BRIEFING

EU Legislation in Progress

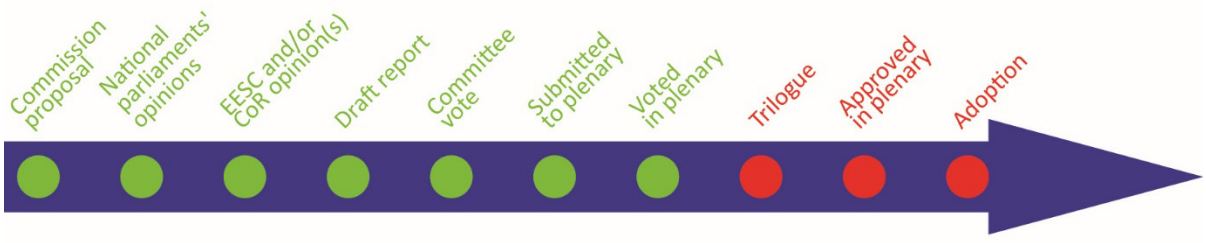
European Parliament

Artificial intelligence act

OVERVIEW

The European Commission tabled a proposal for an EU regulatory framework on artificial intelligence (AI) in April 2021. The draft AI act is the first ever attempt to enact a horizontal regulation for AI. The proposed legal framework focuses on the specific utilisation of AI systems and associated risks. The Commission proposes to establish a technology-neutral definition of AI systems in EU law and to lay down a classification for AI systems with different requirements and obligations tailored on a 'risk-based approach'. Some AI systems presenting 'unacceptable' risks would be prohibited. A wide range of 'high-risk' AI systems would be authorised, but subject to a set of requirements and obligations to gain access to the EU market. Those AI systems presenting only 'limited risk' would be subject to very light transparency obligations. The Council agreed the EU Member States' general position in December 2021. Parliament voted on its position in June 2023. EU lawmakers are now starting negotiations to finalise the new legislation, with substantial amendments to the Commission's proposal including revising the definition of AI systems, broadening the list of prohibited AI systems, and imposing obligations on general purpose AI and generative AI models such as ChatGPT.

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		
Committees responsible:	Internal Market and Consumer Protection (IMCO) and Civil Liberties, Justice and Home Affairs (LIBE) (jointly under Rule 58)	COM(2021)206 21.4.2021 2021/0106(COD)
Rapporteurs:	Brando Benifei (S&D, Italy) and Dragoş Tudorache (Renew, Romania)	
Shadow rapporteurs:	Deirdre Clune, Axel Voss (EPP); Petar Vitanov (S&D); Svenja Hahn, (Renew); Sergey Lagodinsky, Kim Van Sparrentak (Greens/EFA); Rob Rooken, Kosma Złotowski (ECR); Jean-Lin Lacapelle, Jaak Madison (ID); Cornelia Ernst, Kateřina Konecna (The Left)	Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
Next steps expected:	Trilogue negotiations	



EPRS | European Parliamentary Research Service

Author: Tambiama Madiega; Graphic: Samy Chahri
Members' Research Service

PE 698.792 – June 2023

EN

Introduction

AI technologies are expected to bring a wide array of **economic and societal benefits** to a wide range of sectors, including environment and health, the public sector, finance, mobility, home affairs and agriculture. They are particularly useful for improving prediction, for optimising operations and resource allocation, and for personalising services.[1] However, the implications of AI systems for **fundamental rights** protected under the EU Charter of Fundamental Rights, as well as the **safety risks** for users when AI technologies are embedded in products and services, are raising concern. Most notably, AI systems may jeopardise fundamental rights such as the right to non-discrimination, freedom of expression, human dignity, personal data protection and privacy.[2]

Given the fast development of these technologies, in recent years AI regulation has become a central policy question in the European Union (EU). Policy-makers pledged to develop a **'human-centric' approach to AI** to ensure that Europeans can benefit from new technologies developed and functioning according to the EU's values and principles.[3] In its 2020 White Paper on Artificial Intelligence, the European Commission committed to **promote the uptake of AI** and **address the risks associated** with certain uses of this new technology. While the European Commission initially adopted a **soft-law approach**, with the publication of its non-binding 2019 Ethics Guidelines for Trustworthy AI and Policy and investment recommendations, it has since shifted towards a **legislative approach**, calling for the adoption of harmonised rules for the development, placing on the market and use of AI systems.[4]

AI regulatory approach in the world. While the United States of America (USA) had initially taken a lenient approach towards AI, calls for regulation have recently been mounting. The Cyberspace Administration of China is also consulting on a proposal to regulate AI, while the UK is working on a set of pro-innovation regulatory principles. At international level, the Organisation for Economic Co-operation and Development (OECD) adopted a (non-binding) Recommendation on AI in 2019, UNESCO adopted Recommendations on the Ethics of AI in 2021, and the Council of Europe is currently working on an international convention on AI. Furthermore, in the context of the newly established EU-US tech partnership (the Trade and Technology Council), the EU and USA are seeking to develop a mutual understanding on the principles underlining trustworthy and responsible AI. EU lawmakers issued a joint statement in May 2023 urging President Biden and European Commission President Ursula von der Leyen to convene a summit to find ways to control the development of advanced AI systems such as ChatGPT.

