and practices; emphasises the fact that algorithms must always have human oversight and that their decisions must be accountable, contestable and, where relevant, reversible; believes that the training of algorithm developers in ethical, transparency and anti-discriminatory issues should be encouraged;

204. Calls for a European strategy for safe AI use as regards children that is designed to inform children about interacting with AI with the aim of protecting them from risks and potential harm;

205. Calls on the Member States to make digital skills and literacy a component of basic education and lifelong learning; calls for a high-performing AI education system that fosters digital literacy, skills and digital resilience from an early stage, starting with primary education; emphasises that the development of effective curricula for digital education requires political will, sufficient resources and scientific research; calls on the Commission to promote the introduction of AI and computational competence courses in all European schools, universities and educational institutions; highlights that such skills development is needed in adult education as much as in primary or secondary education; calls for a comprehensive and consistent policy initiative from the Commission and the Member States on AI skills and education at EU level, as well as for a legislative initiative on AI in the workplace;

206. Draws attention to the need for multidisciplinary university curricula that focus on digital and AI skills, including in health, and for cross-disciplinary research centres; believes that pathways towards further education to specialise in AI (e.g. Master's and PhD degrees and part-time study) should also be emphasised;

207. Calls upon the Member States to prioritise the development of innovative teaching methods and curricula in STEM fields and programming, in particular to strengthen the quality of mathematics and statistical analysis for the purpose of understanding AI algorithms; calls on the Commission and Member States to promote STEM academic disciplines to increase the number of students in these fields; stresses that other disciplines that interact with the STEM disciplines will also be crucial for promoting digital skills;

208. Encourages the Member States to promote women's participation in STEM, ICT and AI-related studies and careers to achieve gender equality, including by defining a target for the participation of women researchers in STEM and AI projects;

209. Stresses that digital education should also raise awareness on aspects of daily life potentially affected by machine learning, including recommendation engines, targeted advertising, social media algorithms and deep fakes; stresses that digital resilience requires additional media education to help contextualise new digital and AI skills and hence calls for support towards and endorsement on new and already-existing accessible AI literacy courses for all citizens;

210. Calls for measures to ensure that every education facility has broadband access, as well as strong digital learning infrastructure; stresses the need to provide European universities and their networks with the adequate computational resources needed to train AI models, which are becoming increasingly expensive; stresses the need to ensure that teachers have necessary AI skills and tools; calls for an increased focus on technical training for teachers and the development of innovative teaching and learning tools;

211. Requests investment in youth coding skills initiatives to foster youth AI skills and high-level qualifications, including coding academies, summer school programmes and AI-specific scholarships; is of the opinion that the EU's Digital Opportunity Traineeships should be further expanded to vocational training;

ii. RESEARCH

212. Calls for the EU to increase investment in research into AI and other key technologies, such as robotics, quantum computing, microelectronics, the IoT, nano-technology and 3D printing; calls on the Commission to develop and maintain a European strategic research roadmap for AI that addresses major interdisciplinary challenges in which AI can be a part of the solution; underlines that investments should be directed to use cases that are likely to increase sustainable solutions, well-being, and inclusion in society;

213. Encourages all Member States to spend a higher proportion of their GDP on research on digital technologies; urges the continued strengthening of the Horizon Europe programme, notably its AI, data and robotics partnership and the European Innovation Council; urges the expansion of the digital Europe programme and considers that its allocated funding of EUR 7.6 billion should be increased;

214. Stresses the need to prioritise research at EU level in the field of AI; calls on the Commission to simplify the structure of research funding, including grant application requirements and processes; stresses the need to improve the quality and consistency of proposal reviews and increase the predictability of funding instruments and their timing to support long-term planning, using the European AI research roadmap; calls on the Commission to fund more applications in the field of AI by combining different instruments, such as the European Research Council, the Marie Curie Actions, the European Innovation Council and the European Institute of Innovation & Technology;

215. Calls on the Commission and Member States to prioritise funding AI research that focuses on sustainable and socially responsible AI, contributing to finding solutions that safeguard and promote fundamental rights, and avoid funding programmes that pose an unacceptable risk to these rights, including funding systems of mass surveillance, social scoring and other systems that have the potential to lead to negative social impacts, as well as technologies that contribute to environmental harm;

