European Parliament
2019-2024

Special Committee on Artificial Intelligence in a Digital Age

2020/2266(INI)

2.11.2021

DRAFT REPORT

on artificial intelligence in a digital age
(2020/2266(INI))

Special Committee on Artificial Intelligence in a Digital Age

Rapporteur: Axel Voss

PR_INI

CONTENTS

Page

MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

on artificial intelligence in a digital age
(2020/2266(INI))

The European Parliament,

– having regard to Articles 4, 26, 114, 169, 173, 179, 180, 181 and 187 of the Treaty on the Functioning of the European Union (TFEU),

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

– 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 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)[2],

– 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[3],

– 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[4],

– 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 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[5],

– 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[6],

[1] OJ L 123, 12.5.2016, p. 1.
[2] OJ L 119, 4.5.2016, p. 1.
[3] OJ L 166, 11.5.2021, p. 1.
[4] OJ L 170, 12.5.2021, p. 1.
[5] OJ L 303, 28.11.2018, p. 59.
[6] OJ L 136, 22.5.2019, p. 1.

– 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[7],

– 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),

– 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 Commission study of 28 July 2020 entitled ‘European enterprise survey on the use of technologies based on artificial intelligence’,

– 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 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 Artificial Intelligence: Main Capabilities and Disciplines’,

[7] OJ L 256, 19.7.2021, p. 3.

– 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 Artificial Intelligence’,

– having regard to the United Nations Education, Scientific and Cultural Organisation publication of 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 of 22 May 2019 on artificial intelligence,

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

– 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’,

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

– having regard to its resolution of 16 February 2017 with recommendations to the Commission on civil law rules on robotics[8],

– having regard to its resolution of 1 June 2017 on digitising European industry[9],

– having regard to its resolution of 12 September 2018 on autonomous weapon systems[10],

– having regard to its resolution of 12 February 2019 on a comprehensive European

[8] OJ C 252, 18.7.2018, p. 239.
[9] OJ C 307, 30.8.2018, p. 163.
[10] OJ C 433, 23.12.2019, p. 86.

industrial policy on artificial intelligence and robotics[11],

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

– having regard to its resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence[13],

– having regard to its resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies[14],

– 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[15],

– 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’[16],

– having regard to its resolution of 25 March 2021 on a European strategy for data[17],

– having regard to its resolution of 19 May 2021 on artificial intelligence in education, culture and the audiovisual sector[18],

– 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[19],

– 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

[11] OJ C 449, 23.12.2020, p. 37.
[12] OJ C 294, 23.7.2021, p. 14.
[13] OJ C 404, 6.10.2021, p. 107.
[14] OJ C 404, 6.10.2021, p. 129.
[15] OJ C 404, 6.10.2021, p. 63.
[16] Texts adopted, P9_TA(2021)0261.
[17] Texts adopted, P9_TA(2021)0098.
[18] Texts adopted, P9_TA(2021)0238.
[19] Texts adopted, P9_TA(2021)0405.

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 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’,

– 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 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 (A9-0000/2021),

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; stresses that today’s digital revolution is shaped by its unprecedented scale, fast convergence, and the enormous impact of emerging technological breakthroughs on states, economies and societies;

2. Observes that the digital revolution has, at the same time, triggered a global tech race, in which digital sovereignty is seen as a prerequisite for great-power status in both political and economic terms; stresses the growing realisation among decision makers that emerging technologies could lead to a global power shift away from the Western world;

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 in a new ‘winner-takes-most’ or ‘superstar’ economy; underlines the risk of European values being globally replaced, our companies becoming marginalised and our living standards being drastically reduced;

4. Highlights, firstly, that digital tools are increasingly becoming an instrument of manipulation in the hands of authoritarian states and their proxies, used to trigger a clash between political systems; explains that digital espionage, low-scale warfare and disinformation campaigns are deployed in order to pose an existential threat to our democratic societies and question the European way of life;

5. Underlines, secondly, that the EU is failing to commercialise its ground-breaking technological innovations, thereby enabling fast-growing non-European corporations to take our best ideas, talent and companies; points out that, as a result, only eight of today's top 200 digital companies are domiciled in the EU, while our economic growth is constantly declining; notes that Europe's high wages and the world's most generous social welfare systems are financially dependent on us competing with the rest of the world;

6. Warns that as a result of these and other existential threats to our democracy and prosperity, the global tech race has become a fight for survival for the EU; stresses that if the EU does not act swiftly and courageously, it will end up becoming a digital colony of China, the US and other states and risk losing its political stability, social security and individual liberties;

7. Argues that artificial intelligence (AI) is the key emerging technology within the fourth industrial revolution; notes that AI is the control centre of the new data layer that surrounds us and which can be thought of as the fifth element after air, earth, water and fire; states that by 2030, AI is expected to contribute more than EUR 11 billion to the global economy, an amount that almost matches China's GDP in 2020;

8. Explains that there is therefore a race for AI leadership within the global tech race; points out that the countries that master AI will gain key advantages; highlights, however, that AI is not a technology with magical powers but rather an efficient tool that we can put to good use; states that the rise of AI likewise does not require us to completely rewrite our laws to counter new kind of threats or to prevent intelligent machines from taking over; believes that although AI is indeed reshaping the world as we know it, the reality is much less dramatic and most developments in the field of AI are positive;

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

9. Explains that AI is actually an umbrella term that covers a wide range of old and new technologies that often have little more in common than being guided by a given set of human-defined objectives and having some degree of autonomy in their actions; 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;

10. 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;

11. Notes that in the second wave, the automated learning processes of algorithms based on the processing of large amounts of high-quality data, the ability to bring together inputs from multiple radars, lidars and cameras to form a single image of the environment, and the identification of patterns made AI systems more complex, autonomous and opaque; 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;

12. Notes that although today's AI has become much more powerful than symbolic AI, it can still only solve tasks in domain-specific niches such as chess or facial recognition and does not understand the actions it performs; points out that it is therefore referred to as 'narrow' or 'weak' AI and is still not more than a tool that provides recommendations and predictions; explains that self-driving cars operate, for instance, 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 the appropriate decisions;

13. 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 a power shift from humans to AI and create machines that could even break free from human control; stresses, however, that there are significant doubts as to whether this speculative AI can even be achieved with our technologies and scientific laws;

14. Underlines that, on the contrary, the vast majority of AI systems currently in use, are almost or even completely risk-free; refers, for instance, to automatic translations, 'Eureka machines', gaming machines and robots that execute repetitive manufacturing processes; concludes that only a very small number of use cases can be categorised as risky and that only such cases require regulatory action and effective safeguards;

15. Considers that the public debate should therefore be more focused on the enormous potential of AI; believes that AI offers humankind the unique chance to improve almost every area of our lives, from combating global societal challenges such as climate change, pandemics and starvation, to enhancing quality of life through personalised medicine, fitness programmes and assisted living;

16. Explains 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 currently preventing us from fully harnessing the benefits of AI; highlights that the case studies represent some of the most important AI use cases and, at the same time, reflect 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

17. Stresses that AI can unlock solutions in the health sector that could save millions of lives, improve our standards of living and bring a competitive edge to the European ICT sector;

18. Underlines that AI is already being used to detect diseases and abnormalities at an early

stage and more accurately through real-time pattern recognition and image processing, thus speeding up diagnosis and treatment and reducing unnecessary biopsies;

19. Highlights that AI has the potential to speed up the development of new drugs, treatments and vaccines at a lower cost, while improving the quality and overall safety of the production process; finds that AI can help predict the outcome of and responses to treatments with increasing levels of accuracy when based on high-quality data, thus increasing the effectiveness of preventive care;

20. Underlines that AI has the potential to tailor treatments and drug development to specific patient needs and enhance engagement with stakeholders and participants in the healthcare system; finds that AI and access to datasets increase the potential for healthcare professionals to better understand the patterns and symptoms of their patients and therefore provide better feedback, guidance and support;

21. 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, and heightened the need for industry and publicly funded research to be able to deploy AI to strengthen the monitoring and modelling of the spread of future pandemics, without excessive limitations on freedom of movement, the infringement of data protection principles or the risk of establishing excessive surveillance regimes;

22. Highlights the potential of AI systems to relieve healthcare systems, and especially medical staff, by supporting routine tasks such as patient transport and reminding patients of their medication, and to remedy challenges posed by rapidly ageing populations;

23. Stresses that consumer health applications based on AI can help to track an individual's health status, yield data which can apply to early triage questions and encourage healthy behaviour, thus reducing the need to seek advice from a healthcare professional;

24. Stresses that AI in the health sector is particularly dependent on large amounts of personal data, data sharing, data accessibility and data interoperability to realise the full potential of AI and health, which are currently lacking; stresses the need to combat mistrust and to educate and better inform citizens about the benefits of AI in the field of health;

25. Stresses that additional legal steps, time and purpose limitations introduced by the GDPR, and differing interpretations across Member States have led to legal uncertainty and a lack of cooperation in the health sector; underlines that specific consent obligations hinder the processing of used medical data for further analysis and studies; stresses that this leads to lengthy delays to scientific discoveries and a significant bureaucratic burden in health research[20];

26. Underlines that automatic decision-making in healthcare applications may pose risks to patients' well-being, although AI already outperforms doctors' diagnoses in several instances, such as breast cancer[21]; finds that current liability frameworks do not provide

[20] https://www.feam.eu/wp-content/uploads/International-Health-Data-Transfer_2021_web.pdf
[21] https://www.nature.com/articles/s41586-019-1799-6

sufficient legal certainty over who is accountable in the event of misdiagnosis through AI, for example;

b) AI and the Green Deal

27. Highlights that AI applications can bring environmental and economic benefits and strengthen predictive capabilities that contribute to the fight against climate change, to meeting the Sustainable Development Goals (SDGs) and to achieving our target of becoming the first climate-neutral continent; finds that the use of AI has the potential to reduce global greenhouse gas emissions by up to 4 % by 2030[22]; underlines that AI systems themselves need to be designed sustainably to reduce resource usage and energy consumption, thereby limiting the risks to the environment; finds that it has been estimated that ICT technologies are capable of reducing 10 times more greenhouse gas emissions than their own footprint[23];

28. 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 will produce 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 AI and digital solutions have the potential to scale up resource-efficient solutions that would otherwise only be implemented in one company or sector;

29. Emphasises the importance of AI in developing smart cities and smart villages to improve the technological resilience of infrastructures, building on local strengths and opportunities, including public transport, emergency assistance, waste management, urban planning, smart energy and resource optimisation; stresses that AI-based solutions can further assist in optimising architecture, construction and engineering processes to reduce emissions, construction time, costs and waste; finds that this is already a reality in countries such as China and Malaysia, where large-scale urban AI systems manage the transport, energy and safety systems of several cities;

30. Stresses that the energy transition will not take place without digitalisation, which will be achieved to a significant extent through AI; underlines that AI can monitor, optimise and reduce energy consumption and production, as well as support the integration of renewable energies into existing electricity grids;

31. 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 benefits for supply security, especially in the operation, monitoring, maintenance and control of water, gas and electricity networks, must be taken into account in the regulation of these networks;

32. Finds that AI and other digital solutions for mobility and transport have the potential to reduce traffic flows and enhance road safety, by greatly increasing the efficiency of

[22] https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652713/IPOL_STU(2020)652713_EN.pdf

[23] https://www.europarl.europa.eu/cmsdata/231743/Working%20Paper%20-%20AIDA%20Hearing%20on%20AI%20and%20Green%20Deal.pdf

access to transport systems through, for example, autonomous vehicles and optimised public transport planning, thus reducing the environmental footprint of the transport sector, travel times and costs;

33. Believes that AI can have a transformative role in the agricultural sector when it comes to tackling food security issues, enabling the emergence of new harvesting methods and harvest prediction, novel approaches to food processing and retail, agricultural resource management and input efficiency, as well as improved land management and the optimisation of food supply chains; stresses that agriculture is a key sector in which AI can help to cut emissions and the use of pesticides, fertilisers, chemicals and water; further stresses that AI can contribute to the restoration of biodiversity and prevent deforestation by monitoring endangered species and tracking deforestation activities through smart forests;