Parliament's starting position

Leading the EU-level debate, the European Parliament called on the European Commission to assess the impact of AI and to draft an EU framework for AI, in its wide-ranging 2017 recommendations on civil law rules on robotics. More recently, in 2020 and 2021, the Parliament adopted a number of non-legislative resolutions calling for EU action, as well as two legislative resolutions calling for the adoption of EU legislation in the field of AI. A first legislative resolution asked that the Commission establish a legal framework of ethical principles for the development, deployment and use of AI, robotics and related technologies in the Union. A second legislative resolution called for harmonisation of the legal framework for civil liability claims and imposition of a regime of strict liability on operators of high-risk AI systems. Furthermore, the Parliament adopted a series of recommendations calling for a common EU approach to AI in the intellectual property, criminal law, education, culture and audiovisual areas, and regarding civil and military AI uses.

Council starting position

In the past, the Council has repeatedly called for the adoption of common AI rules, including in 2017 and 2019. More recently, in 2020, the Council called upon the Commission to put forward concrete proposals that take existing legislation into account and follow a risk-based, proportionate and, if necessary, regulatory approach. Furthermore, the Council invited the EU and the Member States to

consider effective measures for identifying, predicting and responding to the potential impacts of digital technologies, including AI, on fundamental rights.

Preparation of the proposal

Following the White Paper on Artificial Intelligence[5] adopted in February 2020, the Commission launched a broad public consultation in 2020 and published an Impact Assessment of the regulation on artificial intelligence, a supporting study and a draft proposal, which received feedback from a variety of stakeholders.[6] In its impact assessment, the Commission identifies **several problems** raised by the development and use of AI systems, due to their specific characteristics.[7]

The changes the proposal would bring

The draft AI act has been designed as a **horizontal EU legislative instrument** applicable to all AI systems placed on the market or used in the Union.

Purpose, legal basis and scope

The **general objective** of the proposed AI act unveiled in April 2021 is to ensure the proper functioning of the single market by creating the conditions for the development and use of trustworthy AI systems in the Union. The draft sets out a harmonised legal framework for the development, placing on the Union market, and the use of AI products and services. In addition, the AI act proposal seeks to achieve a set of **specific objectives**: (i) ensure that AI systems placed on the EU market are safe and respect existing EU law, (ii) ensure legal certainty to facilitate investment and innovation in AI, (iii) enhance governance and effective enforcement of EU law on fundamental rights and safety requirements applicable to AI systems, and (iv) facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.[8]

The new AI framework, based on Article 114[9] and Article 16[10] of the Treaty on the Functioning of the European Union (TFEU), would enshrine a **technology-neutral definition of AI systems** and adopt a **risk-based approach**, which lays down different **requirements and obligations** for the development, placing on the market and use of AI systems in the EU. In practice, the proposal defines common mandatory requirements applicable to the design and development of AI systems before they are placed on the market and harmonises the way ex-post controls are conducted. The proposed AI act would complement existing and forthcoming, horizontal and sectoral EU safety regulation.[11] The Commission proposes to follow the logic of the new legislative framework (NLF), i.e. the EU approach to ensuring a range of products comply with the applicable legislation when they are placed on the EU market through conformity assessments and the use of CE marking.

The new rules would apply primarily to **providers of AI systems established within the EU or in a third country** placing AI systems on the EU market or putting them into service in the EU, as well as to **users of AI systems located in the EU**.[12] To prevent circumvention of the regulation, the new rules would also apply to **providers and users of AI systems located in a third country** where the output produced by those systems is used in the EU.[13] However, the draft regulation does not apply to AI systems developed or used exclusively for military purposes, to public authorities in a third country, nor to international organisations, or authorities using AI systems in the framework of international agreements for law enforcement and judicial cooperation.