216. Encourages the creation of more teaching posts on AI at European universities, adequate salaries for AI research and the provision of more public funding in order to properly train and retain the current and next generation of researchers and talent and prevent brain drain; stresses the need to reduce the bureaucratic hurdles for university researchers in accessing funds easily and calls on the Commission to provide tools to increase digital interconnectivity among universities within and across Member States; urges the development of cross-cutting networks for AI across European universities, research institutions and the private sector, as well as dedicated AI multidisciplinary research centres;

217. Recommends that universities strengthen funding for applied research projects in which AI dimensions are taken into account;

218. Calls on the Commission to improve knowledge transfers between AI research and the public by setting up business networks and contact points with legal professionals and business consultants in universities, as well as by setting up citizen panels, science and

society platforms and engaging the public in the framing of AI research agendas; underlines the importance of a smooth transition from academia to industry and the added value of proximity between the two for successful and dynamic AI ecosystems and industrial centres;

219. Stresses the need to accelerate knowledge transfers in the EU from research and science to AI applications in industry and the public sector; welcomes the creation of a dedicated public-private partnership on AI; calls on the Commission to establish European AI data centres, jointly developed with industry and civil society; stresses the importance of testing sites for AI; makes specific reference to the High Performance Computing Joint Undertaking, the Key Digital Technology Joint Undertaking and the Smart Networks and Systems Joint Undertaking;

220. Calls for the establishment of AI lighthouses under the Horizon Europe framework, building on the existing and future networks of regional AI excellence centres, with the aim of building an alliance of strong European research organisations that will share a common roadmap to support excellence in basic and applied research, align national AI efforts, foster innovation and investments, attract and retain AI talent in Europe, and create synergies and economies of scale; believes that the lighthouse concept has the potential to attract the best and brightest minds from abroad, as well as bring substantial private investment into Europe;

221. Adds that the AI lighthouses, in cooperation with other research institutions and industry, should be sufficiently funded; highlights the benefits of well-contained regulatory sandboxes for the testing of AI products, services and approaches in a controlled real world environment before putting them on the market;

222. Points out that the designation of European Digital Innovation Hubs (EDIHs) under the digital Europe programme is another important step in building up an AI ecosystem of excellence based on university-industry clusters; criticises, however, that criteria for EDIH designation remain vague and thus EDIHs across Europe differ in their capabilities and development, and that the interplay with other digital hubs designated by the European Institute of Innovation & Technology and under the Horizon Europe framework remains unclear; suggests, consequently, that more coordination and effort expenditure are needed, as is the establishment of a cooperating overall cluster of decentralised AI hubs based on an EU-wide framework for legal expertise, data, funding, and incentives; welcomes the Commission's initiatives to establish start-up networks across the EU and also beyond, such as Start-up Europe and Start-up Europe Mediterranean in order to foster exchanges of ideas, business, and networking opportunities;

223. Proposes scaling up and aligning existing initiatives, such as the European Laboratory for Learning and Intelligent Systems and the Confederation of Laboratories for Artificial Intelligence Research in Europe, and flagship projects, such as the HumanE AI Network and AI4EU, in order to promote ambitious, collaborative and EU-wide research and development goals and projects;

e) Ecosystem of trust

i. SOCIETY AND AI

224. Proposes that, on top of the suggested AI training, the EU and its Member States create awareness raising campaigns, including public discussions at local level, as an additional means to reach, inform and empower citizens to understand better the opportunities, risks and the societal, legal and ethical impact of AI to further contribute to AI trustworthiness and democratisation; is convinced that this, in parallel with the creation of a clear and sound legal framework on human-centric and trustworthy AI, would contribute to reducing citizens' concerns that may be associated with widespread AI use in Europe;

225. Calls for the EU to ensure that AI development, deployment and use fully respect democratic principles, fundamental rights and uphold the law in a manner that is able to counter surveillance mechanisms and does not improperly interfere with elections or contribute to the dissemination of disinformation;

226. Stresses that governments and businesses should only deploy and procure trustworthy AI systems that are designed, where relevant, to uphold worker's rights and promote quality education and digital literacy and that do not increase the gender gap or discrimination by preventing equal opportunities for all;

227. Supports adjustments to consumer protection laws as another way to build trust in AI, for instance by giving consumers the right to know whether they are interacting with an AI agent, which would allow them to insist upon human review of AI decisions, and by giving them means to counter commercial surveillance or personalised pricing;

228. Stresses that the introduction of certain AI technologies in the workplace, such as those that use workers' data, should take place in consultation with workers' representatives and social partners; points out that workers' and their representatives should be able to request information from employers about what data is collected, where this data is stored, how this data is processed and the safeguards that are in place to protect it;