34. Stresses that AI contributes to a circular economy through increased production output and quality, reduced maintenance costs, better use and the ethical sourcing of raw materials, and reduced waste; highlights that AI has the potential to automatically provide businesses with detailed insight into their emissions, including value chains, and forecast future emissions, thus helping to adjust and achieve individual emission targets; underlines that digital tools help businesses to implement the necessary steps towards more sustainable conduct, especially small and medium-sized enterprises (SMEs) which do not otherwise have the resources to do so;

35. 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 patterns, consumer behaviour, 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

36. Is concerned that the global community does not seem likely to reach an agreement on minimum standards for the responsible use of AI, as the stakes, in particular for the most powerful nations, are too high; believes, however, as a matter of principle, in the potential of democratic nations to jointly shape the international debate, to work together towards certain minimum standards, and thereby to promote multilateralism, interoperability and data sharing on the international stage;

37. Observes that Chinese nationals have assumed leadership positions in the International Organization for Standardization, the International Electrotechnical Commission and the International Telecommunication Union, the three largest and best-established standard-setting organisations in the world, while the Chinese Government has also signed standards and cooperation agreements with 52 other countries through its Belt and Road Initiative; warns that since several of their promoted standards, including on AI technologies and in particular in relation to government surveillance and individual liberties, are not in line with EU values, the Chinese standard offensive poses a crucial geopolitical challenge for the EU, while also giving China a first-mover advantage in economic terms;

38. Stresses that AI technologies, used in military command centres or in missile launch

facilities, could escalate an automated reciprocal conflict before humans have the chance to detect what is happening, understand the causes and intervene; agrees with studies that warn that the impact of AI technologies on warfare could rival that of nuclear weapons[24];

39. Notes that the use of AI systems in defence-related developments is considered a game changer in military operations; states that the key advantage lies in the potential to engage in armed conflicts with a reduced risk of physical harm to one's own military personnel and as a means to reduce military response time;

40. Is concerned about military research and technological developments relating to lethal offensive weapon systems without human oversight that are pursued in countries such as Russia and China with little regard for the risk to humanity; observes that such lethal offensive weapon systems are already used in military conflicts; warns that even non-state armed groups could soon equip drones with AI software for navigation and facial recognition and thus turn them into cheap lethal offensive weapons capable of acting entirely without human oversight;

41. Notes that AI technology can also be used as a means for various forms of hybrid warfare; specifies that it could for instance be mobilised to trigger information warfare, by using fake social media accounts, to weaponise interdependence, by gathering valuable information or denying network access to adversaries, or to create disturbances in the economic and financial systems of other countries;

42. Illustrates that AI technologies could also help perpetrators by simplifying the use of very sophisticated cyberattacks, such as through AI-powered malware, identity theft using biometric data or adversarial AI that causes other AI systems to misinterpret input; points, in particular, to the rise in deepfakes, which already lead to doubts about the authenticity of all digital content, including genuinely authentic videos; 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;

43. Elaborates that the internet of things, as well as the fact that AI systems nowadays run a significant amount of key critical infrastructure, such as energy grids, the food chain, the ATM network and hospital logistics, has created a massive AI cybersecurity threat; predicts that states will focus more and more on protecting their IT logistics and care delivery as a domestic asset, which could in turn create the temptation to invoke 'AI autarchy';

44. Explains that the high level of accuracy that AI can achieve may pose security risks, as it can induce humans to place such confidence in AI as to trust it more than their own judgment; 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; observes that this type of AI overuse has, for example, been cited as a major factor in several aircraft crashes[25];

[24] https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf
[25] https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf

45. Highlights however that AI's core characteristics also make the technology an ideal tool to enhance security; specifies that it can be used to synthesise large amounts of data, perform behavioural analysis of network activities and detect specific patterns; stresses that these elements would allow for better prediction and assessment of the threat level, faster decision-making processes, improved reactivity and the more effective securing of endpoint devices;

46. Underlines, in particular, the potential inherent in enabling law enforcement agencies to proactively assess and predict AI misuse, as well as to counter it effectively by using AI technologies themselves; underlines that such AI-supported law enforcement activities do, however, require clear transparency rules, highly skilled employees and access to large amounts of relevant data;

d) AI and competitiveness

47. Notes that by 2030, products and services along the value chain will be interconnected and technology-driven, with AI and robotics at the core of most manufacturing processes and business models; states that this technological transformation will, however, require massive public and private investment in order to digitalise all sectors of the economy, upgrade the digital infrastructure and reskill the workforce;

48. Observes that the current funding levels are merely a drop in the ocean, which is why most European industries are lagging behind and are far from exploiting the competitive potential of AI technologies; highlights, in this regard, the fact that the EU does not have a single AI ecosystem that can compare with Silicon Valley, Boston, Toronto, Tel Aviv or Seoul;

49. Underlines that AI is a game changer for the competitiveness of EU industry as it increases productivity, accelerates innovation, makes manufacturing processes and end products safer as well as more sustainable, and could help to increase the resilience of European supply chains;

50. Points to the increasing geopolitical risk of well-established supply chains suddenly being disrupted by economic decoupling; stresses that by using AI, the EU would be able to identify problems in value chains much earlier and perform predictive maintenance, guarantee the diversification of suppliers or even bring aspects of delocalised production back to the EU;

51. Notes that companies that have initiated digital disruption have often been rewarded with disproportionate gains in market share, while the profits and revenue growth of incumbent firms have come under severe pressure; notes that recent studies indicate that this pattern is likely to repeat itself with even more intensity as companies that adopt AI tend to strongly enhance their competitive edge as compared to non-adopting firms; stresses that a two-tier economy with large numbers of bankruptcies could be the result;

52. Emphasises that this outlook is particularly concerning since the largest incumbent tech companies will likely also dominate AI technologies and could again become gatekeepers to markets, customers and innovation, 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 advertisements, their existing market dominance could, in itself, become a driver of further market dominance;

53. 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 source of innovation; observes, however, that promising AI ideas and pilots are often too slow to scale up and eventually fail to transform into impactful large-scale projects and actors, or, when they do, that they are acquired by large tech companies;

54. Stresses that the intensive use of algorithms 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, while the few AI providers that are already participating in stock trading could present a systemic risk to the financial markets by jointly triggering extreme market movements or even collapses;

55. Observes that most AI companies within the EU face legal uncertainty regarding how they can develop their products and services in an assured manner as the digital single market lacks established AI standards and norms; notes, furthermore, that overly cautious safety standards and bureaucratic burdens at a time when the success of a new AI technology is not yet foreseeable lead to non-lucrative business cases, as the initial investments that are needed are seen as too risky;

56. Points out that the increasing consolidation of the digital and physical realms, as well as of processes and services, makes it more and more difficult for AI companies to uphold quality standards; concludes that transparency and trustworthiness will decide in the future whether a product or service is eventually accepted by the market;

57. Considers that the EU's intellectual property laws do not always provide a clear and predictable framework allowing European businesses, and in particular start-ups, to adequately and easily secure intellectual property protection; notes that EU companies might often find it easier to protect their AI intellectual property rights in the US;

58. 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 absolutely crucial 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 unutilised, while a single market for data is still in the making;

59. Points also to the legal uncertainties that persist in the field of the sharing and processing of mixed and personal data; specifies that conflicting interpretations by national data protection authorities as well as non-adequate guidance on mixed data and on depersonalisation techniques have proved to be problematic for AI developers; notes, furthermore, that autonomous AI systems are also at odds with the information duties laid down in the GDPR as well as certain of its principles, including purpose limitation, data minimisation and restrictions on secondary use;

e) AI and the future of democracy

60. States that technical developments in the field of AI are very rapid and dynamic,

making it difficult for elected representatives to have sufficient technical knowledge of how new AI applications work and what kind of potential outcomes those applications could produce;

61. Warns that legislative cycles are therefore often out of sync with the pace of technological progress, while many policymakers tend to argue for categorical bans on certain AI technologies or use cases without sufficient prior analysis of the proportionality and necessity of an outright ban; is concerned that such a policy approach to AI could, on the one hand, lead to overregulation which hampers innovation and the competitiveness of EU companies and, on the other hand, even be counter-productive in terms of safeguarding security and fundamental rights;

62. Finds in this regard that using AI to acquire biometric data, by analysing fingerprints or typing cadence, or using voice or facial recognition, can be highly appropriate and beneficial for the individual as well as the general public; refers, for instance, to acts such as scanning criminal suspect databases, identifying victims of human trafficking, preventing children from watching X-rated content, penalising illegal parking and preventing welfare fraud;

63. Acknowledges at the same time that the very same AI technologies used to address fundamental societal problems and achieve important public policy goals could also pose crucial ethical and legal questions; notes that there have already been documented instances which have led to serious wrongdoing within the EU; notes that in practice, Member States rely heavily on the police to collect data, but also on private entities whose activities are often not supervised and who regularly sell the collected and highly sensitive data to other third parties; clarifies that this practice runs counter to European values and undermines the high level of fundamental rights in the EU, in particular the right to privacy;

64. Stresses that many authoritarian regimes apply AI systems to control, spy on, monitor and rank their citizens; believes that any form of unrestricted normative citizen scoring on a large scale by public authorities, especially within the field of law enforcement and the judiciary, leads to the loss of autonomy and is not in line with European values; highlights past cases of EU companies having sold biometric systems which would be illegal to use within the EU to authoritarian regimes in non-EU countries;

65. 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 and knowledge of decisional history than is possessed by public authorities or close personal advisors such as doctors, lawyers or bankers; stresses that this development challenges the sovereignty of our nation states, the foundations of our democratic systems and the safeguarding of our fundamental rights;

66. Points out that digital platforms are also used to spread disinformation, 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 create personalised and convincing messages for potential voters, who are often completely unaware that the content has been created or manipulated through

the use of AI;

67. Underlines that AI could, however, also be used to reduce anti-democratic and unethical activities on platforms and as a means to stop the distribution of fake news; notes that the effective use of AI for this purpose has so far been prevented by strongly diverging definitions of hate speech among Member States and the lack of consensus on how to harness AI to effectively filter out illegal and harmful content; explains that it is also problematic that divisive language leads to greater user engagement, which is why removal of such language would be in direct conflict with the platform's business model, based on maximising user engagement;

68. Stresses that bias in AI systems often occurs due to a lack of diverse and high-quality training data, for instance where data sets are used which do not sufficiently cover discriminated groups, or where the task definition or requirement setting themselves were biased; notes that bias can also arise due to a limited volume of training data, which can result from overly strict data protection provisions, or where a biased AI developer has compromised the algorithm; points out that some biases in the form of reasoned differentiation are, on the other hand, also intentionally created in order to improve the AI's learning performance under certain circumstances;

69. Raises the question of whether certain biases can be resolved by using more diverse datasets, given the structural biases present in our society; specifies in this regard that algorithms learn to be as discriminatory as the society they observe and then suggest decisions that are inherently discriminatory, which again contributes to exacerbating discrimination within society; concludes that there is therefore no such thing as a completely impartial and objective algorithm;

f) AI and the labour market

70. Believes that that the adoption of AI, if combined with the necessary support infrastructure and training, can substantially increase productivity, innovation, growth and job creation, with expectations of labour productivity set to increase by 11-37 %[26] by 2035;

71. Stresses that although AI may replace some tasks, including mundane, labour-intensive or dangerous tasks, it will create new, higher value-added employment; stresses that AI is currently substituting or complementing humans in a subset of tasks but that it is not yet having detectable aggregate labour market consequences[27]; stresses, however, the potential for an increase in income inequality if AI is augmenting high-skill occupations and replacing low-skill occupations, and that such possible effects need to be prepared for;

72. Highlights that AI implementation also represents an opportunity for significant cultural change within organisations, including improved workplace safety, better work-life balance and more effective training and guidance; is of the opinion that human-empowering AI applications could also create new job opportunities, in particular for those who, because of natural restrictions such as disabilities or living circumstances,

[26] https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652713/IPOL_STU(2020)652713_EN.pdf
[27] https://www.nber.org/papers/w28257

were initially bound to less qualified jobs;

73. Is concerned about AI-fuelled surveillance in the workplace and teleworking environment, as well as in the school environment, in the light of the fundamental right to privacy, data protection and the human dignity of the worker, as well as the fundamental rights of children;

74. Considers that the adaptation of the workforce in terms of AI education and retraining is of vital importance, as 52 %[28] of the current European workforce urgently requires retraining; highlights that current concepts of learning and working are still defined to too great an extent by the job market needs of a pre-digital world, which also contributes to a growing skills gap and a new digital divide for both citizens and businesses who do not have access to a secure digital space; stresses that enhancing digital literacy contributes to achieving the SDGs, in particular those on education, human capital and infrastructure;