Definitions

No single definition of artificial intelligence is accepted by the scientific community and the term 'AI' is often used as a 'blanket term' for various computer applications based on different techniques, which exhibit capabilities commonly and currently associated with human intelligence.[14] The High Level Expert Group on AI proposed a baseline definition of AI that is increasingly used in the scientific literature, and the Joint Research Centre has established an operational definition of AI based on a taxonomy that maps all the AI subdomains from a political, research and industrial

perspective. However, the Commission found that the **notion of an AI system** should be more clearly defined, given that the determination of what an 'AI system' constitutes is crucial for the allocation of legal responsibilities under the new AI framework. The Commission therefore proposes to establish a legal definition of 'AI system' in EU law, which is largely based on a definition already used by the OECD.[15] Article 3(1) of the draft act states that '**artificial intelligence system**' means:

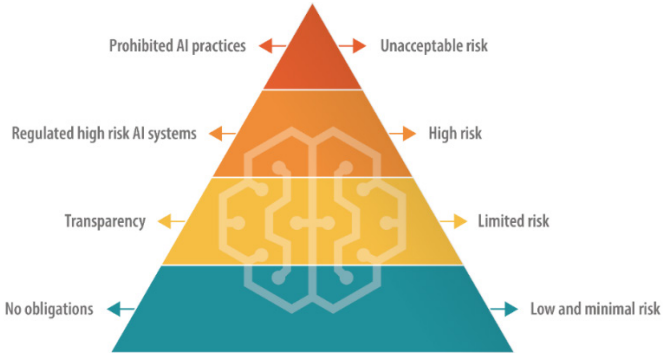
> *...software that is developed with [specific] techniques and approaches [listed in Annex 1] and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.*[16]

Annex 1 of the proposal lays out a **list of techniques and approaches** that are used today to develop AI. Accordingly, the notion of 'AI system' would refer to a range of software-based technologies that encompasses '**machine learning**', '**logic and knowledge-based**' systems, and '**statistical**' approaches. This broad definition covers AI systems that can be used on a stand-alone basis or as a component of a product. Furthermore, the proposed legislation aims to be future-proof and cover current and future AI technological developments. To that end, the Commission would complement the Annex 1 list with new approaches and techniques used to develop AI systems as they emerge – through the adoption of **delegated acts** (Article 4).

Furthermore, Article 3 provides a long **list of definitions** including that of 'provider' and 'user' of AI systems (covering both public and private entities), as well as 'importer' and 'distributor', 'emotion recognition', and 'biometric categorisation'.

Risk-based approach

Pyramid of risks



Data source: European Commission.

The use of AI, with its specific characteristics (e.g. opacity, complexity, dependency on data, autonomous behaviour), can adversely affect a number of fundamental rights and users' safety. To address those concerns, the draft AI act follows a **risk-based approach** whereby legal intervention is tailored to concrete level of risk. To that end, the draft AI act distinguishes between AI systems posing (i) **unacceptable risk**, (ii) **high risk**, (iii) **limited risk**, and (iv) **low or minimal risk**. AI applications would be regulated only as strictly necessary to address specific levels of risk.[17]

Unacceptable risk: Prohibited AI practices

Title II (Article 5) of the proposed AI act explicitly **bans harmful AI practices** that are considered to be a clear threat to people's safety, livelihoods and rights, because of the 'unacceptable risk' they create. Accordingly, it would be prohibited to place on the market, put into services or use in the EU:

- AI systems that deploy harmful manipulative 'subliminal techniques';
- AI systems that exploit specific vulnerable groups (physical or mental disability);
- AI systems used by public authorities, or on their behalf, for social scoring purposes;
- 'Real-time' remote biometric identification systems in publicly accessible spaces for law enforcement purposes, except in a limited number of cases.[18]

High risk: Regulated high-risk AI systems

Title III (Article 6) of the proposed AI act regulates 'high-risk' AI systems that create adverse impact on people's safety or their fundamental rights. The draft text distinguishes between two categories of high-risk AI systems.

- Systems used as a safety component of a product or falling under EU health and safety harmonisation legislation (e.g. toys, aviation, cars, medical devices, lifts).
- Systems deployed in **eight specific areas** identified in Annex III, which the Commission could update as necessary through **delegated acts** (Article 7):
  - Biometric identification and categorisation of natural persons;
  - Management and operation of critical infrastructure;
  - Education and vocational training;
  - Employment, worker management and access to self-employment;
  - Access to and enjoyment of essential private services and public services and benefits;
  - Law enforcement;
  - Migration, asylum and border control management;
  - Administration of justice and democratic processes.