229. Calls for the EU to ensure that AI systems reflect its cultural diversity and multilingualism to prevent bias and discrimination; highlights that in order to address bias in AI, there is a need to promote diversity in the teams that develop, implement, and assess the risks of specific AI applications; stresses the need for gender-disaggregated data to be used to evaluate AI algorithms and for gender analysis to be part of all AI risk assessments;

230. Underlines the importance of continuous research and monitoring on the impacts of AI on various aspects of society, both at national and EU level; suggests that Eurostat and other EU agencies be involved in this;

231. Highlights that, based on the results of the monitoring system, a European transition fund could be considered to help manage, for example, job losses in vulnerable sectors or across regions;

ii. EGOVERNANCE

232. Calls on the Member States to deliver on the Tallinn Declaration on eGovernment, put citizens at the centre of services and put mechanisms in place to provide borderless, interoperable, personalised, user-friendly and end-to-end digital public services based on AI to all citizens at all levels of public administration; is of the opinion that the objective should be to establish the provision of digitalised and AI-based eGovernment

services to citizens over the next five years, while still providing human interaction; recalls that Recovery and Resilience Facility funds and the national recovery and resilience plans will play a key role in this regard; calls on public bodies to support and develop AI in the public sector; welcomes the revision of the eIDAS Regulation[1] and its role in boosting the provision of digital public services; stresses that no one should be left behind and that offline alternatives should always be available;

233. Calls on the Commission to renew the eGovernment action plan and create synergies with the digital Europeprogramme to support public administrations in adopting AI in line with the European open-source software strategy;

234. Highlights that eGovernment plays a significant role in the development of the data economy and digital innovation in the digital single market; notes that collaboration and the sharing of good practices throughout public administrations and across borders are vital parts of the deployment of eGovernment across the EU; calls for standardised, streamlined public administration procedures for more efficient exchanges across EU Member States and all levels of administration;

235. Notes that skilled experts are needed for the development of high-quality online services; stresses the need to increase government recruitment and training policies for digitally skilled people with knowledge of AI;

236. Calls for the implementation of the single digital gateway to be sped up and for the development of interoperable platforms that offer cross-border services in the EU to be promoted, while meeting common security standards in all Member States; stresses that a possible expansion beyond the limited set of services currently included in Regulation (EU) 2018/1724[2] establishing a single digital gateway should be considered;

237. Stresses that the public consultation platforms of EU and Member State institutions increase engagement and access to digital information; recommends investing in improvements to usability and accessibility, such as the provision of summaries and information in multiple languages, as well as in dedicated marketing and targeted outreach for digital public engagement platforms;

238. Recommends intensifying interactive and personal dialogues with EU citizens through online citizens' consultations, stakeholder dialogue formats or digital functions for commenting on EU legislation and initiatives;

iii. eHEALTH

239. Calls for human-centred design and an evidence-based approach to AI in health that focuses on personalised, patient-centred, cost-efficient and high-quality healthcare, developed in close cooperation with health professionals and patients, while upholding human oversight and decision-making; urges the prioritisation of funding, the setting of strategic goals, the fostering of cooperation and the adoption of AI applications in healthcare as a critical sector in which the opportunities offered by AI can bring

---

1 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

2 OJ L 295, 21.11.2018, p. 1.

enormous benefits to citizen health and well-being, as long as the inherent risks are appropriately managed;

240. Highlights that the uptake of AI in healthcare settings should be promoted as a tool to assist and reduce the burden on healthcare professionals, allowing them to focus on clinical tasks, and not as a replacement for healthcare professionals or as an independent actor within health systems; stresses the need to ensure a level of quality, safety and security on par with the regulatory approval process for medicines, vaccines and medical devices; asks for a clinical trial-like method to test the adequacy and monitor the deployment of AI in clinical settings; finds that it would be beneficial to evaluate which healthcare services can be ethically and responsibly automated;

241. Considers that equitable access to healthcare as a principle should be extended to health-related AI applications, including systems for the detection of diseases, the management of chronic conditions, the delivery of health services and drug discovery; emphasises the necessity of adopting appropriate measures to tackle health-related risks concerning the digital divide, algorithmic bias and discrimination, and the marginalisation of vulnerable persons or cultural minorities, who have limited access to healthcare;

242. Recalls the Parliament position that insurance companies or any other service provider entitled to access information stored in e-health applications should not be allowed to use that data for the purpose of discriminating in the setting of prices;

