



Paris, 30 March 2023

POLITICAL OPINION

**Political opinion on the Proposal for a Regulation of the
European Parliament and of the Council laying down
harmonised rules on artificial intelligence and amending
certain legislative acts of the Union
COM(2021) 206 final**

The Senate European Affairs Committee,

Having regard to the Treaty on European Union, in particular Articles 4, 10 and 26 thereof,

Having regard to the Treaty on the Functioning of the European Union, in particular Articles 16 and 114 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, 2000/C 364/1, in particular Articles 7, 8, 20 and 21 thereof,

Having regard to the Convention for the Protection of Human Rights and Fundamental Freedoms, in particular Articles 6, 8, 13 and 14 and Protocol 12 thereof,

Having regard to the Council of Europe Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data of 28 January 1981 and the Additional Protocol thereto of 8 November 2001 (“Convention 108+”), in particular Article 6 thereof,

Having regard to the Regulation 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, repealing Directive 95/46/EC, known as the General Data Protection Regulation (GDPR),

Having regard to Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 September 2022 establishing the Digital Decade policy programme for 2030,

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 legislative acts of the Union, COM(2021) 206 final,

Having regard to the General Approach of the Council on this Proposal for a Regulation, adopted on 25 November 2022, 14954/22,

Having regard to the Proposal for a Directive of the European Parliament and of the Council of 28 September 2022 on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final,

Having regard to the Commission Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions of 25 April 2018 entitled “Artificial Intelligence for Europe”, COM(2018) 237 final,

Having regard to the Commission Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 19 February 2020 entitled “Shaping Europe’s Digital Future”, COM(2020) 67 final,

Having regard to the Commission Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 9 March 2021 entitled “2030 Digital Compass: the European way for the Digital Decade”, COM(2021) 118 final,

Having regard to the Commission Communication to the Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 21 April 2021

entitled “Fostering a European approach to Artificial Intelligence”, COM(2021) 205 final,

Having regard to the Commission Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 26 January 2022 entitled “Establishing a European Declaration on Digital rights and principles for the Digital Decade”, COM(2022) 27 final,

Having regard to the European Declaration on Digital Rights and Principles for the Digital Decade, published on 23 January 2023,

Having regard to the White Paper of 19 February 2020 entitled “Artificial Intelligence – A European approach to excellence and trust”, COM(2020) 65,

Having regard to the Joint Opinion 05/2021 of the European Data Protection Supervisor and the European Data Protection Committee of 18 June 2021,

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

Having regard to the European Parliament resolution of 20 October 2020 on the civil liability regime for artificial intelligence, (2020/2014(INL)),

Having regard to Senate Information Report No. 279 (2018-2019) by André Gattolin, Claude Kern, Cyril Pellevat and Pierre Ouzoulias on behalf of the European Affairs Committee, entitled *Artificial intelligence: the urgent need for European leadership*, submitted on 31 January 2019,

Having regard to Senate Information Report No. 627 (2021-2022) by Marc-Philippe Daubresse, Arnaud de Belenet and Jérôme Durain on behalf of the Laws Committee, entitled *Biometric recognition in public places: 30 proposals to eliminate the risk of a surveillance society*, submitted on 10 May 2022,

Having regard to Senate European Resolution No. 76 (2018-2019) of 8 March 2019 on investment in artificial intelligence in Europe,

Having regard to Senate European Resolution No. 138 (2021-2022) of 22 July 2022 on the European Union's Digital Decade policy programme for 2030,

Whereas digital technologies, and in particular the growing role played by artificial intelligence technologies, are of crucial importance in all economic, social, societal and environmental aspects, in particular for the competitiveness of businesses, the efficiency of public services, and the security and well-being of our societies;

Whereas this process of digitalisation and dissemination of artificial intelligence must in no way undermine the protection of fundamental rights, including the high level of protection of personal data currently enjoyed by Europeans, and whereas these technologies must be at the service of people and subject to the values, principles and fundamental rights of the European Union;

Whereas artificial intelligence technologies pose risks to privacy and personal data protection, data security and non-discrimination on the basis of gender, ethnicity, age, religion, opinion and economic status;

Whereas, however, artificial intelligence (AI) can be used in a positive way to protect fundamental rights;

Whereas the inherent opacity of AI systems presents an unprecedented obstacle to users' information or to the ability of supervisory bodies to carry out their duties;

Whereas there is no universally accepted definition of artificial intelligence systems;

Whereas Europe will only be able to take full advantage of the economic and societal potential of AI if there is greater legal certainty surrounding its deployment, which will require the development of clear, specific rules that can be understood by everyone;

Whereas the speed of technological developments and uses of AI requires that the applicable legal framework can be adjusted at regular intervals;