All of these high-risk AI systems would be subject to a set of new rules including:

Requirement for an ex-ante conformity assessment: Providers of high-risk AI systems would be required to register their systems in an **EU-wide database** managed by the Commission before placing them on the market or putting them into service. Any AI products and services governed by existing product safety legislation will fall under the existing third-party conformity frameworks that already apply (e.g. for medical devices). Providers of AI systems not currently governed by EU legislation would have to conduct their own conformity assessment (**self-assessment**) showing that they comply with the new requirements and can use **CE marking**. Only high-risk AI systems used for biometric identification would require a conformity assessment by a 'notified body'.

Other requirements: Such high-risk AI systems would have to comply with a range of requirements particularly on risk management, testing, technical robustness, data training and data governance, transparency, human oversight, and cybersecurity (Articles 8 to 15). In this regard, providers, importers, distributors and users of high-risk AI systems would have to fulfil a range of obligations. Providers from outside the EU will require an **authorised representative** in the EU to (inter alia), ensure the conformity assessment, establish a post-market monitoring system and take corrective action as needed. AI systems that conform to the new **harmonised EU standards**, currently under development, would benefit from a presumption of conformity with the draft AI act requirements.[19]

Facial recognition: AI powers the use of biometric technologies, including facial recognition technologies (FRTs), which are used by private or public actors for verification, identification and categorisation purposes. In addition to the existing applicable legislation (e.g. data protection and non-discrimination), the draft AI act proposes to introduce new rules for FRTs and differentiate them according to their 'high-risk' or 'low-risk' usage characteristics. The use of real-time facial recognition systems in publicly accessible spaces for the purpose of law enforcement would be prohibited, unless Member States choose to authorise them for important public security reasons, and the appropriate judicial or administrative authorisations are granted. A wide range of FRTs used for purposes other than law enforcement (e.g. border control, market places, public transport and even schools) could be permitted, subject to a conformity assessment and compliance with safety requirements before entering the EU market.[20]

Limited risk: Transparency obligations

AI systems presenting 'limited risk', such as **systems that interacts with humans** (i.e. chatbots), **emotion recognition systems**, **biometric categorisation systems**, and AI systems that generate or manipulate image, audio or video content (i.e. **deepfakes**), would be subject to a limited set of transparency obligations.

Low or minimal risk: No obligations

All other AI systems presenting only low or minimal risk could be developed and used in the EU without conforming to any additional legal obligations. However, the proposed AI act envisages the creation of **codes of conduct** to encourage providers of non-high-risk AI systems to voluntarily apply the mandatory requirements for high-risk AI systems.

Governance, enforcement and sanctions

The proposal requires Member States to designate one or more competent authorities, including a **national supervisory authority**, which would be tasked with supervising the application and implementation of the regulation, and establishes a **European Artificial Intelligence Board** (composed of representatives from the Member States and the Commission) at EU level. National **market surveillance authorities** would be responsible for assessing operators' compliance with the obligations and requirements for high-risk AI systems. They would have access to confidential information (including the source code of the AI systems) and subject to binding confidentiality obligations. Furthermore, they would be required to take any **corrective measures** to prohibit, restrict, withdraw or recall AI systems that do not comply with the AI act, or that, although compliant, present a risk to health or safety of persons or to fundamental rights or other public interest protection. In case of persistent non-compliance, Member States will have to take all appropriate measures to restrict, prohibit, recall or withdraw the high-risk AI system at stake from the market.

Administrative **fines** of varying scales (up to €30 million or 6 % of the total worldwide annual turnover), depending on the severity of the infringement, are set as sanctions for non-compliance with the AI act. Member States would need to lay down rules on penalties, including administrative fines and take all measures necessary to ensure that they are properly and effectively enforced.

Measures to support innovation

The Commission proposes that Member States, or the European Data Protection Supervisor, could establish a **regulatory sandbox**, i.e. a controlled environment that facilitates the development, testing and validation of innovative AI systems (for a limited period of time) before they are put on the market. Sandboxing will enable participants to use personal data to foster AI innovation, without prejudice to the GDPR requirements. Other measures are tailored specifically to small-scale providers and **start-ups**

Advisory committees

The European Economic and Social Committee adopted its opinion on the proposed artificial intelligence act on 22 September 2021.

National parliaments

The deadline for the submission of reasoned opinions on the grounds of subsidiarity was 2 September 2021. Contributions were received from the Czech Chamber of Deputies and the Czech Senate, the Portuguese Parliament, the Polish Senate and the German Bundesrat.

Stakeholder views[21]

Definitions

Definitions are a contentious point of discussion among stakeholders. The Big Data Value Association, an industry-driven international not–for-profit organisation, stresses that the definition of AI systems is quite broad and would cover far more than what is subjectively understood as AI, including the simplest search, sorting and routing algorithms, which would consequently be subject to new rules. Furthermore, they ask for clarification of how components of larger AI systems (such

as pre-trained AI components from other manufacturers or components not released separately), should be treated. AmCham, the American Chamber of Commerce in the EU, suggests avoiding over-regulation by adopting a narrower definition of AI systems, focusing strictly on high-risk AI applications (and not extended to AI applications that are not high-risk, or software in general). AccessNow, an association defending users' digital rights argues the definitions of 'emotion recognition' and 'biometric categorisation' are technically flawed, and recommends adjustments.