243. Is convinced that current EU projects and initiatives, such as EU4 Health, the European health data spaces and the European Platform on Rare Disease Registration, are steps in the right direction, as they allow Member States to pool resources, increase beneficial cooperation between health systems and enable the secure and privacy-preserving exchange of high-quality data for research and innovation;

244. Calls for the proper legal anchoring and positioning of an ‘AI in Health’ framework at Union level; underlines that many levels of risk evolve over time through the advancement of AI technologies;

245. Stresses the need for more guidance on the processing of health data under the GDPR in order to harness the full potential of AI for the benefit of individuals, while respecting fundamental rights; calls on the Commission for faster and better harmonisation of standards governing the processing, including the sharing, anonymising and interoperability, of health data across Member States;

246. Calls on the Commission to promote the integration of ethical rules at every step of the development, design and use of AI applications; stresses the need to promote further research on the methods and biases embedded in a trained AI system so as to avoid unethical and discriminatory conclusions when applied to human health data; recommends the creation of an EU Code of Conduct for processing health data in full compliance with the GDPR;

247. Calls on the Commission to consider an initiative on neurorights with the aim to guard the human brain against interference, manipulation and control by AI-powered neurotechnology; encourages the Commission to champion a neurorights agenda at the UN level in order to include neurorights in the Universal Declaration of Human Rights,

concretely as regards the rights to identity, free will, mental privacy, equal access to brain augmentation advances and protection from algorithmic bias;

248. Calls on the Commission to consider a legal framework for online medical consultations;

249. Stresses the need for measures that promote equal access to healthcare and enhance healthcare providers' uptake of AI solutions;

250. Calls on the Commission to support the establishment of a cooperation mechanism in the context and operation of a European health data space in order to foster the sharing of health data and support the development of electronic health records in line with applicable laws and regulations; urges an improvement in the quality of available data for each EU citizen by enabling digital tools to work properly (e.g. based on self-learning algorithms or big data analysis); recommends that the data stored in line with the GDPR be available for further research, as well as for the development of new drugs and individualised treatments;

251. Underlines that digital and AI skills need to be included in the education of healthcare professionals, as well as knowledge on EU data protection legislation and dealing with sensitive data, including the promotion of data anonymisation;

252. Calls for guidance regarding the applicability of liability frameworks and harmonised approval regimes for AI-based medical applications and medicines developed or tested via AI and machine learning; stresses that harm resulting from an insufficient allocation of resources or lack of care provision by means of AI recommender systems in the healthcare sector should be addressed in any future regulatory reform; emphasises that appropriate best practices, standards and criteria are needed to certify and approve healthcare applications in line with liability risks;

253. Calls on the Commission to provide and make use of human-centric predictive models for pandemics, wherein diverse data sets come together in real time to inform decision-making;

f) Industrial strategy

i. STRATEGIC PLANNING AND INVESTMENTS

254. Is convinced that the EU should place AI and the data economy at the centre of an ambitious digital industrial strategy, with the aim of empowering innovative companies and entrepreneurs to compete for the best technological and business model innovations in Europe and the world and to reinforce the EU's open strategic autonomy while establishing sound legal, ethical, technological and security standards for all AI systems and components that are intended to be used in the EU single market;

255. Encourages the Commission to use big data AI analysis to assist in performing stress tests to assess the resilience of value chains and map dependencies;

256. Urges the Commission to conduct a comprehensive strength-weakness analysis to determine the EU's vulnerabilities, identify critical areas and high-risk dependencies, establish realistic technical and economic expectations with regard to AI and assess effects across all sectors of European industry; underlines that the Commission should cooperate with relevant stakeholders to this end;

257. Suggests that the EU should, on the basis of this analysis, formulate and adopt a long-term AI industry strategy with a clear vision for the next 10 years as an extension of the Digital Compass; explains that this strategy should be complemented by a monitoring system with key performance indicators and yearly updates; stresses, however, the need to consolidate and streamline the vast number of individual initiatives that have been launched by the Commission to support the EU AI industry before incorporating them into this new AI industry strategy;