75. 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; 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 female[29];

g) Three recurring findings in all six case studies

76. Notes that there are a number of transversal obstacles that the EU needs to overcome in order to achieve a widespread use of AI and to fully harness its benefits; states that in particular, legal uncertainty, insufficient digital infrastructure and a lack of AI skills can be observed as barriers to the successful application of AI in all fields analysed;

77. Concludes from the case studies examined, furthermore, that it is not specific AI technologies themselves that are risky, but certain use cases; points in particular to dual-use AI systems such as drones, the uses of which can vary drastically from consumer recreation to warfare, with the worst-case scenario being swarms of inexpensive, armed microdrones used to kill specific human targets;

78. States that while it is important to examine and categorise potential risks posed by AI, the case studies illustrated that AI technologies also enable us to apply, in most cases, very effective counter measures that are able to mitigate or eliminate the very same risks; underlines that, as AI is still in its early stages of development within a wider context of emerging technologies, its real potential can still only be imagined; stresses that the promise and potential benefits of AI in economic and societal terms appear to be tremendous;

[28] https://www.digitaleurope.org/wp/wp-content/uploads/2019/02/DIGITALEUROPE-%E2%80%93-Our-Call-to-Action-for-A-STRONGER-DIGITAL-EUROPE.pdf

[29] https://ec.europa.eu/info/sites/default/files/communication-digital-compass-2030_en.pdf

3. The EU's place in the global AI competition

79. Observes fierce AI competition that involves not only the two frontrunners, the US and China, but also countries such as Canada, India, Israel, Japan, Russia, South Korea and the UK; underlines that the previous chapter has already indicated that the EU is so far struggling to meet its aspiration[30] of becoming a global leader in AI;

80. Examines in the following 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 situation and investments;

a) Regulatory approach

81. Notes that the US refrains from introducing horizontal legislation in the digital field, while focusing instead on sector-specific laws and private sector innovation, in particular among its tech giants and leading universities; observes that the US approach on AI up to 2019 can therefore be summarised as providing legal guidance to businesses, investing in research projects and removing barriers to innovation;

82. 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 administration of President Biden plans to bring forward a new bill of rights to limit AI harms in 2022, the US approach will remain market-driven, aiming to avoid regulatory overreach;

83. Highlights that Chinese President Xi Jinping underlined 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 offers an opportunity to overtake the US in terms of military supremacy; 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 AI standardisation white paper further outlined how the socialist market economy can develop international standards and strategically engage in international standardisation organisations;

84. Observes that on the global stage, China actively promotes international AI partnership as a way to export its own AI-based government surveillance practices, social scoring system and censorship strategies; emphasises that heavy investment abroad under the Digital Silk Road initiative are also used as a means to spread Chinese AI globally and to bring other countries under Chinese influence; concludes that the Chinese approach is therefore built upon deploying AI domestically as well as exporting AI technologies that follow predetermined standards that are in line with the ideology of the Chinese Communist Party;

85. Notes that the Commission started its work on regulating AI in 2018 by publishing the

[30] https://ec.europa.eu/commission/presscorner/detail/en/speech_21_1866

European AI strategy, setting up a High Level Expert Group and introducing a coordinated plan[31] 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[32], which was presented with a revised coordinated plan on AI[33] in April 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;

86. Emphasises that central to the EU regulatory approach is a strong attention to ethical considerations in line with core human rights values and democratic principles; underlines that the Commission thereby hopes to achieve another GDPR-like 'Brussels effect', meaning that the EU's regulatory and market power leads to a competitive edge in AI; states that establishing the world's first regulatory framework for AI could indeed leverage a first-mover advantage in setting international AI standards based on European values, as well as successfully exporting 'trustworthy AI' around the world;

b) Market situation

87. Is aware that that the vast majority of the 100 leading AI companies globally are domiciled in the US, whereas only three Chinese companies and four EU companies fall into this category[34]; notes that the US also leads in the total number of AI start-ups, hosting 40 % of all new AI companies, followed by the EU with 22 % and China with 11 %[35];

88. Points out that in recent years, many of the EU's most successful digital companies have been acquired by US tech giants; refers also to the ongoing debate about so-called 'killer acquisitions'; notes that US firms, with 130 acquisitions in 2020 alone, acquired many more AI companies than EU and Chinese firms combined, which made 30 and three comparable acquisitions respectively;

89. 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 only 7 % of all EU companies are currently using AI technologies, while just 30 % are planning to do so in the future[36]; states that there is also a clear gap in AI readiness between different business sectors as well as among Member States, with southern and eastern Europe lagging behind, while northern Europe is, in general, very advanced, even by global standards;

90. Underlines 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 fragmented and features

---

[31] European Commission, Coordinated Plan on Artificial Intelligence (COM(2018)0795).

[32] 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).

[33] 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).

[34] https://www.analyticsinsight.net/top-100-artificial-companies-in-the-world/

[35] https://asgard.vc/wp-content/uploads/2018/05/Artificial-Intelligence-Strategy-for-Europe-2018.pdf

[36] https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20210413-1

many barriers; stresses that the development of AI products and services is further slowed down by the existence of 27 different national AI strategies and the fact that the EU's AI assets such as talent, capital and research are spread widely across the continent;

91. Points also to the problem that inconsistencies in EU law, contradictions between EU and national laws, different legal interpretations and a lack of enforcement among Member States is putting European companies in operational and financial jeopardy as they cannot determine whether their AI innovations are later likely to be assessed as non-compliant with EU law;

92. Notes that the insufficient legal certainty for AI companies is further exacerbated by the fact that common standards and norms are missing in some sectors, while others are compromised by overregulation or the presence of legislative proposals that have been pending for long periods of time without being adopted; highlights as an example the fact that EU AI developers face a data challenge that neither their US nor Chinese counterparts do; observes that they often do not have enough high-quality data to train their algorithms, struggle with strict data protection rules and are affected by a lack of sectoral data spaces and cross-sectoral interoperability, as well as constraints on cross-border data flows;

c) Investments

93. Points out that although private investments in the EU AI industry are rising strongly, with EUR 3.4 billion invested in 2018, the investment gap compared with the US (EUR 31 billion) and China (EUR 21 billion) has grown further[37]; states that the US is also leading in venture capital and private equity funding, which is particularly important for AI start-ups, with EUR 12.3 billion, against EUR 4.8 billion for China and EUR 1.2 billion for the EU; notes that as a consequence, many European AI entrepreneurs are crossing the Atlantic to scale up their businesses in the US;

94. States that together with national initiatives, the estimated annual public investment of the EU in AI of EUR 1 billion is also much lower than the EUR 5.1 billion invested annually in the US and up to EUR 6.8 billion in China[38]; states, however, that between 2017 and 2020, EU public funding for AI research and innovation increased by 70 % compared to the previous period; acknowledges that the Commission plans to increase investment further through the digital Europe programme, Horizon Europe, the European Structural and Investment Funds (ESIF), the European Investment Fund (EIF), the Recovery and Resilience Facility and various cohesion policy programmes[39];

95. Stresses that AI companies within the EU have problems finding qualified employees as 42 % of the EU population lacks basic digital skills[40]; points out that the EU also struggles with AI-relevant university degrees, as the number of bachelor's degrees

[37] https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000505746/%28How%29_will_the_EU_become_an_AI_superstar%3F.pdf
[38] https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000505746/%28How%29_will_the_EU_become_an_AI_superstar%3F.pdf
[39] European Commission, A Europe fit for the digital age - Excellence and trust in artificial intelligence (2021)
[40] https://digital-strategy.ec.europa.eu/en/policies/desi

awarded in ICT is decreasing while the number of postgraduate degrees awarded is 50 % lower than in the US; underlines that the EU also faces a cybersecurity skills gap, with more than 350.000 experts needed; recognises that US and increasingly also Chinese companies have a clear advantage in attracting and retaining AI talent from the rest of the world;

96. Observes that although the EU still has an excellent community of researchers who are producing many AI research papers that are often cited and downloaded, the EU's global impact is steadily declining, with a brain drain of top EU researchers to the US and China[41]; notes that the EU only spends 2 % of its GDP on research and development (R&D), while the US spends 2.8 %; emphasises that the total R&D spending of US software and computer services firms in 2019 was EUR 100 billion, which is much higher than comparative figures in China and the EU, where private R&D spending amounted to EUR 20 billion and EUR 12.5 billion respectively;

97. Notes that the EU's digital infrastructure is underdeveloped, with just 25 % of people in the EU being able to connect to a 5G network, compared to 76 % of people in the US[42]; observes that the EU in general lacks high-performance digital infrastructure with interoperable data spaces, affordable energy supply, high transmission rates and volumes, reliability and short delays as well as a genuine AI ecosystem with excellence clusters such as can be found in the US or China[43];

d) Conclusion

98. Concludes that the US is still the overall leader in AI as it is ahead in almost every category, in particular when it comes to market power, investment, AI talent, research and infrastructure; highlights, however, that China, which five years ago was still significantly lagging behind the US in all indicators, is now quickly catching up in almost every category; notes that China could in fact achieve its goal of becoming the global leader in AI by 2030 or even earlier; recognises that both countries have the advantage of a unified single market, greater flexibility in digital governance and stronger political commitment to remaining a leader in AI;

99. Stresses that the EU is behind the US and China in virtually every category and that despite its current measures, it is losing further ground; notes that the EU is, however, ahead on regulatory approaches; points out that a viable EU strategy for becoming more competitive on AI would be to quadruple efforts to catch up when it comes to AI research and innovation, skills, infrastructure and investment, while at the same time trying to create a first-mover advantage by establishing a future-oriented and innovation-friendly regulatory framework for AI development and use;

100. Underlines that the EU's efforts to strengthen its global AI footprint were severely set back by Brexit, as the UK was one of the leading EU countries in AI with London as one of the EU's most important AI hubs, home to 1.000 AI companies, 35 tech hubs and reputed research centres such as the Alan Turing Institute;

---

[41] https://datainnovation.org/2021/01/who-is-winning-the-ai-race-china-the-eu-or-the-united-states-2021-update/

[42] https://www.ft.com/content/d2fd9b8a-fddc-4c90-ad11-2d05c542d10b

[43] Working paper of the AIDA Committee on AI and Competitiveness.

101. Concludes that the EU is currently on the losing side, far from fulfilling its aspiration of becoming a global leader in AI; maintains that there is still a small window of opportunity to change this situation, even though it will close very soon; states that the special committee therefore proposes to swiftly implement the following EU Roadmap for AI;

102. 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 that a political process be launched with the aim of pulling all Member States in the right direction and drastically improving the performance of those that are lagging furthest behind; refers in this regard to the EU 2000 Lisbon agenda, which, despite the criticism, played a part in guiding the EU's policy orientation over 20 years and in keeping up the pressure on Member States to reform;

4. EU Roadmap for AI: how to become a global leader

a) Favourable regulatory environment

i. LAW-MAKING AND AI

103. Calls on the Commission to propose only 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 swiftly adaptable, principle-based and future-proof, while adopting a risk-based approach; stresses, furthermore, the importance of legal certainty and, consequently, the need for robust, practical and unambiguous applicability criteria, definitions and obligations in all legal texts;

104. Highlights the principle of proportionately in the EU Treaties, which determines that any proposed means of intervention must be proportionate to the stated goals, without being overly prescriptive or invasive; states that new digital laws in areas such as AI must therefore find the right balance and prevent unnecessary new administrative burdens for SMEs, start-ups, academia and research; considers that 'as much as necessary, as little as possible' should serve as the guiding principle for the regulator;

105. Believes that the Better Regulation Agenda is a key element for making the EU AI-strategy a success; calls on the Commission and the co-legislators to commit to drastically reducing the number of new EU legislative acts and to instead shift their focus to the review, adaptation, implementation and enforcement mechanisms for existing laws; proposes that the REFIT platform, together with a comprehensive group of stakeholders such as the European AI Alliance, be used to evaluate the suitability of legislation in the light of changing contexts;

106. Urges the Commission to perform more in-depth impact assessments with adequate foresight and risk analysis, prior to issuing any new digital proposals in areas such as AI and across the different DGs; emphasises that, by default, impact assessments should systematically map and evaluate all existing horizontal and sector-specific legislation, as well as all ongoing proposals under negotiation that could be relevant to AI and other digital technologies;

