# Artificial Intelligence Act

2021/0106(COD) - 13/03/2024 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 523 votes to 46, with 49 abstentions, a legislative resolution on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts.

The European Parliament's position adopted at first reading under the ordinary legislative procedure amends the proposal as follows:

***Subject matter***

The purpose of this Regulation is to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter of Fundamental Rights, including democracy, the rule of law and environmental protection, against the harmful effects of artificial intelligence systems (AI systems) in the Union, and to support innovation.

This Regulation does not apply to AI systems or AI models, including their output, specifically developed and put into service for the sole purpose of scientific research and development.

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.

This Regulation applies to AI systems released under free and open source licences, unless they are placed on the market or put into service as high-risk AI systems.

***AI literacy***

Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

***Prohibited AI Practices***

The new rules prohibit the following AI practices:

- AI system that deploys **subliminal techniques** beyond a person’s consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of, materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing a person to take a decision that that person would not have otherwise taken;

- AI system that exploits any of the **vulnerabilities of a person or a specific group of persons due to their age, disability or a specific social or economic situation**, with the objective, or the effect, of materially distorting the behaviour of that person;

- AI systems with **social scores** (classification of natural persons based on their social behaviour or known, inferred or predicted personal or personality characteristics);

- AI system for making **risk assessments of natural persons** in order to assess or predict the likelihood of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics;

- AI systems that create or expand **facial recognition databases** through the untargeted scraping of facial images from the internet or CCTV footage;

- AI systems to **infer emotions** of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons;

- **biometric categorisation systems** that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation;

- **'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement**, unless and in so far as such use is strictly necessary for one of the following objectives: (i) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as searching for missing persons; (ii) the prevention of a genuine threat of a terrorist attack; (iii) the identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation, prosecution or executing a criminal penalty for offences punishable by a custodial sentence of a maximum duration of at least four years.

The use of the real-time remote biometric identification system in publicly accessible spaces should be authorised only if the relevant law enforcement authority has completed a **fundamental rights impact assessment**. In addition, their use remains limited to what is strictly necessary concerning the period of time as well as the geographic and personal scope. In any case, no decision producing an adverse legal effect on a person should be taken based solely on the output of the remote biometric identification system.

***Obligations for high-risk systems***

The Regulation lays down 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).

The following have been added to the list of high-risk systems, in particular, systems intended to be used:

- as safety components in the management and operation of **critical digital infrastructure**, road traffic and the supply of water, gas, heating and electricity;

- to determine the access, admission or assignment of individuals to **educational and vocational training establishments**, at all levels;

- for the recruitment or selection of natural persons, in particular for publishing **targeted job offers**, analysing and filtering applications and evaluating candidates;

- to assess the eligibility of individuals for essential **social security benefits** and services, including healthcare services;

- for risk assessment and pricing of **life and health insurance** for individuals;

- in the context of **migration, asylum and border control management**, for the purposes of detecting, recognising or identifying natural persons;

- to **influence the outcome of an election or referendum** or the electoral behaviour of natural persons in the exercise of their vote.

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.

***General-purpose AI (GPAI)***

General-purpose AI systems, and the GPAI models such as ChatGPT 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.