258. Calls on the Commission to consider how the overall industrial strategy can be complemented through targeted public investment; points out, however, that excessive undirected investment programmes for complex technologies may, in some cases, risk distorting the efficient allocation of capital and may lead to stranded investment; stresses, in this context, that empowering businesses, entrepreneurs and researchers to develop and market AI technology solutions based on private enterprise is a core part of the EU industrial strategy, including by enforcing a level playing field and completing the digital single market and the capital markets union; suggests facilitating access to finance, especially risk finance instruments, in particular for early-stage financing; is of the opinion that the proportion of resources devoted to AI through InvestEU and the digital Europe programme should be reviewed and, where appropriate, significantly increased;

259. Stresses the need for the swift implementation of the recently adopted EU framework for screening of foreign direct investment[1] and the recently revised regulation on the EU regime for the export control of dual-use items[2]; states that AI, as well as robotics and other digital infrastructure, should be considered a critical sector; notes that the protection of intellectual property rights and the outflow of critical technologies should be subject to stronger enforcement;

260. Stresses that it is crucial for Europe to equip itself with adequate digital infrastructure; welcomes initiatives such as the European Processor Initiative, the newly proposed Chips Act and the European High Performance Computing Joint Undertaking;

ii. SMEs AND START-UPS

261. Proposes that EU and government level support be provided to AI start-ups through access to private capital and skilled employees, the ability to procure high-quality data sets to train algorithms and the ability to scale across Member State borders; stresses further that a very effective public policy tool to support a start-up economy is the effective enforcement of competition law to prevent abuses of dominant market power and to counter barriers to market entry; underlines, in this regard, that the EU should amplify its efforts to offer SMEs and start-ups development paths and services; finds that this could also include the introduction of a ‘buddy’ system that connects experienced AI-oriented businesses with smaller businesses looking to implement the technology; stresses that the inability to afford sizeable legal teams often poses an entry barrier to complex regulatory environments for start-ups and entrepreneurs; underlines the need for SMEs to access specific legal and technical support; highlights, as well, the need to foster partnerships where AI-driven companies and those entering the market could cooperate; urges the Commission and the Member States to provide better counselling and more concrete support through networks, digital hubs, AI trainers,

---

1 OJ L 79 I, 21.3.2019, p. 1.
2 OJ L 206, 11.6.2021, p. 1.

business mentoring, site visits and legal clinics; underlines the importance of people-to people exchange programmes, such as Erasmus for Young Entrepreneurs, and that they should be further developed and encouraged;

262. Suggests easing the administrative burden for SMEs and start-ups in AI, for instance by streamlining reporting, information or documentation obligations, and by providing guidance on common procedural civil law standards to be adopted at national level; calls for the swift implementation of the single digital gateway to establish a single EU online portal in different languages containing all necessary procedures and formalities to operate in another EU country; stresses that all points of single contact established at national level should be easily accessible through the single digital gateway and should provide information and offer administrative services in the Member States, including with regard to rules on VAT and information on requirements for the provision of services, using accessible terminology and with full availability, with trained help desk staff providing effective user-friendly support;

263. Notes that potential ways in which the EU Member States can support SMEs and start-ups include: tax breaks for deep research, better access to computer capacities and high-quality data sets and support for technology scouting and AI education, training and reskilling for employees;

264. Underlines that SMEs and start-ups in AI need better access to public procurement; urges the Commission to redesign application procedures for public tenders and EU programme funding to allow start-ups and SMEs to have a fair chance of being awarded public procurement projects and research and development grants; recalls, in this regard, the successful GovTech programmes that have supported small business engagement in digital public procurement; stresses that stock option schemes for AI start-ups across Europe should also be promoted;

iii. INTERNATIONAL STAGE

265. Points out that the EU should forge and lead by example on a strong international core value-based technology alliance, working together with like-minded partners in order to establish common regulatory standards, benefit from best practices in the fields of AI, privacy rights, data flows and competition rules, and remedy strategic vulnerabilities by building on each other's assets and pooling resources in areas where it is mutually beneficial to do so; underlines that the EU should also actively support strengthened international cooperation on ethical, trustworthy and human-centric AI in relevant multilateral and bilateral forums, for example within the UN system, the OECD, the Council of Europe, the World Trade Organization, the World Economic Forum and the G20; welcomes, in particular, the establishment of the EU-US TTC, which lists cooperation on AI standards as a key priority and argues that, given its strategic potential, the TTC needs to be reinforced by an interparliamentary dimension, involving the European Parliament and the US Congress;

266. Suggests that a specific transatlantic working group on AI also be established, including representatives from governments, standardisation organisations, the private sector and civil society, to work on common standards and ethical guidelines for AI; proposes setting up a long-term platform for exchange on AI and other important digital and trade issues based on the current TTC, together with other like-minded partners;