107. Underlines the particular relevance for new AI legislation of the New Legislative Framework, the GDPR, the ePrivacy Regulation, the Platform-to-Business Regulation, the Data Governance Act, the Open Data Directive, the Cybersecurity Act, the NIS Directive, the Law Enforcement Directive, the Product Liability Directive and the Digital Services Act, as well as the Directives on Unfair Commercial Practices, Unfair Contract Terms, Consumer Rights, the Sale of Consumer Goods and Price Indication;

108. Finds that both the Council's general approach and Parliament's first reading position should also undergo rigorous impact assessments before the inter-institutional negotiations start; proposes that the co-legislators institutionalise a structured dialogue on AI with the European AI Alliance and with the EU-level bodies that have a role in the implementation of the law, for instance through the issuance of guidelines or the development of common standards;

109. Calls for the Parliament, the Commission and the Council to reduce 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 in question and its market relevance; requests, in this regard, a review of Annex VI of the Rules of Procedures of the European Parliament and specifies that the entire process of establishing and attributing the competences of standing committees needs to be revised;

110. Is convinced that Parliament should process horizontal files on topics such as AI exclusively in new ad hoc committees with legislative powers; states that each of these ad hoc committees, named in alignment with the political priorities of the Commission, such as 'Europe fit for the digital age', would exist for the whole political term, incorporate MEPs from all standing committees and work on all digital legislative files;

ii. GOVERNANCE AND ENFORCEMENT

111. Calls for the creation of an adequately resourced mechanism to supervise the uniform, EU-wide implementation and enforcement of the upcoming AI laws; prefers a European AI Board over the creation of a costly new EU Agency for AI; suggests, however, that this board should be made up of not only the national AI supervisory authorities and the European Data Protection Board (EDPB), but also a broad range of relevant EU bodies, such as the EU Agency for Fundamental Rights, the High-Level Expert Group on AI, the EU Agency for Cybersecurity, the European Consumer Consultative Group, and standardisation organisations the European Committee for Standardization, the European Committee for Electrotechnical Standardization and the European Telecommunications Standards Institute;

112. Highlights the need to learn from GDPR flaws such as its low-compliance rate by realising that just focusing on ex post controls by courts and regulatory agencies will only scratch the surface of the legal challenges posed by emerging technologies; concludes that the 'pacing problem' requires the EU to combine ex ante and ex post approaches by complementing its legislative toolbox with alternative governance approaches that are able to deliver much quicker, more adaptable and more effective solutions; supports, therefore, the increased use of regulatory sandboxes, private-public partnerships, standards and certification;

113. Explains that regulatory sandboxes would give AI developers the unique chance to experiment in a fast, agile and controlled manner outside the strict application of regulatory rules, but under the supervision of competent authorities; notes that these regulatory sandboxes would be experimental spaces in which to challenge existing legislation, detect regulatory obstacles to innovation and test, under real-world conditions, new business models that could potentially achieve more significant benefits and higher levels of user protection than those on which the original regulations were based;

114. Explains that private-public partnerships such as the European Alliance for Industrial Data, Edge and Cloud are another promising governance approach; elaborates that this approach would enable the EU's AI ecosystem to operationalise its principles, values, objectives and industrial interests at the level of software code, making compliance binding by design, but at the same time keeping the set of protocols flexible enough for technological advances;

115. Explains that any new digital laws in areas such as AI should also go hand in hand with the promotion of consensus-based and industry-led voluntary standards; warns, however, that the EU should avoid the fragmentation of standards, discrepancies with international standards and overlaps with sectoral standards; proposes, therefore, that EU standardisation organisations be used as a platform to translate the essential requirements, determined by digital legislation in areas such as AI, into product-specific and state-of-the-art technical standards and design instructions; notes that these could then be combined with labelling schemes as a way to build consumer trust and develop, for instance, a European AI brand that stands for trustworthy services and products;

116. Explains that an open certification platform could also establish an ecosystem of trust that involves governments, civil society, businesses, accounting firms and other stakeholders; explains that such certificates would license AI developers and producers to operate while also validating that they provide secure digital products, technologies and services throughout their entire lifecycle; notes that such an approach would allow for up-to-date and technology-specific minimum standards to be maintained, while facilitating the continuous adaptation of certificates and verification information based on the newest technological developments observed by approved platform subscribers;

iii. LEGAL FRAMEWORK FOR AI

117. Highlights that the underlying objective of the EU's digital strategy, as well as that of the AI strategy is to create a 'European Way' in a digitalised world; clarifies that this approach should be human-centred, value-oriented and based on the concept of the social market economy; underlines that the individual, with their respective dignity and individual freedoms, should always remain at the centre of all political considerations;

118. 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, covering high-level ethical standards combined with appropriate liability rules and sector-specific provisions, while at the same time providing the private sector with enough flexibility, practicability and legal certainty to develop new business models based on AI technologies;

119. States that the co-legislators should aim to align the AI definition in future legislation with the concepts, terminologies and standards developed together with other like-minded democratic countries in the OECD[44]; stresses that doing so would give the EU an advantage in shaping a future international AI governance system;

120. Is convinced that it is not AI as a technology that should be regulated, but that the type, intensity and timing of regulatory intervention should solely depend on the type of risk incurred by the use of an AI system; underlines, in this regard, the importance of distinguishing between a minority of 'high-risk' and the vast majority of 'low-risk' AI use cases; concludes that while only the former category indeed demands legislative safeguards, businesses should self-regulate 'low-risk' technologies by choosing measures that deliver the best outcomes;

121. Specifies that the classification of technologies as 'high-risk' should be based on the concrete use and context, complexity and autonomy of the AI system, the probability and likelihood of the worst-case scenario, the severity of the harm and its irreversibility, the techniques used and the governance arrangements adopted; stresses that this classification should be introduced together with best practices and guidance for AI developers and should also recognise that AI technologies can significantly reduce certain risks;

122. Notes that the requirements that AI systems need to fulfil differ significantly in a business-to-business (B2B) environment compared to a business-to-consumer (B2C) environment; points out that while consumer rights need to be legally protected through consumer protection legislation, companies can solve liability and other legal challenges more quickly and cost-effectively by contractual means with business partners directly; concludes that, in particular, SMEs and start-ups investing in AI technologies would benefit from a B2B exclusion as they are disproportionately affected by new legal obligations, which also harms their ability to attract investments;

123. Underlines the need to address open ethical questions raised by new technological possibilities, but clarifies that new AI ethical guidelines should not set up stricter rules than those already existing for human or automated actions; proposes that on these grounds the EU should introduce ethical guidelines that consist of three categories of core values and principles;

124. Explains that the first category could list fundamental, mandatory principles such as the non-maleficence principle, the principle of respecting human dignity or the protection of the democratic process; states that the second category could include good practices in AI development such as human-centric AI, responsible governance and the principles of transparency and explainability; concludes that the last category could include principles of sustainable AI that would be fully aligned with the UN 2030 Agenda for Sustainable Development;

125. Highlights, with regard to the third category, the gap in leadership on AI global governance, which gives the EU the chance to become the leading voice in aligning AI with the UN SDGs and using AI technologies to push worldwide for their achievement;

[44] Recommendation of the OECD Council on artificial intelligence of 22 May 2019.

stresses, however, that not all AI technologies developed or applied in the EU should need to comply with all three categories; suggests, for example, that sustainable AI could only be mandated for AI implemented or procured by public tender or in specific sectors, while the majority of AI developers and companies would only be encouraged to align with the second and third categories through soft law;

126. Is convinced that efforts to completely ‘de-bias’ AI algorithms are frequently misguided, because this strategy wrongly suggests that bias-free data sets exist; notes that in this regard the requirement that data used to train AI systems is ‘complete and free of errors’ needs to be revisited; stresses, however, that the EU should at the same time cooperate very closely with AI developers to counterbalance structural biases in our societies and daily life;

127. Elaborates that transparency or explainability obligations for AI systems, while helpful in certain cases, may not be possible to implement in every instance; notes that both concepts also need to be balanced against other factors, including the interests of businesses in maintaining trade secrets or the potential value of exposed data to potential competitors; stresses, however, that a mandatory self-identification of AI systems or accessible machine logs seem to be very useful for many AI use cases that interfere with the fundamental rights of individuals or affect consumers;

128. 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 and new forms of patent licensing to ensure that tools are available to regions and initiatives that could not otherwise afford them; recognises that it will also be necessary to clarify whether AI will be able to hold intellectual property rights in itself;

129. Elaborates that obligatory *ex ante* risk self-assessments, comparable with CE markings or data protection impact assessments, combined with market surveillance based on clear rules and standards, and complemented with ex post enforcement for high-risk AI systems, seem to be a sufficiently robust governance approach for AI; warns that overly burdensome conformity assessment obligations could create significant burdens that make the business models of AI developers and companies economically unviable;

130. Notes that in order to increase product safety and improve the identification of faults, the developers of high-risk AI should at least be obliged to ensure that accessible logs of algorithmic activity are maintained securely; considers that developers should also design high-risk AI systems with embedded mechanisms – ‘kill switches’ – for human intervention to immediately halt automated activities at any moment;

131. Is convinced that despite the legal challenges caused by AI systems, there is no need for a complete revision of the existing liability rules; stresses that the Product Liability Directive and the national fault-based liability regimes can in principle remain the centrepiece legislation for countering most harm caused by AI; underlines that only in some cases could there be inappropriate outcomes, but warns that any revision should take the existing product safety legislation into account and should solely be based on clearly identified gaps;

132. 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, do however seem necessary to ensure that compensation is available for harm caused by emerging technologies; stresses, however, that an overly broad approach to the definition of ‘product’ should be avoided, as this may make it difficult to differentiate between AI and other algorithms;

133. Points out that, due to the characteristics of AI systems, such as their autonomy and opacity, there could also be cases where neither an updated Product Liability Directive nor national fault-based liability regimes apply and where persons who suffer harm or whose property is damaged would end up without compensation; suggests, therefore, the introduction of a limited new liability mechanism for legal claims against the operator, who controls the risks associated with the AI system and who also often is the cheapest cost avoider; specifies that while high-risk AI systems should fall under strict liability, combined with mandatory insurance cover, victims of low-risk AI systems should only benefit from a presumption of fault against the operator;

iv. EU DATA CHALLENGE

134. Agrees with the conclusion drawn by the Commission in its 2020 communication entitled ‘A European strategy for data’ that the creation of a single European data space is key to ensuring the EU’s global competitiveness in AI, as well as its strategic sovereignty and economic prosperity; recalls the essential link between the availability of high-quality data and the development of AI;

135. Highlights, however, that EU data governance is currently highly uncoordinated; asks the Commission, therefore, to streamline its various policy and funding streams, to rectify existing overlaps and to present a consistent overall system that ensures seamless data flows as well as the protection of user rights; proposes that solutions that leverage decentralised data analytics and edge architectures also be prioritised, as these could be more cost-efficient, resilient and sustainable alternatives to the structures currently in place;

136. Stresses the key importance of opening data silos and fostering access to data for AI researchers and companies; underlines the need to establish the required legal certainty and technical infrastructure, while also motivating the European industry to make better use of the large amounts of available but unutilised data, and ceasing to cede most of the value generated to dominant platforms; considers that voluntary data sharing between businesses based on fair contractual arrangements and triggered by incentives such as subsidies or tax breaks would help to achieve this goal;

137. Recommends interoperability be further strengthened and consensus-based, industry-led common standards be established in order to guarantee that the free movement of data between different machines and entities can take place in an innovative manner; notes that besides open standards, open source software, creative commons licenses, open codes and open application programming interfaces (APIs) can also play a key role in accelerating data sharing;

138. Calls on 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 interfering with contractual freedom; underlines that a single European data space will require companies to be allowed to closely cooperate with each other, and therefore considers that safe harbours and block exemptions on cooperation for data sharing and pooling, as well as more guidance for businesses on competition law matters from the Commission, are needed;

139. Calls on Member States, with regard to government-held data, to quickly implement the Open Data Directive, making high value datasets available 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;