Whereas global competition in the AI sector is fierce and it is essential to ensure that the European Union can cope with it;

Whereas, in order to achieve its digital objectives, in particular with regard to security and the protection of fundamental rights, the European Union must combine its regulatory approach with support for the digital transition, enabling the development of a genuinely European offer guaranteeing it full sovereignty in all aspects of its digital development;

Whereas a balanced division of powers between the Commission and the national supervisory authorities is an essential prerequisite for effective regulation of the AI sector;

On the principle of the Regulation

Welcomes the European Commission's intention to introduce harmonised, horizontal regulations for artificial intelligence at the European level and to bring it into force as soon as possible;

Welcomes the fact that all providers targeting the European market, even those established in a third country, are subject to the obligations laid down in the Regulation, and that subsidiary obligations are laid down for importers and distributors of AI systems;

Calls for providers of AI systems for generic use to also be subject to specific obligations under this Regulation, in view of the increasingly frequent use of such systems and the risks they may pose;

Supports the establishment of a list of banned AI practices, including "high-risk" practices, in view of the threat they pose to fundamental rights;

Regrets that the Proposal does not specifically address the risks of mass surveillance arising from large private companies using artificial intelligence algorithms to collect and process a considerable amount of personal and non-personal data;

On the definition of AI systems

Considers that the ability of the Commission to use delegated acts, after the entry into force of the Regulation, to modify the techniques and approaches listed in Annex I as those characterising an AI system is excessive;

Suggests that the definition of AI systems as laid down by the Organisation for Economic Co-operation and Development (OECD), which is technology-neutral and therefore less likely to become obsolete, be included directly in the Regulation;

On “high-risk” AI systems

Emphasises the need to be able to add to the list of high-risk systems as technologies and uses evolve;

Expresses hope that changes to the list of high-risk systems will first be subject to careful scrutiny by AI scientists and practitioners, based on objective and documented evidence, for example within the framework of the future European Artificial Intelligence Board;

Recommends that the high-risk systems referred to in Annex III be described in greater detail in order to define their scope accurately and to prevent any risk of over-compliance, which would be detrimental to the European economic development of AI;

Requests that AI systems which may influence or negatively impact the rights of vulnerable persons, in particular children; which may have a direct impact on people’s state of health; which are used to determine insurance premiums; which are used to evaluate medical treatments or for medical research purposes; which are components of health and wellness applications; which are intended to prioritise the dispatch of police services, be classified as high-risk applications;

Calls for systemic risks, i.e. risks to individuals as a whole, to be considered in the definition of high-risk AI systems; expresses hope that the list of high-risk AI systems will include, in particular, applications that may cause environmental damage and content recommendation algorithms designed to maximise users’ time on social media networks by promoting disinformation and divisive content;

Recommends that a public register of public bodies or authorities using high-risk AI systems be set up so that the general public can be fully informed of the decision-making processes associated with the use of AI technologies by the public sector,

except in cases where such transparency would jeopardise the work of law enforcement authorities;

On banned AI practices

Considers that AI practices banned in the public sector should also be banned in the private sector;

Calls for a ban on practices that may exploit the potential economic and social vulnerabilities of a group of people and that may result in social or economic harm;

Calls for a general ban on emotional recognition systems; on social rating systems; on systems for categorising people in public places; on systems for classifying individuals based on biometric data into groups that fall under categories of sensitive data;

Considers that the ban on remote biometric identification systems in public places should not be limited to those allowing remote biometric identification in real time;

On the AI systems used by security forces and law enforcement authorities

Supports excluding from the scope of the Regulation AI systems developed or used for military purposes, including dual AI systems;

Calls for excluding from the scope of the Regulation AI systems developed or used for national defence and security activities;

Considers that, subject to appropriate safeguards for the protection of fundamental rights, the rules governing the use of AI systems by law enforcement authorities must be adjusted to maintain their ability to take action;

Considers in particular that in terms of transparency, the legal framework applicable to AI systems used by law enforcement authorities must take account of the need to keep certain sensitive operational data confidential;

Expresses hope that, in the law enforcement sector and in the migration, asylum and border control management sector, the use of results obtained through remote biometric identification systems

will be subject to the requirement of human control, but not double control, which would be costly and ineffective from a fundamental rights protection perspective;

Calls for a better definition of the criteria for activating exceptions to the ban on “real-time” remote biometric identification systems by law enforcement authorities, to prevent any abuse in this area;

Recommends, given the rapid development of the metaverse, that the concept of virtual public spaces be integrated, so that the same restrictions on the use of AI are applied to virtual public spaces as in physical public spaces;

On the obligations of providers

Expresses hope that third-party conformity assessment of AI systems will become widespread;