267. Underlines that the EU should promote a socially responsible and ethical use of AI and cooperate with international standardisation bodies to further improve standards on ethics, safety, reliability, interoperability and security; welcomes recent standardisation initiatives launched by actors such as the Joint Technical Committee of the International Organization for Standardization and the International Electrotechnical Commission aiming to globally harmonise divergent AI codes; stresses, moreover, that Europe should promote and develop standards, including in the fields of smart manufacturing, the IoT, robotics and data analytics; proposes providing better support for academics, civil society and SMEs for participating in standardisation forums;

268. Supports the World Trade Organization's eCommerce initiative to develop an inclusive, high-standard, commercially meaningful, evidence-based and targeted policy to better tackle barriers to digital trade; underlines that the agreement should also reflect the principles of good governance and provide governments with the ability to counter digital protectionism, while protecting and promoting consumer trust and creating real value for the global economy;

269. Suggests that the Commission continue to address unjustified trade barriers, in particular non-tariff barriers or market access restrictions for European AI companies in third countries; stresses that trade, neighbourhood and development policy should also be actively used to shape the international debate on AI and promote European ethical AI principles;

g) Security

i. AI AND LAW ENFORCEMENT

270. Stresses the importance of law enforcement agencies' ability to identify and counter criminal activity, aided by AI technology;

271. Stresses the potential for misuse of AI in law enforcement to cause harm, including automated discrimination and unlawful treatment of citizens, while providing few means of recourse; urges the Member States to implement meaningful human oversight requirements and guarantee means of recourse for those subject to decisions carried out by AI;

272. Suggests that the EU should participate in the soft law approaches established by the UN Interregional Crime and Justice Research Institute, which has developed operational AI toolkits and started a partnership with Interpol, serving as a unique forum for dialogue and cooperation on AI between law enforcement agencies, industry, academia and civil society, fully in line with the EU data protection and privacy acquis;

273. Notes Europol's role in developing, training and validating AI tools to fight organised crime, terrorism and cybercrime in partnership with the European Data Protection Supervisor and in full respect for EU fundamental values, in particular non-discrimination and the presumption of innocence;

274. Calls on the Commission to strengthen the financial and human resources of the EU Innovation Hub for Internal Security; welcomes the efforts of Eurojust, the EU Agency for Fundamental Rights and Europol to develop a toolkit of universal accountability principles for the use of AI by justice and internal security practitioners (the AP4AI

framework); calls on the Commission to provide dedicated financial support for this initiative to promote EU accountability standards and values in the field of AI;

ii. CYBERSECURITY

275. Asks the Member States to enhance cooperation in the field of cybersecurity at the European level in order to enable the EU and the Member States to better pool resources, more efficiently coordinate and streamline national cybersecurity policies, further increase cybersecurity capacity building and awareness raising, and swiftly provide cybersecurity knowledge and technical assistance to SMEs, as well as to other more traditional sectors;

276. Encourages the EU to take the lead in developing strong cryptography and other security standards that enable trust in and interoperability of AI systems; highlights that, to create international convergence in the area of ICT risk oversight, existing international standards should be built upon and taken into account as much as possible;

277. Proposes the introduction of horizontal cybersecurity requirements based on existing legislation and, where appropriate, on new horizontal legislative acts in order to prevent fragmentation and ensure a consistent cybersecurity approach across all product groups; notes that AI products on the digital single market that carry the CE marking could, in the future, stand for both a high level of physical safety and a risk-adequate level of cyber resilience and signal compliance with relevant EU legislation;

278. Proposes that Member States incentivise cybersecurity requirements for AI systems through public procurement policies, including by making certain ethical, security and safety principles mandatory for the procurement of AI applications, in particular in critical sectors;

279. Requests that the EU Agency for Cybersecurity (ENISA) carry out sectoral security risk assessments, starting with sectors, both public and private, engaged in the most high-risk and sensitive uses of AI, and with the highest potential for negative impacts on human health, safety, security and fundamental rights; stresses that ENISA, together with the European Cybersecurity Competence Centre and the Network of National Coordination Centres, should assess cybersecurity incidents with the objective of identifying gaps and new vulnerabilities and advising the EU institutions in a timely manner on adequate corrective actions;

280. Encourages companies that use, develop or deploy AI-enabled systems active in the digital single market to develop a clear and independently evaluated cybersecurity strategy, based on its individual risk situation; encourages the inclusion of AI systems in threat modelling and security risk management; suggests that the Commission, ENISA and national authorities support this process;