140. Calls on the Commission to ensure that GAIA-X is scaled up into the European Alliance for Industrial Data, Cloud and Edge'; stresses that a GAIA-X, which is coherently linked to the mechanisms in the alliance and which establishes a 'compliance by design' mechanism based on EU legislation, could become the blueprint for setting up common European data spaces; notes that an updated EU Cloud Rulebook would also help to translate common EU principles and values into actionable processes and checks for technical practitioners;

141. 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 internet of things (IoT) machines, and in particular the rights to access to data, to data portability, to urge another party to stop using data, and to correct or delete data;

142. Takes note of the Commission's 2019 practical guidance on how to process mixed datasets[45]; underlines, however, that in practice further specifications concerning the distinction between personal and non-personal data, as well as the definition of 'inextricably linked', seem necessary; points out that not sharing any commercial datasets continues to often be the best option for AI researchers and companies due to the complexity of the existing rules and significant legal uncertainty as to whether data is sufficiently anonymised;

143. Considers WP 216 on Anonymisation Techniques of the Article 29 Working Party to be insufficient in practice; proposes instead the introduction of a clear legal basis, guidelines based on specific use cases and relevant situations for different types of data processors, and 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 modern AI systems show in experiments that they nevertheless manage to re-identify a person;

144. Suggests, therefore, 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,

[45] https://digital-strategy.ec.europa.eu/en/library/practical-guidance-businesses-how-process-mixed-datasets

certifications for truly high risk applications, personal information management systems, and the use of synthetic data also show promise;

145. Calls for a limited revision of the GDPR to replace or reinterpret some of its key concepts, such as purpose limitation, data minimisation, the obligation to provide information or processing records, restrictions on secondary use and informed consent, as a way to make data protection laws more applicable to autonomous and self-learning AI; proposes in this regard the replacement of the concept of data minimisation with the concept of data sovereignty, which would allow users to make sovereign decisions about the use of their data; underlines that the ePrivacy proposal discussed does not include any reference to the current legislative efforts on AI and focuses solely on consent and data minimisation; stresses, in this regard, that a new impact assessment should be conducted with a focus on the proposed changes to the current regime and on technologies that had not yet been developed during the previous legislative term in 2016;

146. Calls for a push for a uniform implementation of the GDPR across the EU by making the consistency mechanism compulsory and by streamlining the diverse national interpretations of the law; finds that there is also a need to reduce the frequent use of opening clauses in the GDPR, to better equip data protection authorities, and to clarify unambiguously in the law that data protection is not an absolute fundamental right but should instead be balanced with other fundamental rights and interests, such as the right to life, liberty and security, the freedom to conduct a business and the freedom of the press;

147. 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;

148. Stresses, in this regard, that the free flow of data and metadata across international borders is a crucial enabler for digital innovation in Europe; calls on the Commission to therefore refrain from imposing data localisation requirements, except in limited, proportionate and well-justified cases where such a policy is in the interest of the EU or necessary to uphold our high European standards;

149. Calls on the Commission to decisively respond to the ruling of the Court of Justice of the European Union that the EU-US Privacy Shield is invalid by creating an alternative workable system that respects the requisite safeguards, but also simplifies EU-US data flows again; calls on the Commission to continue pursuing data adequacy talks with other third countries, as this is the best way to promote privacy policies of the EU and allow the international exchange of data;

150. Asks the Commission to honour the risk-based approach to security measures set out in Articles 25(1) and 32(1) of the GDPR and thus to not require standard contractual clauses to ensure advanced encryption and full unreadability of personal data at every stage of the processing of data outside the EU; notes that researchers and companies in areas such as AI should not be obliged to undertake ‘mini-adequacy’ assessments for each of their data transfers; stresses that requiring researchers and companies to assess

the laws of the country of destination themselves and, on that basis, to decide which safeguards would be the most appropriate, is not feasible in practice;

151. Encourages, furthermore, the stronger use of codes of conduct, binding corporate rules and certification mechanisms as potential alternatives to adequacy decisions and standard contractual clauses; asks the EDPB to issue more guidance for researchers and companies in areas such as AI on how to use those mechanisms to effectively process personal data outside the EU in a GDPR-compliant way;

b) Completing the digital single market

i. NATIONAL AI STRATEGIES

152. Calls on the Member States to review their national AI strategies that they developed in accordance with the 'coordinated plan on AI', as the vast majority of them remain vague and lack clear goals; recommends that they formulate more concrete, quantifiable and specific actions, while trying to create synergies between them;

153. Calls upon the Commission to help Member States to set priorities and strongly align their national AI strategies 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 companies would face major obstacles if they are subject to different operating parameters and regulatory obligations in each of the 27 Member States;

ii. MARKET BARRIERS

154. Urges the Commission to continue its work on removing key barriers for developers and companies in areas such as country-based discrimination, burdensome market access procedures and high regulatory costs, as well as to address the frequent use of derogations which results in diverging rules among different Member State jurisdictions;

155. Underlines the need to swiftly conclude the legislative negotiations on all pending legislative files that aim to complete the Digital Single Market; proposes to focus in particular on telecom networks and the logistic aspects of cross-border e-commerce;

156. Calls upon the Commission to strictly enforce the rules of the Single Market as the number of infringements by Member States is constantly on the rise; believes that the enforcement of these rules should not depend on political considerations but instead solely on legal grounds; finds that the focus of the EU institutions should in general shift from creating new obligations to the effective enforcement of the existing rules;

157. Notes that the New Legislative Framework (NLF) should be carefully updated and aligned with digital products and services; proposes to focus on modernising and simplifying compliance procedures by introducing digital alternatives to paper-based procedures;

158. Supports the introduction of a Digital Euro in the form of tokenised central bank money issued by private sector intermediaries, as a complementary payment instrument,

supervised by the European Central Bank and the national central banks, as well as an integrated European payment platform, with high security standards to support pan-European digital payment services and solutions, pre-empt unfavourable initiatives from third countries or large platforms, and to avoid becoming dependent on foreign services;

159. Encourages the Commission to tackle barriers faced by offline businesses wishing to go online; underlines, however, that those barriers are not only policy-related but also related to demand-side issues such as language and cultural differences; proposes information campaigns and better market surveillance as a means to increase the trust as well as knowledge of European consumers;

iii. LEVEL PLAYING FIELD

160. 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, as well as to better address the risks of new emerging monopolies without compromising innovation;

161. 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, while also improving the practical and actual control over data, introducing clear rules of conduct for market-dominant platforms and increasing legal certainty for cooperation in the digital economy;

162. States in this regard that the Commission should adapt its market definition practices and merger rules to define markets more accurately and in line with modern market realities in the digital sector, taking account of global market conditions and adopting a dynamic analysis and long-term view to assess the existence of competitive pressures; stresses that allowing mergers and other deals between EU companies more often could be a key element in boosting European AI companies' growth and scale up;

163. Calls upon the Commission and national competition authorities to increase their efforts of monitoring digital markets on an ongoing basis, identifying competitive constraints and competition bottlenecks, and subsequently imposing more frequently remedies on companies that abuse their dominant position or that engage in anti-competitive behaviour; notes that it is crucial that the principle of "same activities, same risks, same rules" is respected by all market players;

164. Calls upon Member States to substantially increase the funding 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 ought to speed up abuse proceedings and, where necessary, apply interim measures to prevent the negative impact of infringements and to avoid markets from tipping while at the same time guaranteeing the procedural defence rights of companies;

165. Welcomes the new OECD tax deal as it is a balanced instrument that will establish a fair and more effective taxation approach towards globally active digital companies; calls upon Member States to swiftly sign the multilateral convention and implement it;

c) Digital green infrastructure

i. CONNECTIVITY AND COMPUTING POWER

166. 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 reach climate neutrality; finds that the allocation of EUR 2.07 billion in funding for digital infrastructure under the Connecting Europe Facility (CEF)[46] is insufficient;

167. Stresses that the shift in the volume and processing of data for AI requires the development and deployment of new data processing technologies encompassing the edge, thereby moving away from centralised cloud-based infrastructure models towards increasing decentralisation of data processing capacities; urges the strengthening of European intense-computing AI architectures as a key strategic priority to maximise investment and research, including distributed clusters, the deployment of edge nodes, digital microcontroller initiatives, and the capacity to enable faster data collection and processing in all aspects of society;

168. Stresses that AI requires powerful hardware to make sophisticated algorithms useable, including high-performance and quantum computing and the IoT; urges the maximisation of funding and research for such AI-enabled emerging technologies; finds that, similarly, nano-technologies and chips are essential to enabling AI to be embedded in, for example, medical devices, which also requires priority funding;

169. Highlights that a functioning and fast infrastructure for AI must be based on a fair, safe and high-quality foundation by avoiding gaps in digital high-speed connectivity, which requires 5G roll-out in all urban areas by 2030, as well as ultra-fast broadband networks and spectrum policy with licence conditions that do not distort competition; urges Member States to continue to implement the 5G toolbox, specifically enabling legislation related to the risk assessment of suppliers and service providers; calls for the Broadband Cost Reduction Directive to be put into practice to facilitate network deployment;

170. Calls on the Commission to establish timetables and financial incentives for Member states, cities, regions and industry, and to accelerate the administrative approval processes for 5G; supports the incentivisation of private investment in 5G roll-out; requests that in regions where roll-out is not carried out by the private sector, more funds are made available; calls for funding for broadband and connectivity projects under the multiannual financial framework, with easier access for local authorities to avoid the underutilisation of public funds;

171. Calls on the Commission to establish a precise strategy with a clear timetable for 6G roll-out to better prepare for the next wave of digital infrastructure, enabling Europe to take the lead;

[46] Regulation (EU) 2021/1153 of the European Parliament and of the Council of 7 July 2021 establishing the Connecting Europe Facility and repealing Regulations (EU) No 1316/2013 and (EU) No 283/2014, OJ L 249, 14.7.2021, p. 38.

172. Finds that it will not be possible to achieve the necessary deployment of dense edge-node connectivity for 5G in rural areas, where half of European households are not even connected through fibre; 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; recommends that European Investment Bank support for connectivity projects in rural areas be enhanced;

173. Stresses that the significant investment required for network deployment, coupled with the ambitious expectations of public authorities and consumers regarding roll-out timing and coverage, will be impossible to achieve without infrastructure-sharing agreements, which are also key to promoting sustainability and reducing energy consumption;

ii. SUSTAINABILITY

174. Urges the EU to take the lead in making green digital infrastructure climate neutral and energy efficient by 2030; calls for coordinated global multilateral action to use AI in the fight against climate change and environmental degradation;

175. Highlights the need for clear rules and guidelines for environmental impact assessments for AI; calls for a circular economy plan for digital technologies and AI in particular to incentivise companies to reduce the carbon footprint of data centres and devices; stresses the need to ensure that the processes associated with AI products and services do not have undue sustainability impacts; recommends fostering the use of AI-based solutions such as digital twins in all sectors, to coordinate sustainable standards for businesses and to enable the monitoring of energy efficiency, collecting information on emissions and product lifecycles;

176. Calls on the Commission to launch competitions and missions for AI solutions tackling specific environmental problems and to strengthen this component in Horizon Europe;

177. Believes that supporting and fostering the application of codes of conduct to enable the integration of sustainability data sets into already existing data space activities or upcoming data spaces at local, cross-sectoral or cross-country level should become a guiding principle; stresses the need to define principles to ensure that relevant climate and sustainability data can be integrated when setting up new sustainability data spaces;

178. Calls on the Commission to set up and support testing facilities where AI applications can be tested on their sustainability performance and to offer experience on how to improve the environmental footprint of these applications, including autonomous vehicles; encourages the adaptation of existing testing facilities to focus on use cases in circular production;

179. Calls on the Commission to invest in and cooperate closely with the private sector in order to create lighthouse projects in volunteering smart cities, where all available state-of-the-art technologies including AI are combined and where real-life tests are constantly conducted, covering smart buildings, smart grids, connected cars, mobility platforms, public services and logistics; supports the development of an ‘EU Smart City App Store’ as a common collection of projects and applications that other cities can adopt; urges the effective mobilisation of cohesion policy and for AI in an urban context to be addressed specifically;

180. Calls on the Commission to promote and invest in coherent sustainable transport infrastructure that uses AI built on best practices in order to optimise transport systems to increase efficiency, decrease pollution and promote adaptability to user needs;