Risk-based approach

While they generally welcome the proposed AI act's risk-based approach, some stakeholders support wider prohibition and regulation of AI systems. Civil rights organisations call for a ban on indiscriminate or arbitrarily targeted use of biometrics in public or publicly accessible spaces, and for restrictions on the uses of AI systems, including for border control and predictive policing. AccessNow argues that the provisions concerning prohibited AI practices (Article 5) are too vague, and proposes a wider ban on the use of AI to categorise people based on physiological, behavioural or biometric data, for emotion recognition, as well as dangerous uses in the context of policing, migration, asylum, and border management. Furthermore, they call for stronger impact assessment and transparency requirements.

The European Enterprises Alliance stresses that there is general uncertainty about the roles and responsibilities of the different actors in the AI value chain (developers, providers, and users of AI systems). This is particularly challenging for companies providing general purpose application programming interfaces or open-source AI models that are not specifically intended for high-risk AI systems but are nevertheless used by third parties in a manner that could be considered high-risk. They also call for 'high-risk' to be redefined, based on the measurable harm and potential impact. AlgorithmWatch underlines that the applicability of specific rules should not depend on the type of technology, but on the impact it has on individuals and society. They call for the new rules to be defined according to the impact of the AI systems and recommend that every operator should conduct an impact assessment that assesses the system's risk levels on a case-by-case basis. Climate Change AI calls for climate change mitigation and adaptation to be taken into account in the classification rules for high-risk AI systems and impose environmental protection requirements.

Consumer protection

The European Consumer Organisation, BEUC, stresses that the proposal requires substantial improvement to guarantee consumer protection. The organisation argues that the proposal should have a broader scope and impose basic principles and obligations (e.g. on fairness, accountability and transparency) upon all AI systems, as well as prohibiting more comprehensively harmful practices (such as private entities' use of social scoring and of remote biometric identification systems in public spaces). Furthermore, consumers should be granted a strong set of rights, effective remedies and redress mechanisms, including collective redress.

Impact on investments and SMEs

There are opposing views on the impact of the proposed regulation on investment. A study by the Centre for Data Innovation (representing large online platforms) highlights that the compliance costs incurred under the proposed AI act would likely provoke a chilling effect on investment in AI in Europe, and could particularly deter small and medium-sized enterprises (SMEs) from developing high-risk AI systems. According to the Centre for Data Innovation, the AI act would cost the European economy €31 billion over the next five years and reduce AI investments by almost 20 %. However, such estimates of the compliance costs are challenged by the experts from the Centre for European Policy Studies, as well as by other economists. The European Digital SME Alliance warns against overly stringent conformity requirements, asks for effective representation of SMEs in the standards-setting procedures and for making sandboxes mandatory in all EU Member States.

Academic and other views

While generally supporting the Commission's proposal, critics call for amendments, including revising the 'AI systems' definition, ensuring a better allocation of responsibility, strengthening enforcement mechanisms and fostering democratic participation.[22] Among the main issues are:

AI systems definition

The legal definition of 'AI systems' contained in the proposed AI act has been heavily criticised. Smuha and others warn the definition lacks clarity and may lead to legal uncertainty, especially for some systems that would not qualify as AI systems under the draft text, while their use may have an adverse impact on fundamental rights.[23] To address this issue, the authors propose to **broaden the scope of the legislation** to explicitly include all computational systems used in the identified high-risk domains, regardless of whether they are considered to be AI. According to the authors, the advantage would be in making application of the new rules more dependent on the domain in which the technology is used and the fundamental rights-related risks, rather than on a specific computational technique. Ebers and others consider that the scope of 'AI systems' is overly broad, which may lead to **legal uncertainty** for developers, operators, and users of AI systems and ultimately to over-regulation.[24] They call on EU law-makers to exempt AI systems developed and used for **research purposes** and **open-source software** (OSS) from regulation. Other commentators question whether the proposed definition of 'AI systems' is truly **technology neutral** as it refers primarily to 'software', omitting potential future AI developments.

