AI Act: Parliament and Council Reach Provisional Agreement on World's First AI Rules

Anna Pingen

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Anna Pingen
Researcher
Max Planck Institute for the Study of Crime, Security and Law

Published in
2023, Vol. 18(4) eucrim pp 316 – 317
ISSN: 1862-6947
https://eucrim.eu

After intense negotiations, the Council and the European Parliament reached a provisional agreement on the Artificial Intelligence (AI) Act. This legislation aims to ensure the safety of AI systems on the European market and respect for fundamental rights and stimulate investment and innovation in AI in Europe. The provisional agreement, which was announced on 9 December 2023, covers the following points:

Definition and scope

The definition of an AI system is aligned with the approach proposed by the Organisation for Economic Co-operation and Development (OECD): "An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments".

It is clarified that the regulation does not apply to areas outside the scope of EU law and should not affect Member States' competences in national security. The AI act will not apply to:

- Systems used exclusively for military or defense purposes;
- Systems solely used for research and innovation;
- People using AI for non-professional reasons.

Classification of AI systems as high-risk and prohibited AI practices

A horizontal layer of protection for AI systems is established, using a high-risk classification to avoid unnecessary regulation of low-risk AI. Limited-risk systems are subject to minimal transparency obligations.

A wide range of high-risk AI systems will be authorised but will have to comply with certain requirements and obligations in order to access the EU market. The co-legislators have refined these conditions to make them technically feasible and less burdensome for stakeholders, including data quality considerations and technical documentation for small and medium-sized enterprises (SMEs) to demonstrate compliance. The compromise agreement clarifies roles and responsibilities within AI value chains, in particular for providers and users. It also outlines the relationship between responsibilities in the AI Act and in existing legislation, ensuring consistency with data protection and sector-specific legislation.

The following applications of AI are recognized as posing an unacceptable risk to citizens' rights and democracy and are therefore prohibited:

- Biometric categorisation systems that use sensitive characteristics (e.g. political, religious, philosophical beliefs; sexual orientation; race);
- Untargeted scraping of facial images from the Internet or CCTV footage to create facial recognition databases;
- Emotion recognition in the workplace and educational institutions;
- Social scoring based on social behaviour or personal characteristics;
- AI systems that manipulate human behaviour to circumvent their free will;
- AI exploitation of the vulnerabilities of people (age, disability, social, or economic situation).

Exceptions for law enforcement authorities

Recognising the specificities of law enforcement authorities, several changes were agreed on for the use of AI systems for law enforcement purposes. In order to preserve their operational capabilities and respect the confidentiality of sensitive data, an emergency procedure was introduced to allow the use of a high-risk AI tool in urgent situations. However, a mechanism has also been put in place to ensure the protection of fundamental rights against potential misuse of AI systems.

With regard to real-time biometric remote identification systems in public places, the provisional agreement specifies the necessary objectives for law enforcement use and introduces additional safeguards. It also limits exceptions to cases involving victims of specific crimes and supports the prevention of genuine threats, such as terrorist attacks and searches for persons suspected of the most serious crimes.

Specific rules for General Purpose AI systems and foundation models

New provisions will address the use of AI systems for different purposes, in particular General Purpose AI (GPAI) technology integrated into high-risk systems. Specific rules have been outlined for foundation models where pre-market transparency obligations are required. A stricter regime is to be applied for "high impact" foundation models with advanced complexity and capabilities that may pose systemic risks along the value chain.

Governance structure

A new governance architecture will be established to oversee AI models under the AI Act. This includes the creation of an AI Office within the Commission, responsible for overseeing advanced AI models, setting standards, conducting testing, and enforcing common rules across Member States. A scientific panel of independent experts will advise the AI Office on GPAI models, in this way contributing to the development of evaluation methodologies, advising on high-impact models, and monitoring safety risks.

Sanctions

The AI Act provides for fines for violations, calculated as a percentage of the company's global annual turnover or a predetermined amount, whichever is higher. The fines are set at €35 million or 7% of global annual turnover for banned AI applications, €15 million or 3% for violations of obligations under the AI Act, and €7.5 million or 1.5% for providing incorrect information.

What's next?

It was agreed that the AI Act should apply two years after its entry into force, with certain exceptions for specific provisions. Work on the compromise text will now be continued at the technical level before a legal-linguistic revision is made. Afterwards, the text needs to be formally adopted by the Council and the European Parliament.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union