181. Urges the use of AI to monitor energy consumption in municipalities and develop energy efficiency measures; calls on the Commission to incentivise the outsourcing of data to energy efficient data centres;

d) Ecosystem of excellence

i. TALENT

182. Calls on the Commission to create an AI competence framework for individuals that builds on the digital competence framework for citizens, which helps individuals and SMEs to find relevant AI training and learning opportunities and to improve the sharing of knowledge, best practices, digital skills initiatives and funding between organisations and companies, at both EU and national level; recommends the establishment of a central body for the European AI skills data space to coordinate European skills training on sectoral and regional levels in all Member States; urges the Commission and the Member States to support free online courses that enhance digital literacy such as basic training in AI;

183. Calls on the Commission, in cooperation with the Member States, to develop policies for the re-skilling and up-skilling of the workforce in AI for all generations and all forms of employment by drawing on existing public-private cooperation initiatives to provide for a regular solutions-oriented policy dialogue; calls on the Commission to incentivise and invest in multi-stakeholder skills partnerships to test best practices; highlights the need for digital and AI skills to be included in life-long learning initiatives; is of the opinion that Member States need to give up legislative competences in this area and consequently calls for a comprehensive and consistent legislative initiative from the Commission on AI skills and education at EU level;

184. Urges engagement in horizon scanning to gain an understanding of which skills will become less relevant and which will be in higher demand or at risk of shortage in the future; believes that this will enable a more targeted policy to help workers transition between jobs or acquire necessary new skills, to anticipate the new skills that workers may need and to foster the development of those skills in a timely manner;

185. Calls for a high-performing AI education system that fosters digital literacy, skills and digital resilience from an early stage, starting with primary education; calls on the Commission to promote the introduction of mandatory AI and computational competence courses in all European schools, universities and educational institutions; stresses that digital resilience, including awareness of deep fakes, requires additional media education that helps to contextualise new digital and AI competences;

186. Is convinced that in order to help raise awareness of and skills related to AI, the use of AI tools for (off- and online) services directed towards EU citizens should be announced and explained in full transparency, with short communication material adapted to the target audience, especially children; calls for a European strategy for better and safer AI for children, in line with the European strategy for a better internet

for children, designed to empower children while also protecting them from risks and potential harm;

187. Calls for action to ensure that every education facility has broadband access as well as strong digital learning infrastructure; stresses the need to ensure that teachers have the necessary AI skills and tools to provide a digital learning environment; calls on the Commission to support technical training for teachers and the development of innovative teaching and learning tools;

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

189. Calls on the Commission to support the development of innovative solutions such as AI-based intelligent tutorial systems; asks that universities be provided with grants to develop AI concepts and programme them together with education technology (EdTech) companies;

190. Requests investment in youth coding skill initiatives to foster 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 (DOT), further expanded to vocational training, could provide cross-border opportunities to get hands-on working experience in AI jobs;

191. Calls on the Commission to promote and increase the funding for STEM (academic disciplines to increase the number of students in these fields; underlines that women and minorities should be encouraged to pursue STEM-related educational and professional opportunities such as vocational training; stresses that other disciplines that interact with the STEM disciplines will also be crucial for promoting digital skills;

192. Stresses the need to train talent in AI at all levels and to address the talent shortage by ensuring 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, and to close the gender gap in this sector; stresses that AI skills and talent need to be fostered in all sectors including health, transport, energy and agriculture; stresses that in order to retain top AI talent and prevent brain drain, the EU needs to enable competitive salaries, working conditions, cross-border cooperation and a competitive innovation infrastructure;

193. Stresses that the acquisition and teaching of digital and AI skills needs to be accessible to all; stresses further that EU policies must strive to remove obstacles to the participation of women and other discriminated groups in the digital economy and empower them to take the lead as tech investors and entrepreneurs; requests an incentive system to encourage companies to ensure their teams of developers and engineers include gender balance and minority inclusion;

194. Stresses that within the EU, most AI talent is located in Western Europe with fewer resources in other regions; emphasises, therefore, the need to strengthen innovation cohesion among EU regions and Member States;

ii. RESEARCH

195. Calls for the EU to increase investment in research into key technologies such as AI, robotics, quantum computing, microelectronics, batteries, the Internet of Things, nano-technology, distributed ledger technology and 3D printing; calls on the Commission to develop and maintain a European strategic research roadmap for AI which includes major interdisciplinary challenges where AI can be a part of the solution;

196. Encourages all Member States to spend a significant proportion of their GDP on research into digital technologies, and for annual combined public and private investments in the EU to reach at least EUR 20-25 billion; urges the continued strengthening of the Horizon Europe programme, notably its AI, data and robotics partnership and the European Innovation Council, and to expand the digital Europe programme, whose allocated funding of EUR 7.6 billion[47] is insufficient to remain competitive;

197. Calls on the Commission to simplify and streamline the structure of research funding instruments by reducing the effort and time needed to obtain decisions when applying for grants; stresses the need to improve the quality and consistency of proposal reviews and to increase the predictability of funding instruments and their timing to support long-term planning, using the European AI research roadmap;

198. Encourages the creation of more chairs on AI at European universities as well as competitive salaries for AI research and the provision of more funding in order to properly train and retain the next generation of researchers and entrepreneurs and prevent brain drain to locations outside the EU; stresses the need to reduce the bureaucratic burden for university researchers in accessing funds and calls on the Commission to provide tools to increase digital interconnectivity between universities; urges the development of cross-cutting networks for AI across European universities and research institutions;

199. Calls on the Commission to improve knowledge transfer between AI research and the business world by setting up business networks, regulatory sandboxes and contact points with legal personnel and business consultants in universities;

200. Stresses the need to accelerate knowledge transfer in the EU from research and science to AI applications in industry and the public sector; recommends the creation of a dedicated public-private partnership (PPP) on AI; calls on the Commission to establish European AI data centres, jointly developed by government and industry and using strong encryption to protect the stored data in an appropriate manner; stresses the need to support the development of large-scale testing sites for AI; calls on the Commission to provide financial incentives at EU level to launch pilot projects in Member States;

201. Supports strongly the establishment of an AI lighthouse under the Horizon Europe framework, which would be the continent’s pioneering centre of excellence for AI research and development; notes, however, that the EU and the Member States should commit to a long-term and much more substantial investment plan in the region of EUR

47 https://ec.europa.eu/info/strategy/eu-budget/performance-and-reporting/programmes-performance/digital-europe-programme-performance_en

1 billion per year over the next 10 years; adds that the AI lighthouse would be an excellent place to create regulatory sandboxes, meaning time- and space-limited areas for experimenting with, testing and finessing specific AI applications that carry some risk but also have high potential for public good;

202. 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, the fact that the hubs are dotted across the continent and that the interplay with other digital hubs designated by the European Institute of Innovation & Technology (EIT) and under the Horizon Europe framework remains unclear; suggests, consequently, that more coordination is 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;

203. Proposes to scale up and align existing mission such as ELLIS, platforms such as CLAIRE and flagship projects such as HumanE AI and AI4EU with the goal of promoting ambitious, collaborative and EU-wide research and development goals as well as projects; explains that a single AI mission with clear milestones and regular evaluation would attract the most talented researchers, bringing them together to address the biggest scientific questions in AI;

e) Ecosystem of trust

i. SOCIETY AND AI

204. Proposes that on top of the suggested AI training, the EU and its Member States should create awareness raising campaigns, including public discussions at local level, as an additional means to reach, inform and empower citizens to understand better the capabilities, limitations and impacts of AI;

205. Underlines the added value of establishing monitoring mechanisms at national and EU level to continuously analyse, measure and score the social impact of AI; explains that those mechanisms could help us to keep track of the positive and negative impacts that AI has on our society and allow us to adapt or redirect our AI strategies and policies; suggests that Eurostat and other EU agencies be involved in order to guarantee high quality outcomes;

206. Highlights that this monitoring mechanism might illustrate that the transformation initiated by AI technologies will lead to such radical changes to our lives and habits that the EU might in turn need to rethink further elements of our normative framework, adapt certain social and environmental principles or even establish a fully-fledged European transition fund, helping to manage, for example, new social gaps or temporary job losses in vulnerable sectors; underlines, however, that potential additional costs during this area of adjustments do not ‘kill the case’ for AI as the positive effects of AI will strongly outweigh the costs in the medium to long term;

207. Supports adjustments to consumer protection laws as another way to build trust in AI, for instance by giving consumers at least in some cases the right to know whether they are subject to algorithmic decision-making or if they are interacting with an AI agent,

allowing them to insist upon human review of AI decisions or giving them means to counter commercial surveillance or personal pricing;

ii. eGOVERNANCE

208. Calls on Member States to deliver on the Tallinn Declaration on eGovernment and put mechanisms in place to provide borderless, interoperable, personalised, user-friendly, and end-to-end digital public services based on AI to all individuals and businesses at all levels of public administration; is of the opinion that the objective should be to increase the number of people that use eGovernment services, with a focus on AI, to up to 80 % of all EU citizens over the next five years;

209. Calls for collaborative ecosystems for developing AI eGovernment tools that include both suppliers and local governments; supports efforts to harmonise eGovernance structures and calls for standardised, streamlined public administration procedures for more efficient exchange across EU Member States and all levels of administration; calls on the Commission and Member States to further promote the use of AI in support of evidence-based and reliable legislation;

210. Calls on the Commission to renew the eGovernment action plan and use it together with the digital Europe programme as a common legal framework to support all central public administrations and as many local administrations as possible in fully adopting AI wherever it is beneficial and feasible and in line with the European open-source strategy;

211. Calls for a common platform for eGovernance where AI solutions and best practices can be offered and exchanged within and among EU administrations; stresses that platforms enable fast and economical sharing of open-source software within administrations down to the local level that can be shared across the EU in a user friendly way;

212. Stresses the need to focus government recruitment and training policies on bringing digitally skilled people with deep knowledge of AI into administrations as well as the judicial sector;

213. Calls for the implementation of the digital single gateway to be sped up and for the development of interoperable platforms that offer cross-border services in the European Union to be promoted, while meeting common security standards for all services in all Member States; supports expansion beyond the limited set of services currently involved in the single digital gateway act;

214. Stresses that governments and businesses should only deploy and procure trustworthy AI systems that are designed to be respectful of the law and fundamental rights, are aligned with ethical principles, are socio-technically robust and are able to counter surveillance;

215. Calls on the Commission and the Member States to strengthen online connectivity to political decision-making processes, as well as user engagement and analysis, in order to strengthen political participation based on AI; urges for the public consultation platforms of EU and Member State institutions to increase digital information and engagement; 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;

216. Recommends intensifying the interactive and personal dialogue with EU citizens through AI tools via online citizens' consultations, stakeholder dialogue formats or digital functions for commenting on EU legislation and initiatives;

217. Supports the development of digital voting systems based on AI to make elections more accessible, auditable, efficient, secure and transparent, while still providing analogue voting options and preserving analogue voting result backups;

iii. eHEALTH

218. Calls for human-centred design and an evidence-based approach to AI in health that focuses on patient-oriented and high-quality digital healthcare and that seeks consumer and user feedback throughout the development process; calls on the Commission to set the global tone on cutting-edge healthcare and well-being, placing the benefits of AI at the centre of policy-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;

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

220. Stresses the need for sector-specific legislation for health data in order to seize the full potential of AI; calls on the Commission to harmonize governing rules across Member states for the sharing, processing, standardising, curating, anonymising, interoperability and collaborative use of health data; finds that the objective should be to provide all involved actors (e.g. doctors, hospitals, health companies) with all necessary personal health data without identifying a specific patient;

221. Stresses the need for measures and incentives that enhance health care providers' potential to scale up the uptake of AI solutions and share them with others; calls on the Commission to provide interoperable data architectures adapted to local needs for countries to adapt to digital solutions and AI;

222. Calls on the Commission to support the setup and operation of a European health data space in order to foster the sharing of health data; supports the establishment of a central health data entity at EU level to select standards and profiles for interoperability, as well as a health data entity in each Member State to implement those standards;

223. Call on the Commission to promote the integration of ethical rules at a very early stage in the development and design of AI applications; stresses the need to promote further research on the methods and bias embedded in a trained AI system so as to avoid unethical and discriminatory conclusions when applied to human health data; recommends to create an EU Code of Conduct for processing health data;

224. Urges to create the legal and technological basis for a European Digital Health Ledger as a system to protect individual information by not identifying the respective person, while at the same time improving the quality of available data for each European citizen by allowing digital tools to work properly (e.g. based on self-learning algorithms or big data analysis); recommends that the data of this system should be stored in pseudonymised form in Open Data Trust Centres and should be available for further research as well as the development of new drugs and treatments;

