WilhelmGilliéron

AVOCATS

TECH & DATA

The EU AI Act – Subject matter and scope

Auteur: Wilhelm Avocats | Le : 8 February 2024

# The EU AI Act – Subject matter and scope

This is the first of our series papers related to the EU AI Act.

On February 4th, 2024, EU countries gave crucial final nod to the first-of-a-kind Artificial Intelligence Law as Luca Bertuzzi put it. As stated by Luca Bertuzzi, "*The European Parliament's Internal Market and Civil Liberties Committees will adopt the AI rulebook on 13 February, followed by a plenary vote provisionally scheduled for 10-11 April. The formal adoption will then be complete with endorsement at the ministerial level. The AI Act will enter into force 20 days after publication in the official journal. The bans on the prohibited practices will start applying after six months, whereas the obligations on AI models will start after one year. All the rest of the rules will kick in after two years, except for the classification of AI systems that have to undergo third-party conformity assessment under other EU rules as high-risk, which was delayed by one additional year*".

Taking into account the fact that, so far, the final text has only been published in English, this series papers will only be released in English to ensure that we stick to the official version and its wording.

## 1. Subject matter of the EU AI Act – notion of artificial intelligence

### *a) Underlying principles*

The EU has chosen a human centric approach to the regulation of AI, which is heavily based on the seven principles adopted on April 8, 2019 by the High-Level Expert Group in its Ethic Guidelines for Trustworthy AI, namely:

- *Human agency and oversight*: AI systems should be developed and used as tools to serve people, respect human dignity and remain under the control of human beings, with the ultimate aim of increasing human well-being.
- *Technical robustness and safety*: AI systems should be developed and used in a way that allows robustness in case of problems and resilience against attempts to alter the use and performance of the AI system.
- *Privacy and data governance*: AI systems should comply with existing data protection laws and regulations, while processing should meet high standards in terms of quality and integrity.
- *Transparency*: AI systems should be developed and used in a way that allows appropriate traceability and explainability, while making humans aware that they interact with an AI system, as well as duly informing users of the capabilities and limitations of the AI system and affected individuals about their rights.
- *Diversity, non–discrimination and fairness*: AI systems should be developed and used in a way that include diverse actors and promotes equal access, gender equality and cultural diversity, while avoiding discriminatory impacts and unfair biases.
- *Social environment well–being*: AI systems should be developed and used in a sustainable and environmental friendly, as well as in a way to benefit all human beings.

These principles, which are largely in line with the OECD AI Principles, should be taken into account in the design and use of AI models, a goal that the EU AI Act tries to achieve in setting up a robust regulatory framework. They should also serve as basis for the drafting of codes of conduct under the Regulation.

### *b) Underlying principles*

While the notion of AI leads to endless discussions, the EU AI Act has finally rightfully decided to opt for a definition with mirrors the one retained by international organizations such as the OECD, so as to ensure legal certainty, facilitate international convergence and wide acceptance. That notion is based upon key characteristics of an AI system in comparison with traditional software or programming approach, namely (1) capability to infer, (2) using techniques such as machine learning approaches enabling such inferences, which (3) are designed to operate with varying levels of autonomy. These characteristics have led to the following definition:

"*An AI system is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, after 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*".

## 2. Scope of the EU AI Act

### *a) Material scope*

The EU AI Act does not apply to the following activities:

- *Personal non-professional activity for individuals* (art. 1.5c);

Interestingly, this means that use of an AI system or model built within a group and used internally would still be submitted to the requirements of the EU AI Act.

- AI systems and models, including their output, specifically developed and put into service for the sole purpose of *scientific research and development* (AI systems as a research tool) (art. 1.5a);

- *Research, testing and development activities on AI systems* or models prior to such systems or models being placed on the market or put into service (research on AI systems) (art. 1.5b);

- *Military and national security* (art. 1.3); provided, however, that such systems shall exclusively be used for such purposes. The Commission considered that public international law is the appropriate legal framework to regulate the use of lethal forces, respectively that national security remains the sole responsibility of Member States.

  Two remarks there: first, in a world of uncertainty, we may already fear that the notion of "national security" will enjoy wide discretion and may lead to discretionary exclusions of what is considered as a "national security" concern. Second, AI systems and models will remain or become subject to the requirements laid down in the EU AI Act as soon as they are used for purposes other than military. Taking into account the fact that dual use systems are likely to exist, authorities will have to pay attention to the use made of such systems and ensure that they are only exempted from complying with the requirements of the EU AI Act if their use remains limited to military or national security purposes.

- *AI systems released under free and open source licenses*; provided, however, that they do amount to prohibited practices, high-risk systems or general models submitted to the transparency obligations laid down in Title IV (art. 1.5g).

  While the preamble does not seem to expressly refer to this exclusion, the *underlying rationale* probably stems from the fact that the open source nature of these AI systems and models will enable third parties to assess their compliance with the above mentioned principles. Taking into account the fact that these systems will however remain submitted to the requirements put down by the EU AI Act if they are considered as a prohibited practice, high-risk system or general models, the requirements set out in the EU AI Act will however ultimately remain largely applicable to them.

- *Public authorities in a third country or international organizations using AI systems for law enforcement and judicial cooperation*; provided however, that these third countries provide an adequate level of protection to fundamental rights.

### *b) Geographical scope*

The EU AI Act aims at applying to the whole supply chain of AI systems, from their manufacturing to their use. As a result, it lays down obligations to developers (defined as "providers"), distributors, importers, as well as users (defined as "deployers"). Interestingly, the EU AI Act also refers in part to the notion of "product manufacturer", which is understood as being part of the "operators" along with the above-mentioned concepts, but without defining it on its own or laying down specific obligations upon the "product manufacturer". While I tend to consider that "product manufacturers" seem to be fairly close to "developers" and may therefore potentially be submitted to the same obligations, the fact that the notion of "operator" seems to make a distinction between both terms leave some uncertainty that will need to be clarified.

In an approach that reminds us of the GDPR, the EU AI Act adopts an extra-territorial approach (art. 2).

The EU AI Act will therefore apply to:

- Developers, product manufacturers, importers, distributors as well as users of AI systems and models that have their place of establishment or who are located in the Union.

- Developers of such systems (including general-purpose AI models) who place them on the market or put them into service in the Union, irrespective of their place of establishment (*i.e.* also potentially outside the Union).

  This in particularly means that any such AI system or model that may be accessed to and used from EU deployers notably through a web interface (such a general-purpose AI models in particular), will always be submitted in my understanding to the EU AI Act, as such access will lead to placing such systems and models on the market in the EU.

- Developers and users who are located outside of the EU, but whose output generated by their AI systems is used in the Union.

  In most instances, the generation of an output in the EU will imply that the AI system is put on the market or in service in the EU. One may however foresee cases where such AI systems may only be made available and accessible in third party countries, but where users (notably for instance in a group of companies such as insurances, banks, etc.) would share and use the output generated by such systems to affiliates, subsidiaries or even third parties based in the EU. In such cases, both developers and users of such systems would be submitted to the EU AI Act (at the exclusion, in my understanding, of the recipient of such output that does not seem to be considered in itself as using the AI system).

This was the first of our series paper on the EU AI Act. Next week, we shall focus on the classification and provide an analysis of the prohibited practices and general-purpose AI models.

---

***Source : https://www.wg-avocats.ch/en/actualites/intellectual-property/the-eu-ai-act-subject-matter-and-scope/***