Risk-based approach

Academics also call for amendments, warning that the risk-based approach proposed by the Commission would not ensure a high level of protection of fundamental rights. Smuha and others argue that the proposal does not always accurately recognise the wrongs and harms associated with different kinds of AI systems and therefore does not appropriately allocate responsibility. Among other things, they recommend adding a procedure that enables the Commission to **broaden the list of prohibited AI systems**, and propose banning existing manipulative AI systems (e.g. deepfakes), social scoring and some biometrics. Ebers and others call for a **more detailed classification of risks** to facilitate industry self-assessment and support, as well as **prohibiting more AI systems** (e.g. biometrics), including in the context of **private use**. Furthermore, some highlight that the draft legislation does not address **systemic sustainability risks** created by AI especially in the area of climate and environmental protection.[25]

Experts seem particularly concerned by the implementation of Article 5 (prohibited practices) and Article 6 (regulated high-risk practices). One of the major concerns raised is that the rules on prohibited and high-risk practices may prove ineffective in practice, because the risk assessment is left to provider **self-assessment**. Veale and Zuiderveen Borgesius warn that most providers can arbitrarily classify most high-risk systems as adhering to the rules using self-assessment procedures alone. Smuha and others recommend exploring whether certain high-risk systems would not benefit from a conformity assessment carried out by an **independent entity** prior to their deployment.

Biometrics regulation. A study commissioned by the European Parliament recommends, inter alia, to empower the Commission to adapt the list of prohibited AI practices periodically, under the supervision of the European Parliament, and the adoption of a more comprehensive list of 'restricted AI applications' (comprising real-time remote biometric identification without limitation for law enforcement purposes). Regulation of facial recognition technologies (FRTs) is one of the most contentious issues.[26] The European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB) have called for a general ban on any uses of AI for the automated recognition of human features in publicly accessible spaces.

Governance structure and enforcement and redress mechanisms

Ebers and others stress that the AI act **lacks effective enforcement structures**, as the Commission proposes to leave the preliminary risk assessment, including the qualification as high-risk, to the providers' self-assessment. They also raise concerns about the excessive delegation of regulatory power to private European standardisation organisations (ESOs), due to the lack of democratic oversight, the impossibility for stakeholders (civil society organisations, consumer associations) to influence the development of standards, and the lack of judicial means to control them once they have been adopted. Instead, they recommend that the AI act codifies a set of legally binding requirements for high-risk AI systems (e.g. prohibited forms of algorithmic discrimination), which ESOs may specify through harmonised standards. Furthermore, they advocate that European policy-makers should **strengthen democratic oversight of the standardisation process**.

Commentators deplore a crucial gap in the AI act, which does not provide for **individual enforcement rights**. Ebers and others stress that individuals affected by AI systems and civil rights organisations have no **right to complain** to market surveillance authorities or to sue a provider or user for failure to comply with the requirements. Similarly, Veale and Zuiderveen Borgesius warn that, while some provisions of the draft legislation aim to impose obligations on AI systems users, there is **no mechanism for complaint or judicial redress** available to them. Smuha and others recommend amending the proposal to include, inter alia, an **explicit right of redress for individuals** and **rights of consultation and participation for EU citizens** regarding the decision to amend the list of high-risk systems in Annex III.

It has also been stressed that the text as it stands **lacks proper coordination** mechanisms between authorities, in particular concerning **cross-border infringement**. Consequently, the competence of the relevant authorities at national level should be clarified. Furthermore, guidance would be desirable on how to ensure compliance with transparency and information requirements, while simultaneously **protecting intellectual property rights and trade secrets** (e.g. to what extent the source code must be disclosed), not least to avoid diverging practices in the Member States.

Legislative process

The **Council** adopted its common position in December 2022. The Council's proposes, inter alia to:

- narrow the definition of AI systems to systems developed through machine learning approaches and logic- and knowledge-based approaches;
- extend to private actors the prohibition on using AI for social scoring, and add cases when the use of 'real-time' remote biometric identification systems in publicly accessible spaces could exceptionally be allowed;
- impose requirements on general purpose AI systems by means of implementing acts;
- add new provisions to take into account situations where AI systems can be used for many different purposes (general purpose AI); and
- simplify the compliance framework for the AI Act and strengthen, in particular, the role of the AI Board.

In **Parliament**, the file was assigned jointly (under Rule 58) to the Committee on Internal Market and Consumer Protection (IMCO) and the Committee on Civil Liberties, Justice and Home Affairs (LIBE), with Brando Benifei (S&D, Italy) and Dragos Tudorache, Renew, Romania) appointed as rapporteurs. In addition, the Legal Affairs Committee (JURI), the Committee on Industry, Research and Energy (ITRE) and the Committee on Culture and Education (CULT) are each associated to the legislative work under Rule 57, with shared and/or exclusive competences for specific aspects of the proposal. Parliament adopted its negotiating position (499 votes in favour, 28 against and 93 abstentions) on 14 June 2023, with substantial amendments to the Commission's text, including:

- **Definitions**. Parliament amended the definition of AI systems to align it with the definition agreed by the OECD. Furthermore, Parliament enshrines a definition of

'general purpose AI system' and 'foundation model' in EU law.