225. Finds that it is necessary to determine which health care services can be ethically and responsibly automated; stresses that it must be ensured that automated decisions cannot be influenced, altered or modified by malicious parties;

226. Calls for a clear liability framework and harmonised approval regimes for AI-based medical applications and medicines developed or tested via AI and machine-learning; urges that practical best practice regulation, standards and criteria are needed to certify and approve health care application in line with liability risks;

227. Calls on the Commission to create a sector-specific chapter on health in the GDPR to ensure the processing of data for scientific purposes in healthcare; stresses the need to reduce the obligation for additional consent, when using AI in medical research; calls on the Commission to update data protection rules so that an "opt-out" alternative is considered sufficient when personal data is used by public bodies or in public-private partnerships to train and develop AI applications for purposes of public good;

228. Calls on the Commission to provide and make use of people-centric predictive models of pandemics with diverse data sets coming together in real time to inform decision-making;

229. Requests a legal framework for online medical consultation and promote the interconnectivity between European health entities by using international accepted standards (e.g. FHIR, SNOMED) in order to facilitate best practices and evidence-based treatments;

230. Underlines that digital and AI skills, need to be included in the education of health care professionals, as well as skills in applying data protection legislation and dealing with sensitive data, including the promotion of data anonymisation;

f) Industrial strategy

i. STRATEGIC PLANNING AND INVESTMENTS

231. Is convinced that the EU should implement an ambitious AI industrial strategy, that attempts to reduce the EU's dependence on non-European hardware, software and services while establishing sound ethical, technological and security standards for those elements that are not produced in the EU or where the purchasing of imports makes more sense from an economic point of view; declares that this approach does not aim to make the EU protectionist, but to strengthen its role as a champion of international cooperation and trade;

232. Encourages the Commission to use big data AI analysis to increase transparency,

perform stress tests to assess the resilience of value chains, map dependencies, warn about future supply bottlenecks, diversify suppliers and reshoring some aspects of production back to the EU; warns however that the EU should not nationalize or territorialize supply chains or endorse types of AI sovereignty as these approaches regularly lead to major economic setbacks;

233. Urges the Commission to conduct a comprehensive strength-weakness-analysis to determine the EU's vulnerabilities and high-risk dependencies, establish realistic technical-economic expectations with regard to AI and assess the effects across all sectors of the European industry; underlines that the Commission should thereby cooperate closely with business alliances and multi-stakeholder initiatives;

234. Continues that the EU should, on the basis of this analysis, formulate and adopt a fully-fledged AI industry strategy combined with a 10-year vision and a concrete rolling action plan; explains that this strategy should be complemented by bold missions, clear timetables, adequate governance and a monitoring system with key performance indicators and yearly updates;

235. Stresses the need to firstly consolidate and streamline the vast number of individual initiatives that were launched by the Commission to support EU industry, before secondly, incorporating them into the new AI industry strategy; warns that so far there is a chaotic system of overlapping sector-specific as well as horizontal policies whereas many of them feature contradicting timelines, indicators, definitions or targets;

236. Calls on the Commission to add a genuine investment strategy to the overall digital industry strategy, aiming at achieving an optimal balance between public and private investments; suggests to establish new mechanisms that facilitate access to finance, more risk-tolerant investment strategies in new ideas (early-stage financing) and the creation of a specific AI investment fund, which is managed by leading investors and overseen by a multidisciplinary advisory board comprising of both scientists and business leaders;

237. Holds that the proportion of resources devoted to AI within the InvestEU and Digital Europe Programme should be reviewed and strongly increased;

238. Stresses to strongly support the recently adopted common framework for the screening of foreign investments but underlines that sensitive technologies with potential dual-use applications must be better protected; states that AI should be considered a critical sector that deserves protection through the investment-screening mechanism; continues that the protection of intellectual property rights as well as the outflow of critical technologies, in particular in partnerships with Chinese firms and research bodies, should become subject of much higher scrutiny;

ii. SMEs AND START-UPS

239. Proposes to offer an alternative to the buy-out vision of many AI start-ups by ensuring that government support is provided at all stages of their development; underlines in this regard that the EU should amplify its efforts at offering SMEs and start-ups development paths and services, especially by promoting the use of digital tools, developing AI transition plans and further expanding the exchange of best practices;

urges the Commission and the Member States to provide better counselling and more concrete support through networks, digital hubs, AI trainers, business mentoring and site visits;

240. Stresses that it needs to be worth for SMEs and start-ups to invest in AI research as well as in human resources; notes that tax breaks for doing research, better access to computer capacities and datasets, an EU-Visa scheme for tech-talents, temporary support in technology scouting or in paying the salaries of AI specialists, and state aid exemptions in the area of AI education, training and reskilling of employees are potential ways of how the EU and Member States can help;

241. Suggests to ease the administrative burden for SMEs and start-ups in AI, for instance by reducing extensive reporting, information or documentation obligations, and by harmonising the civil procedure law; proposes also the establishment of a single EU online portal in different languages concerning all necessary procedures and formalities to operate in another EU country, of a single point of contact in the home country that can certify the company's eligibility to provide services in another EU country as well as of a standardized EU-wide VAT declaration in the respective native language;

242. Underlines that SMEs and start-ups in AI need better access to public procurement and venture capital; notes in this regard that, similar to the USA, the EU should establish a new mind-set by promoting the continuous search for the 'next big thing' on AI; stresses that stock option schemes for AI start-ups across Europe should also be promoted as they would allow European founders to compete with their non-EU counterparts by selling a share of their idea to high-skilled employees;

243. Calls for the creation of a dedicated EU stock exchange that is sought along the lines of NASDAQ as this would allow fast-growing technology companies to finance themselves in Europe instead of migrating to the USA for scaling up;

iii. INTERNATIONAL STAGE

244. Points out that the EU should forge a strong international core value-based AI technology alliance, working together with like-minded partners in order to overcome regulatory divergence in the fields of privacy rights, data flows or competition rules and to remedy strategic vulnerabilities by building on each other's assets and pooling resources in areas where it is mutually beneficial to do so;

245. Welcomes the EU-US Trade and Technology Council (TTC) as a platform to deepen the partnership and collaboration, to develop compatible standards and to ensure the security of critical supply chains; suggests to establish in addition a specific transatlantic working group on AI, including representatives from government, the private sector and civil society to work on common standards and ethical guidelines for AI; wishes in this regard also to continue a close EU-UK cooperation on AI;

246. Stresses that the EU should leverage its regulatory power as well as industrial and technological capabilities to advance the European approach on AI in multilateral fora and international bodies such as the United Nations, the OECD, the WTO, the WEF and the G20;

247. Supports the WTO's eCommerce initiative to develop an inclusive, high-standard, commercially meaningful, evidence-based and targeted policy to better tackle barriers to digital trade including AI; underlines that the agreement should also reflect 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;

248. Points out that the EU should act as first-mover with regard to ethical guidelines and standards on AI and identify respective gaps in international standards in order to prevent countries like China or Russia to push for international standards that are not compatible with European standards and values;

249. Calls on the Commission and the Member States to increase their participation in international standardisation forums; proposes to provide better incentives and support to academics, civil-society and SMEs for participating in standardization forums as the related costs and travel expenses are often high, while recognition is rather low;

250. Encourages the uptake of recent standardisation initiatives from actors such as the Institute of Electrical and Electronics Engineers (IEEE) and the Joint Technical Committee (JTC) of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), which are both aiming to globally harmonise divergent AI codes;

251. Suggests that the European Commission continues to address unjustified trade, in particular non-tariff barriers, or market access restrictions for European AI companies in third countries as well as infringements with regard to intellectual property rights; stresses that trade, neighbourhood and development policy should also be actively used to shape the international debate on AI and to promote European ethical principles on AI;

g) Security and military deterrence

i. AI AND LAW ENFORCEMENT

252. Considers it to be of paramount importance for the safety and security of citizens that law enforcement agencies are well advanced in AI development, making full use of the potential of digital technologies to prevent and investigate serious crimes through real-time facial recognition in select locations; underlines that diligently developed algorithms for crime prevention and investigation, based on highly qualitative data, may provide a higher level of efficiency, neutrality and legal certainty than human law enforcement agents, and should thus be promoted;

253. Warns of the grave consequences of limiting law enforcement agencies' use of state-of-the-art technology in a time when organised crime increasingly has access to sophisticated technology, becomes increasingly violent, and operates across borders; asks instead for the inclusion of AI applications for law enforcement purposes in the category of high-risk AI systems, ensuring that sufficient safeguards are put in place;

254. Suggests that the EU should furthermore participate in the soft law approaches established by the United Nations Interregional Crime and Justice Research Institute

(UNICRI), which has developed operational AI toolkits and started a partnership with Interpol, serving as a unique platform for dialogue and cooperation on AI between law enforcement agencies, industry, academia and civil society;

ii. CYBERSECURITY

255. Asks Member States to confer competences in the field of cybersecurity to the European level in order to enable the EU 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;

256. Proposes to Member States to enforce cybersecurity requirements for AI systems through public procurement policies by making certain ethical and safety principles mandatory for the procurement of AI applications in certain critical sectors;

257. Requests to enable ENISA to perform sectorial security risk assessments, starting with industries engaged in the most high-risk and sensitive uses of AI, and with the highest potential of negative impacts on human health, safety, security and fundamental rights; stresses that ENISA, together with the European Cyber-security Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, should also be instructed to assess cybersecurity incidents as well as to review the latest AI-cybersecurity research with the objective to identify gaps and new vulnerabilities and timely advise the EU-institutions on adequate corrective actions;

258. Encourages every AI company that is active in the Digital Single Market to develop a clear and independently evaluated cybersecurity strategy, based on its individual risk situation; encourages furthermore to include AI systems into threat modelling and security risk management; suggests that the Commission, ENISA and national authorities support this process by establishing a common interactive platform that shares best practices, lists the latest vulnerabilities, provides legal advice and facilitates the sharing of cybersecurity relevant data between AI companies;

259. Proposes the introduction of horizontal, product-centred and mandatory cybersecurity requirements based on the principles of the New Legislative Framework (NLF) as only a new horizontal legislative act can avoid fragmentation of cybersecurity requirements, while at the same time, guaranteeing a consistent cybersecurity approach across all product groups; notes that AI products on the Digital Single Market that carry the CE marking would as a result stand for both a high level of physical safety as well as a risk-adequate level of cyber-resilience;

260. States that mandatory cyber security requirements for all digital and in particular AI products should cover the entire lifecycle from development, e.g. code testing and verification, to maintenance, e.g. patching and updates, until the end of its lifetime; 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; suggests that there should be a close corporation with the private sector in order to make the requirements relevant to the market and keep them up-to-

date with the pace of technological change as well as the evolution of threats;

261. Continues that the certification schemes developed under the EU Cybersecurity Act could complement the mandatory requirements of the new horizontal legislation; proposes to take also the existing initiatives of certain Member States for an EU wide certification schemes for trustworthy AI, such as the German AI Cloud Service Compliance Criteria Catalogue (AIC4) or the Maltese AI certification program, into account;

262. Encourage the use of strong, globally accepted and deployed cryptography and other security standards that enable trust and interoperability in AI systems; highlights that to create international convergence of ICT risk oversight, the alignment of all cybersecurity legislation with existing international standards and industry best practices is of utmost importance;

iii. CYBER DEFENCE

263. Urges Member States to pursue an active policy of European cyber diplomacy by denouncing and attributing foreign-supported AI-powered cyberattacks, while leveraging the full toolbox of EU diplomacy; advises that this should include diplomatic responses, the termination of financial aid and sanctions against those countries or proxies that engage in malicious cyber activities or that sponsor cybercrimes; believes that the EU, in close cooperation with NATO, should consider using AI to execute cyber counter-strikes against repeat offenders;

264. Suggests furthermore the creation of an EU Cyber Defence Agency with executive powers as a way to establish a centralised EU body that has the competences to develop and implement clear EU-wide procedures based on AI for a coordinated and quick reaction to cyber-attacks, covering measures in the political, economic, diplomatic and military domain; notes that this new agency should also monitor the implementation of cyber defence policies in each Member State, have the oversight of the entire EU cyber defence architecture and assess the allocation of relevant resources within the EU;