281. States that cyber security requirements for AI products should cover their entire lifecycle; highlights that it has to be also clear that each company in the supply chain has to play its role in contributing to the creation of resilient AI products; points out that the new requirements should be based on the associated risk in the specific product group and the degree of influence on the risk level in order to avoid disproportionate burdens for SMEs and start-ups;

282. Proposes that existing initiatives in certain Member States, such as the German AI Cloud Service Compliance Criteria Catalogue or the Maltese AI certification programme, be taken into account for the development of an EU-wide certification scheme for trustworthy AI;

iii. CYBER DEFENCE

283. Urges the Member States to pursue an active policy of European cyber diplomacy by denouncing and attributing foreign-supported cyberattacks, including AI-powered ones, while leveraging the full toolbox of EU diplomacy; welcomes that the EU cyber toolbox includes the termination of financial aid and sanctions against those countries or proxies that engage in malicious cyber activities or hybrid, attacks including disinformation campaigns, or that sponsor cybercrimes; recognises that, to a certain degree, AI-powered cyber defence is more effective if it also contains some offensive means and measures, provided that their use is compliant with international law;

284. Suggests, furthermore, strengthening cybersecurity capabilities within the European Defence Agency, including by using AI-based systems to support a coordinated and quick reaction to cyberattacks; recommends monitoring the implementation of cyber defence policies in each Member State and assessing the allocation of relevant resources within the EU;

285. Stresses the need to analyse the impact of AI on European security and develop recommendations on how to address the new security challenges at EU level, in cooperation with the Member States, the private sector, researchers, scientists and civil society;

286. Encourages the Member States to take measures to reward vulnerability and discovery and support audits of AI-based products, systems and processes;

iv. MILITARY USE OF AI

287. Notes that any use of military AI must be subject to strict human control and oversight mechanisms, ethical principles and full respect for international human rights and humanitarian law; notes, moreover, that the EU should work with its like-minded partners on an international framework for secure research, development and use of AI-assisted weaponry that reinforces international humanitarian law, including in the context of the law of armed conflict; recalls the international norms and principles, such as proportionality in force, that have to be respected when developing and using new military technologies;

288. Notes that AI-based technologies are an increasingly important component of military equipment and strategy; stresses that exclusive military and national security uses of AI should be treated as strictly distinct from civilian use cases; recalls that issues related to emerging technologies in the military field are dealt with in the Group of Governmental Experts on emerging technologies in the in the area of lethal autonomous weapons systems, including issues related to AI, and in which EU Member States are represented;

289. Welcomes the future EU Strategic Compass that is due to provide a framework and a certain level of ambition in addressing security and defence aspects of AI; recalls that the Permanent Structured Cooperation under the common security and defence policy

and the European Defence Fund will allow Member States and the Union to enhance investments, capabilities and interoperability in the field of new technologies, including AI;

290. States that the EU should consider AI a crucial component of European technological sovereignty;

291. Concludes that the Member States should continue to train their military staff to ensure that they have the necessary digital skills to use AI in control, operational and communication systems; welcomes the European Defence Fund's approach to lethal autonomous weapons systems and its Article 10(6); highlights the importance of the European Defence Fund in supporting cross-border cooperation between EU countries in military AI research, developing state-of-the-art defence technologies and constructing the necessary infrastructure, namely data centres with strong cyber capabilities;

292. Calls on the Council to adopt a joint position on autonomous weapons systems that ensures meaningful human control over their critical function; insist on the launch of international negotiations on a legally binding instrument that would prohibit fully autonomous weapons systems; states that such an international agreement should determine that all lethal AI weapons must be subject to meaningful human oversight and control, meaning that human beings remain in the loop, and are therefore ultimately responsible for the decision to select a target and take lethal action;

293. Calls for closer cooperation with NATO in the cyber defence field and calls on NATO allies to support the multilateral efforts to regulate the military use of AI;

5. Conclusion: an urgent call for action!

294. Believes that the ongoing digital transformation, in which AI plays the key role, has triggered a global competition for tech leadership; stresses that the EU has so far fallen behind with the result that future technological standards risk being developed without sufficient EU contributions, oftentimes by non-democratic actors, which presents a challenge to political stability and economic competitiveness; concludes that the EU needs to act as a global standard-setter on AI;