- **Prohibited practices**. Parliament substantially amended the list of AI systems prohibited in the EU. Parliament wants to ban the use of biometric identification systems in the EU for both real-time and ex-post use (except in cases of severe crime and pre-judicial authorisation for ex-post use) and not only for real-time use, as proposed by the Commission. Furthermore, Parliament wants to ban all biometric categorisation systems using sensitive characteristics (e.g. gender, race, ethnicity, citizenship status, religion, political orientation); predictive policing systems (based on profiling, location or past criminal behaviour); emotion recognition systems (used in law enforcement, border management, workplace, and educational institutions); and AI systems using indiscriminate scraping of biometric data from social media or CCTV footage to create facial recognition databases.
- **High-risk AI systems**. While the Commission proposed to automatically categorise as high-risk all systems in certain areas or use cases, Parliament adds the additional requirement that the systems must pose a 'significant risk' to qualify as high-risk. AI systems that risk harming people's health, safety, fundamental rights or the environment would be considered as falling within high-risk areas. In addition, AI systems used to influence voters in political campaigns and AI systems used in recommender systems displayed by social media platforms, designated as very large online platforms under the Digital Services Act, would be considered high-risk systems. Furthermore, Parliament imposes on those deploying a high-risk system in the EU an obligation to carry out a fundamental rights impact assessment.
- **General-purpose AI, generative AI and foundation models.** Parliament sets a layered regulation of general-purpose AI. Parliament imposes an obligation on providers of foundation models to ensure robust protection of fundamental rights, health, safety, the environment, democracy and the rule of law. They would be required to assess and mitigate the risks their models entail, comply with some design, information and environmental requirements and register such models in an EU database. Furthermore, generative foundation AI models (such as ChatGPT) that use large language models (LLMs) to generate art, music and other content would be subject to stringent transparency obligations. Providers of such models and of generative content would have to disclose that the content was generated by AI not by humans, train and design their models to prevent generation of illegal content and publish information on the use of training data protected under copyright law. Finally, all foundation models should provide all necessary information for downstream providers to be able to comply with their obligations under the AI act.
- **Governance and enforcement**. National authorities' competences would be strengthened, as Parliament gives them the power to request access to both the trained and training models of the AI systems, including foundation models. Parliament also proposes to establish an AI Office, a new EU body to support the harmonised application of the AI act, provide guidance and coordinate joint cross-border investigations. In addition, Members seek to strengthen citizens' rights to file complaints about AI systems and receive explanations of decisions based on high-risk AI systems that significantly impact their rights.
- **Research and innovation**. To support innovation, Parliament agrees that research activities and the development of free and open-source AI components would be largely exempted from compliance with the AI act rules.

Policy debate latest issues. The recent and rapid development of general-purpose artificial intelligence technologies has framed the policy debate around, inter alia, defining general-purpose AI models, the application of the EU copyright framework to **generative AI**, how to ensure foundation models' compliance with AI Act principles, and the design of efficient auditing procedures for **large language models** (LLMs). A risk of **over-regulation** detrimental for investment in AI in the EU has been identified should overly stringent obligations of risk assessment, mitigation and management be imposed on **foundation models** and on SMEs. How to set pro-competitive rules for sandboxing and open-source AI systems has also been discussed. While there are concerns that AI poses societal-scale risks similar to nuclear weapons, calls for a pause in AI development have been made by civil society organisations, AI experts and tech executives. The question how to address dual-use and military AI applications has also been raised. Furthermore, given EU regulation will take time to take effect, the adoption of voluntary codes of conduct and of an AI Pact are envisaged to mitigate the potential downsides of generative AI. A pressing issue is to set a **common** terminology so that lawmakers around the globe have the same understanding of the technologies they need to address.

EP SUPPORTING ANALYSIS

General-purpose artificial intelligence, EPRS, Madiega T., March 2023.

Biometric Recognition and Behavioural Detection, European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, August 2021.

Regulating facial recognition in the EU, EPRS, Madiega T. A. and Mildebrath H. A., September 2021.

Artificial intelligence in criminal law, EPRS, Voronova S., September 2021.

Artificial Intelligence Act: Initial Appraisal of the European Commission Impact Assessment, Dalli H., EPRS, July 2021.

Artificial intelligence at EU borders: Overview of applications and key issues, Dumbrava C., EPRS, July 2021.