Calls for this conformity assessment to take greater account of the actions of all parties involved in the design and implementation of AI systems, in particular users, given that risks to safety or fundamental rights may arise from both the design of AI systems and the conditions and methods used in their implementation;

Calls for the obligation on providers to list all foreseeable misuses of a system to be described more clearly;

Considers that the obligation for providers to manage and mitigate risks must be limited to the risks identified;

Expresses hope that, prior to the use of any personal or non-personal data, providers will be required to verify that such data have been obtained lawfully and in accordance with European data protection regulations;

Calls therefore for stricter requirements for the documentation on data sets used for training systems, both in terms of the conditions of collection under which they are collected and in terms of any shortcomings identified;

Considers it necessary to guarantee better protection for people who may be affected by AI without being direct users, within the meaning of the Regulation;

Requests in this regard that providers and users of AI systems provide information that is understandable and accessible to all, ensuring that people exposed to an AI system can be systematically informed of it;

Recommends that consideration be given to developing an alert mechanism to be used by persons affected by AI systems to report to regulators, providers or users any misuse or poor performance of AI systems, along with breaches of the rules laid down in the European AI Regulation, even where these do not result in direct and immediate harm to the person affected;

On the relationship with the General Data Protection Regulation (GDPR)

Expresses hope that the AI Regulation will be without prejudice to the GDPR and that this is explicitly stated in the Regulation;

Emphasises that an AI system's compliance with the AI Regulation does not automatically imply its compliance with the GDPR and vice versa;

Recommends that the European Data Protection Committee or, failing that, the national data protection authorities issue guidelines on the relationship between the AI Regulation and the GDPR, in particular to clarify the degree of flexibility with which the GDPR can be interpreted in the context of the development of AI in Europe;

Supports the possibility for providers to process special categories of personal data to combat bias and the potentially discriminatory nature of the way certain AI systems operate, under the supervision of national data protection authorities;

Emphasises however that this exemption must be sufficiently supervised to guard against any risk of misuse of such sensitive data, particularly for commercial purposes;

On supporting innovation

Welcomes any European initiative aimed at supporting the development of AI within the framework of existing and future European rules;

Notes that the ex-ante conformity assessment obligation is inconsistent with the momentum of product research, which requires a two-way flow between development in a closed environment and the market;

Strongly supports the introduction of regulatory sandboxes;

Expresses hope that they will operate in as uniform a manner as possible across the Member States, in order to encourage innovation;

Approves of granting small businesses and start-ups preferential access to these regulatory sandboxes;

Recommends that the procedures and conditions for setting up and operating these regulatory sandboxes be submitted to the European Artificial Intelligence Board for an opinion;

Emphasises also how important it is for the European Union and its Member States to become involved in international standardisation bodies as a means of promoting ambitious standards in the areas of robustness, cybersecurity and the protection of fundamental rights;

Calls, in addition to the proposed legislative and regulatory changes, for the implementation of an ambitious industrial policy in the digital sector, including the mobilisation of the necessary investment, to enable the development of a sovereign European artificial intelligence offering;

On enforcing the Regulation

Notes the disparity in the technical and human resources allocated to the national supervisory authorities within the European Union and emphasises the difficulties that such a situation could pose for the uniform application of the Regulation;

Emphasises that support for and monitoring of the implementation of the Regulation will require substantial resources from European and national supervisory authorities, and calls for advance planning of the provision of these resources, given the risks to fundamental rights caused by the deployment of non-compliant AI systems;

Calls for it to be made clear that safeguards on intellectual property and trade secrets imply an obligation on the part of regulatory authorities not to disclose data of which they have knowledge and not a right for the companies concerned to object to their data being accessed by the authorities;

On governance

Emphasises the crucial role of the European Artificial Intelligence Board set up by the Regulation in ensuring effective cooperation between Member States on AI, an essential requirement for the uniform and consistent application of this Regulation within the European Union;

Emphasises that the European Artificial Intelligence Board will only be able to fulfil its role of assisting Member States and advising the Commission if it is given a sufficient degree of autonomy;

Recommends to this end that the composition of this Board be reviewed, in particular to include AI scientists and practitioners able to provide technical expertise and operational advice within a short time frame;

Calls for the Board's consultative powers to be strengthened, ensuring that it is closely involved in amendments to the Regulation made after its adoption, especially when they relate to the list of high-risk applications in Annex III;

Expresses hope that the Board will be granted a right of initiative, enabling it to formulate opinions and recommendations without referring first to the Commission, thereby strengthening the forward-looking nature of its work;

Recommends that the links between the Board and all stakeholders in the AI ecosystem be strengthened to ensure that this new body is properly integrated into this ecosystem, in particular through regular consultations.