295. Highlights that AI, while often portrayed as an unpredictable threat, can be a powerful digital tool and a game changer on many important aspects, including by offering innovative products and services, increasing consumer choice and rendering production processes more efficient; notes that there are clear benefits and opportunities from the adoption of AI technologies for the entirety of society, including in the fields of healthcare, sustainability, security and competitiveness; points out that, at the same time, AI technologies carry the risk of reducing human agency and substituting for human autonomy; stresses that both these benefits and risks should guide and inform regulation and public communication on AI;

296. Highlights that the EU has the potential to shape the international debate on AI and develop globally leading common rules and standards, promoting a human-centric, trustworthy and sustainable approach to AI, fully in line with fundamental rights; highlights, however, that the opportunity for consolidating such a distinctive European approach to AI on the international stage requires swift action, which is why the EU needs to agree on a joint AI strategy and regulatory framework soon; stresses that

shaping international technology norms and standards requires closer coordination and cooperation with like-minded democratic partners;

297. Stresses that currently, the EU is still far from fulfilling its aspiration to become competitive in AI on a global scale; emphasises, in this context, the importance of providing harmonised rules and standards, legal certainty and a level playing field to foster AI uptake and innovation, including by removing unnecessary administrative barriers for start-ups, SMEs and civil society; recognises that radical change of this scale impacts various parts of society differently and emphasises that the digital transition must be in full respect for fundamental rights; calls on the Commission, the Member States and Parliament, including its relevant committees, to follow up on the recommendations issued in the EU Roadmap for AI;

298. Calls for a regulatory environment for AI that provides effective governance and protection of fundamental rights, while facilitating competitive access to digital markets for actors of all size to promote innovation and economic growth for the benefit of all; underlines that a competitive, accessible and fair data economy, based on common standards, is a prerequisite for the adequate development and training of AI; points, in this context, to the risk of market concentration in the data economy extending into the economy for AI applications;

299. Concludes that advances in the EU's digital ambitions in fields such as AI require a much stronger degree of integration and harmonisation in the digital single market to promote cross-border exchange and guarantee that the same rules and standards apply across the EU; stresses, in this regard, that EU institutions need to combat abuses of market power in order to level the playing field;

300. Concludes that that necessary steps must be taken to ensure that the digital transition promotes and does not hamper the green transition; concludes that AI systems require robust infrastructure and connectivity capabilities; stresses that digital infrastructure in line with the Green Deal will target all sectors and value chains and should follow the principles of a circular economy; stresses that AI will not, however, be functional without the adequate deployment of digital infrastructure, including broadband, fibre, edge nodes and 5G; stresses the importance of mitigating increasing energy consumption and resource use to achieve climate neutral digital infrastructure by 2030;

301. Highlights that rapid technological progress introduced by AI will also affect the livelihoods of all those who do not possess the skills to adapt fast enough to these new technologies; remarks that upskilling and reskilling can help address many of the resulting socioeconomic concerns, but stresses that these impacts should also be addressed in the context of social welfare systems, urban and rural infrastructure and democratic processes; concludes that in order to promote the adoption of innovations in AI, increase the acceptance of AI-based applications and avoid leaving anyone behind, it is necessary to provide people with the means to acquire digital skills; stresses that in order to increase digital literacy and resilience, ICT- and STEM-based education needs to start at an early stage and remain accessible throughout all stages of life; finds that initiatives to establish AI ecosystems of excellence, attract AI talent to the EU and counter brain drain are of vital importance;

302. Stresses the importance of addressing AI-driven challenges to fundamental rights, thus allowing AI to effectively become an instrument that serves people and society and pursues the common good and general interest; concludes that in order to build trust in

AI among citizens, their fundamental rights need to be protected in all aspects of life, including in the context of the use of AI in the public sphere and the workplace; emphasises, in particular, the need to reflect the rights, objectives and interests of women and minority communities in the digital transition; stresses that public services and their administrative structures need to lead by example; stresses that the EU needs to accelerate the uptake of AI-based systems and eGovernance in order to facilitate the secure use of AI in public administrations; stresses furthermore that AI can unlock new solutions in the healthcare sector, if the risks are appropriately managed and equitable access to healthcare as a principle fully extends to health-related AI applications;

303. Concludes that the EU's AI strategy should not overlook military and security considerations and concerns that arise with the global deployment of AI technologies; stresses that international cooperation with like-minded partners needs to be increased in order to safeguard fundamental rights and at the same time cooperate to minimise new technological threats;

°

° °

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