OTHER SOURCES

Artificial Intelligence Act, European Parliament, Legislative Observatory (OEIL).

Ebers M., and others, The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS), J 4, no 4: 589-603, October 2021.

Smuha N., and others, How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act, Elsevier, August 2021.

Veale M., Zuiderveen Borgesius F., Demystifying the draft EU AI Act, 22(4) *Computer Law Review International*, July 2021.

ENDNOTES

1 See European Commission, Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) 2021/0106 (COD), Explanatory memorandum (Commission proposal for an AI act). While the exact definition of AI is highly contested (see below), it is generally acknowledged that AI combines a range of technologies including machine-learning techniques, robotics and automated decision-making systems.

2 See for instance, High-Level Expert Group, Ethics Guidelines for Trustworthy AI, 2019.

3 See European Commission, Communication on Building Trust in Human-Centric Artificial Intelligence, COM(2019) 168.

4 See European Commission, Communication on Fostering a European approach to Artificial Intelligence, COM(2021) 205.

5 See European Commission, White Paper on Artificial Intelligence, COM(2020) 65 final.

6 For an overview see H. Dalli, Artificial intelligence act, Initial Appraisal of a European Commission Impact Assessment, EPRS, European Parliament, 2021.

7 According to the Commission impact assessment, the five specific characteristics of AI are (i) opacity (limited ability of the human mind to understand how certain AI systems operate), (ii) complexity, (iii) continuous adaptation and unpredictability, (iv) autonomous behaviour, and (v) data (functional dependence on data and the quality of data).

8 See Commission proposal for an AI act, Explanatory Memorandum and Recitals 1 and 5.

9 For the adoption of a harmonised set of requirements for AI systems.

10 For the adoption of specific rules for the processing of personal data in the context of biometric identification.

[11] The proposal complements both the sectoral product safety legislation, based on the new legislative framework (NLF) including the General Product Safety Directive, the Machinery Directive, the Medical Device Regulation and the EU framework on the approval and market surveillance of motor vehicles. The AI Act is also part of a broader EU regulatory framework comprising in addition the proposal for a new AI liability directive and the proposal for a revision of the product liability directive.

[12] See Article 2. The proposed regulation would also apply to the Union institutions, offices, bodies and agencies acting as a provider or user of AI systems.

[13] This covers the case of a service (digitally) provided by an AI system located outside the EU.

[14] See Council of Europe, Feasibility Study, Ad hoc Committee on Artificial Intelligence, CAHAI(2020)23 .

[15] OECD, Recommendation of the Council on Artificial Intelligence, 2019.

[16] See Article 3(1) and Recital 6.

[17] See impact assessment at pp. 48-49. A risk approach is also adopted in the United States Algorithmic Accountability Act of 2019 and in the 2019 Canadian Directive on Automated Decision-Making.

[18] FRTs would be allowed (i) for targeted search for potential victims of crime, including missing children, (ii) to prevent a specific, substantial and imminent threat to the life or physical safety of persons or of a terrorist attack, and (iii) for the detection, localisation, identification or prosecution of a perpetrator or individual suspected of a criminal offence referred to in the European Arrest Warrant Framework Decision.

[19] Harmonised standards are defined in accordance with Regulation (EU) No 1025/2012 and the Commission could, by means of implementing acts, adopt common technical specifications in areas where no harmonised standards exist or where there is a need to address specific safety or fundamental rights concerns.

[20] For an overview, see T. Madiega and H. Mildebrath, Regulating facial recognition in the EU, EPRS, September 2021.

[21] This section aims to provide a flavour of the debate and is not intended to be an exhaustive account of all different views on the proposal. Additional information can be found in related publications listed under 'EP supporting analysis'.

[22] For an in-depth analysis of the proposals and recommendations for amendments see N. Smuha and others, *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*, Elsevier, August 2021; M. Ebers, and others, *The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)*, J 4, no 4: 589-603, October 2021.

[23] N. Smuha, and others, above at pp. 14-15. See also E. Biber, Machines Learning the Rule of Law – EU Proposes the World's first Artificial Intelligence Act, August 2021. There are also calls for a shift in approach, to identify problematic practices that raise questions in terms of fundamental rights, rather than focusing on definitions; M. Veale and F. Zuiderveen Borgesius., Demystifying the draft EU AI Act, 22(4) *Computer Law Review International*, July 2021.

[24] See M. Ebers and others, above.

[25] See V. Galaz and others, Artificial intelligence, systemic risks, and sustainability, Vol 67, *Technology in Society*, 2021.

[26] For an overview, see T. Madiega and H. Mildebrath, above.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)

Second edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.