265. Proposes that the EU should also establish a European Security Commission on AI incorporating representatives from Member States, the private sector, and civil society; explains that this Security Commission should analyse the impact of AI on European security and develop recommendations on how to address the new security challenges;

266. Encourages to use white hats, meaning hackers that seek to identify vulnerabilities so they can be fixed, while also using hackers to form 'red teams' that are deployed to attack the systems; notes that such teams could test various AI tools that are already in use for malicious purposes and by doing so, providing constructive insights on existing AI systems and applications;

iv. MILITARY USE OF AI

267. Notes that exclusive military and national security uses of AI should be exempt from civilian AI legislation, since overregulation in the field of security and defence could pre-emptively restrict the EU’s capacity to innovate and deploy AI technologies, placing it at a disadvantage to its adversaries that do not have such constraints;

268. Continues that the EU should therefore consider AI as a crucial component of European strategic autonomy, which could significantly enhance the detection, protection, and preparation capabilities against security and defence threats; underlines that not using AI systems for military aspects means to decrease the EU's security level and also hamper the ability of EU militaries to remain interoperable with US forces;

269. Concludes that Member States should train their military staff to ensure that they have the necessary digital skills to use AI in control, operational and communication systems as well as to use AI in lethal defensive AI weapons with a human in the loop or on the loop; highlights the importance of the European Defence Fund to support cross-border cooperation between EU countries in military AI research, to develop state-of-the-art defence technologies and to build up the necessary infrastructures, namely data centres with strong cyber capabilities;

270. Calls upon the EU institutions to push for a combination of dynamic soft law mechanisms and a legally binding international treaty to address the concerns in relation to lethal offensive AI weapons with no human oversight; states that within the international agreement, it should be determined that all lethal AI weapons must be subject to meaningful human oversight and control, meaning that human beings remain either in the loop or on the loop, and are therefore ultimately responsible for the decisions to select a target and to take lethal action;

271. Underlines that the NATO alliance should be used to deter other countries from using lethal offensive AI weapons with no human oversight and to develop a multilateral strategy to effectively sanction those countries that do not join the international treaty but instead further advance the development, production and use of lethal offensive AI weapons with no human oversight;

5. Conclusion: an urgent call for action!

272. Believes that the ongoing digital transformation, where AI plays the key role, has triggered a global tech race that will determine the future political and economic power status of the European Union; urgently stresses that the EU is so far falling further and further behind in this race with the result that current technological standards are being actively developed and determined outside of Europe, presenting an existential threat to our democracy and prosperity; concludes that in order to remain both competitive and a global power, the EU needs to become a global leader in AI;

273. Highlights that AI, while often portrayed as an unpredictable threat, is in reality a powerful digital tool that is already a game changer in core fields that bring benefits for the good of society, including in our aspirations to combat climate change, provide innovate healthcare, revolutionise employment, strengthen our security and democratic systems and boost our competitiveness on a global scale; stresses that these benefits should guide and inform regulation and public communication on AI;

274. Highlights further that the EU, with its regulatory and market powers, has the potential to shape the international debate on AI and to push for common standards for the ethics-driven, sustainable and trustworthy development and use of this technology, fully in line with European principles and values; highlights, however, that the window of opportunity for consolidating such a distinctive European approach to AI on the

international stage is closing fast, which is why the EU needs to join forces and agree on a joint AI strategy, including a balanced regulatory framework, very soon;

275. Stresses that currently, the EU does not meet any of the preconditions that would allow us to fully capture the potential of AI, especially compared to the AI frontrunners China and the US; finds that a lack of legal certainty, access to and sharing of high-quality data, harmonised rules and standards, funding, research, skills and infrastructure for core technologies, as well as high regulatory burdens, have led to a situation in which the EU's competitiveness is constantly decreasing; is convinced that only by executing a bold and comprehensive EU Roadmap for AI will the EU manage to catch up; states that Parliament needs an ad hoc digital committee with legislative powers in order to be able to respond effectively to these horizontal challenges, ; notes that as long as this committee is not established, clear competences among existing committees need to be defined in order to enable them to follow up effectively on all specific parts of this Roadmap;

276. Concludes that it is the EU's responsibility to quickly set up a favourable regulatory environment for AI that provides for swift digital law-making, effective governance and balanced ethical standards, while at the same time preventing overregulation and giving enough leeway for innovation; urges that the adequate development and training of AI will require better access to high-quality data, common standards and incentives for voluntary data sharing; calls on its Committees on Legal Affairs (JURI), Internal Market and Consumer Protection (IMCO), Industry, Research and Energy (ITRE), Civil Liberties, Justice and Home Affairs (LIBE), and Constitutional Affairs (AFCO) to ensure that these goals are met;

277. Concludes that our digital ambitions in fields such as AI can only be achieved through a fully integrated and fully harmonised digital single market that promotes cross-border exchange and that guarantees that the same rules and standards apply to all AI researchers and companies across the EU; stresses in this regard that the EU also needs to target abuses of market power in order to level the playing field; calls on the Economic and Monetary Affairs (ECON), IMCO and JURI Committees to guarantee this;

278. Concludes that AI systems require robust infrastructure and connectivity; stresses that digital green infrastructure which is in line with the Green Deal will target all sectors, including agriculture, electricity, housing, transport, businesses, value chains and the circular economy; stresses that AI will not, however, be functional without strong deployment of broadband, fibre, edge nodes and 5G, or if key emerging technologies such as quantum computing are not made a priority; calls on the Environment, Public Health and Food Safety (ENVI), Agriculture and Rural Development (AGRI), Regional Development (REGI), Transport and Tourism (TRAN), ITRE, ECON and IMCO Committees to follow up on these points;

279. Concludes that in order to promote innovation in AI, it is necessary to provide EU citizens with the means to acquire digital skills; stresses that in order to increase digital literacy and resilience and to combat the digital divide among citizens in the digital age, digital and AI education needs to start at an early stage and remain available at all levels of employment; finds that initiatives to establish AI ecosystems of excellence, to

increase the pool of AI talent in the EU and to combat brain drain are of vital importance; calls on the Culture and Education (CULT), Employment and Social Affairs (EMPL) and ITRE Committee to focus their resources on these fields;

280. Concludes that in order to build trust in AI among citizens, public services and their administrative structures need to lead by example; stresses that the EU needs to accelerate the uptake of AI in eGovernance in order to facilitate the secure use of AI in public administrations and to strengthen democratic structures as well as the EU's core ethical principles; stresses furthermore that AI in the healthcare sector, if provided with the means to securely access patients' data, will revolutionise healthcare systems; calls on the ENVI, ITRE, JURI and LIBE Committees to monitor and accelerate these developments;

281. Concludes that the EU's AI strategy should not overlook military and security considerations 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 our ethical principles and values but also to protect our continent against new technological threats; finds that our entire security system is affected by the digital transformation; urges the EU, therefore, to come up with new policy responses and tactics; calls on the Foreign Affairs (AFET), International Trade (INTA) and LIBE Committees, and the Subcommittee on Security and Defence (SEDE) to develop effective responses;

°

° °

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

EXPLANATORY STATEMENT

Artificial Intelligence (AI) determines the current digital transformation as the key technology. As a term encompassing a wide range of technologies that are guided by a given set of human-defined objectives and have some degree of autonomy in their actions, AI processes and responds to the data it receives, leading to learning, reasoning, planning, decision-making and creativity. Therefore, AI covers technologies that are already in widespread use, technologies that are currently under development as well as speculative inventions that might exist in the future. Within the current digital transformation, the impact of AI cannot be understated. It will continue to transform and improve the way we work, we move and we communicate. It will continue to transform and improve our society, our administration, our industries, our economy, our health care and our security system. Thus, AI has an impact on every sector and every part of our day-to-day life.

The Committee on Artificial Intelligence in the Digital Age (AIDA) was set up to present a EU Roadmap for AI that encompasses the steps the European Union needs to take in order to respond to these economic and societal challenges within the next few years. Within the global competition, the EU has already fallen behind. Significant parts of AI innovation and even more the commercialisation of AI technologies take place outside of Europe. We neither take the lead in development, research or investment in AI. If we do not set clear standards for the human-centred approach to AI that is based on our core European ethical standards and democratic values, they will be determined elsewhere. The consequences of falling further behind do not only threaten our economic prosperity but also lead to an application of AI that threatens our security, including surveillance, disinformation and social scoring. In fact, to be a global power means to be a leader in AI.

Therefore, the goal of the AIDA committee and this report is an urgent call to action. It provides a holistic approach for a common, long-term position that highlights the EU's key values and objectives relating to AI in the digital age that ensures that the digital transition is human-centric and consistent with the Charter of Fundamental Rights of the European Union. In line with its mandate, the report first defines the European approach to AI and reiterates its importance within the digital transformation. Instead of focusing on threats, a human-centric approach to AI based on our values will use AI for its benefits and give us the competitive edge to frame AI regulation on the global stage. Rather than an unpredictable and fully autonomous system, with the right rules, safeguards and regulations, AI is merely a tool for data processing that can revolutionize systems for the good of society.
The report thus continues by analysing the future impact of AI in the digital age, balancing its benefits towards certain risks on the EU economy, in particular on health, infrastructure, sustainability, transport, agriculture, energy, defence, industry, democracy, e-government, employment, skills and education. Moreover, based on this analysis, the report demonstrates the EU's current place in the global digital competition, which uncovers several deficiencies. It shows that the EU currently does not meet any of the preconditions that enable innovation to fully capture the potential of AI and other emerging technologies. A lack of access to and sharing of high-quality data, a lack of harmonized rules and standards, high regulatory burden and a lack of funding, research, skills and infrastructure for AI lead to the EU's stagnating competitiveness.

In order to tackle these deficiencies and with the goal to make the EU a global leader in AI,

the report presents its EU Roadmap for AI with clear policy recommendations for the next years. With a holistic approach and built on the key takeaways from the previous chapters, the Roadmap underlines several horizontal goals with clear recommendations for the European Commission, EU Member States and the European Parliament.

For one, there is a clear need for a favourable regulatory environment established by dynamic law-making and modern governance. Current regulatory frameworks, both on EU and Member State level, are too fragmented, too ponderous and do not provide for legal certainty. Thus, it is necessary to speed up and streamline legislative and governance processes when it comes to digital policy. Only high-risk AI applications need to be strictly regulated in order to achieve leeway for innovation and avoid regulatory burden. Moreover, AI is entirely dependent on high-quality data. Current frameworks do not provide for timely access and sufficient sharing of data, which needs to be revised and extended.

Our ambitions on AI can only be achieved through a fully integrated and fully harmonized completed digital single market that facilitates cross-border exchange and innovation. AI requires a robust infrastructure and connectivity roll-out with access for every citizen. The digital infrastructure must be based on sustainable principles in line with the Green Deal, targeting all sectors, including agriculture, electricity, housing, transport, businesses, value chains and the circular economy. Moreover, AI will not be functional without strong deployment of broadband, fibre, edge nodes and 5G as well as making key emerging technologies such as quantum computing a priority.

In addition, it is key to achieve an ecosystem of AI excellence where every EU citizen is provided with the means to acquire digital and AI skills at all stages of education and employment. That way, we can also establish AI centres of excellence as well as increase and retain AI talent to combat brain drain and remain competitive on the global scale. In order to build trust in AI among citizens, public services and their administrative structures need to lead with example by taking up AI in e-governance and e-health.

Lastly, the EU’s AI strategy should not overlook military and security aspects that arise with its deployment. The EU needs to cooperate internationally with like-minded partners to be able to promote its human-centric vision of AI and secure the EU’s ethical principles in the global competition.

AIDA committee - draft report - structure

1. Introduction

2. Potential opportunities, risks and obstacles in the use of AI: six case studies examined by the AIDA Committee
   a. AI and health
   b. AI and the Green Deal
   c. External policy and security dimension of AI
   d. AI and competitiveness
   e. AI and the future of democracy
   f. AI and the labor market
   g. Three recurring findings in all six case studies

3. The EU's place in the global AI competition

4. EU Roadmap for AI: how to become a global leader
   a. Favorable regulatory framework
   b. Complete the Digital Single Market
   c. Digital Green Infrastructure
   d. Ecosystem of excellence
   e. Ecosystem of trust
   f. Industry Strategy
   g. Security and military deterrence

5. Conclusion: an urgent call for action!