
Artificial Intelligence Act: MEPs adopt landmark law

-
- Safeguards on general purpose artificial intelligence
 - Limits on the use of biometric identification systems by law enforcement
 - Bans on social scoring and AI used to manipulate or exploit user vulnerabilities
 - Right of consumers to launch complaints and receive meaningful explanations
-



The untargeted scraping of facial images from CCTV footage to create facial recognition databases will be banned © Alexander / Adobe Stock

On Wednesday, Parliament approved the Artificial Intelligence Act that ensures safety and compliance with fundamental rights, while boosting innovation.

The regulation, [agreed in negotiations with member states in December 2023](#), was endorsed by MEPs with 523 votes in favour, 46 against and 49 abstentions.

It aims to protect fundamental rights, democracy, the rule of law and environmental sustainability from high-risk AI, while boosting innovation and establishing Europe as a leader in the field. The regulation establishes obligations for AI based on its potential risks and level of impact.

Banned applications

The new rules ban certain AI applications that threaten citizens' rights, including biometric categorisation systems based on sensitive characteristics and untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases. Emotion recognition in the workplace and schools, social scoring, predictive policing (when it is based solely on profiling a person or assessing their characteristics), and AI that manipulates human behaviour or exploits people's vulnerabilities will also be forbidden.

Law enforcement exemptions

The use of biometric identification systems (RBI) by law enforcement is prohibited in principle,

except in exhaustively listed and narrowly defined situations. “Real-time” RBI can only be deployed if strict safeguards are met, e.g. its use is limited in time and geographic scope and subject to specific prior judicial or administrative authorisation. Such uses may include, for example, a targeted search of a missing person or preventing a terrorist attack. Using such systems post-facto (“post-remote RBI”) is considered a high-risk use case, requiring judicial authorisation being linked to a criminal offence.

Obligations for high-risk systems

Clear obligations are also foreseen for other high-risk AI systems (due to their significant potential harm to health, safety, fundamental rights, environment, democracy and the rule of law). Examples of high-risk AI uses include critical infrastructure, education and vocational training, employment, essential private and public services (e.g. healthcare, banking), certain systems in law enforcement, migration and border management, justice and democratic processes (e.g. influencing elections). Such systems must assess and reduce risks, maintain use logs, be transparent and accurate, and ensure human oversight. Citizens will have a right to submit complaints about AI systems and receive explanations about decisions based on high-risk AI systems that affect their rights.

Transparency requirements

General-purpose AI (GPAI) systems, and the GPAI models they are based on, must meet certain transparency requirements, including compliance with EU copyright law and publishing detailed summaries of the content used for training. The more powerful GPAI models that could pose systemic risks will face additional requirements, including performing model evaluations, assessing and mitigating systemic risks, and reporting on incidents.

Additionally, artificial or manipulated images, audio or video content (“deepfakes”) need to be clearly labelled as such.

Measures to support innovation and SMEs

Regulatory sandboxes and real-world testing will have to be established at the national level, and made accessible to SMEs and start-ups, to develop and train innovative AI before its placement on the market.

Quotes

During the plenary debate on Tuesday, the Internal Market Committee co-rapporteur [Brando Benifei \(S&D, Italy\)](#) said: “We finally have the world’s first binding law on artificial intelligence, to reduce risks, create opportunities, combat discrimination, and bring transparency. Thanks to Parliament, unacceptable AI practices will be banned in Europe and the rights of workers and citizens will be protected. The AI Office will now be set up to support companies to start complying with the rules before they enter into force. We ensured that human beings and European values are at the very centre of AI’s development”.

Civil Liberties Committee co-rapporteur [Dragos Tudorache \(Renew, Romania\)](#) said: “The EU has delivered. We have linked the concept of artificial intelligence to the fundamental values that form the basis of our societies. However, much work lies ahead that goes beyond the AI Act itself. AI will push us to rethink the social contract at the heart of our democracies, our education models, labour markets, and the way we conduct warfare. The AI Act is a starting point for a new model of governance built around technology. We must now focus on putting this law into practice”.

Next steps

The regulation is still subject to a final lawyer-linguist check and is expected to be finally adopted before the end of the legislature (through the so-called [corrigendum](#) procedure). The law also needs to be formally endorsed by the Council.

It will enter into force twenty days after its publication in the official Journal, and be fully applicable 24 months after its entry into force, except for: bans on prohibited practises, which will apply six months after the entry into force date; codes of practise (nine months after entry into force); general-purpose AI rules including governance (12 months after entry into force); and obligations for high-risk systems (36 months).

Background

The Artificial Intelligence Act responds directly to citizens’ proposals from the Conference on the Future of Europe (COFE), most concretely to [proposal 12\(10\)](#) on enhancing EU’s competitiveness in strategic sectors, [proposal 33\(5\)](#) on a safe and trustworthy society, including countering disinformation and ensuring humans are ultimately in control, [proposal 35](#) on promoting digital innovation, (3) while ensuring human oversight and (8) trustworthy and responsible use of AI, setting safeguards and ensuring transparency, and [proposal 37 \(3\)](#) on using AI and digital tools to improve citizens’ access to information, including persons with disabilities.

Further information

[Link to adopted text \(13.03.2024\)](#)

[Plenary debate \(12.03.2024\)](#)

[Press conference on the plenary vote \(13.03.2024\)](#)

[Procedure file](#)

[EP Research Service: compilation of studies on Artificial Intelligence](#)

[Result of roll-call votes \(13.03.2024\)](#)

[Committee on the Internal Market and Consumer Protection](#)


[Committee on Civil Liberties, Justice and Home Affairs](#)

Contacts

Yasmina YAKIMOVA

Press Officer

 (+32) 2 28 42626 (BXL)


 (+32) 470 88 10 60

 yasmina.yakimova@europarl.europa.eu

 [@EP_SingleMarket](https://twitter.com/EP_SingleMarket)

Janne OJAMO

Press Officer

 (+32) 2 284 12 50 (BXL)

 (+32) 470 89 21 92

 janne.ojamo@europarl.europa.eu

 [@EP_Justice](https://twitter.com/EP_Justice)
