EU Proposes New Artificial Intelligence Regulation

Kluwer Competition Law Blog
April 16, 2021

Jay Modrall (Norton Rose Fulbright, Belgium)

Please refer to this post as: Jay Modrall, 'EU Proposes New Artificial Intelligence Regulation', Kluwer Competition Law Blog, April 16 2021, http://competitionlawblog.kluwercompetitionlaw.com/2021/04/16/eu-proposes-new-artificial-intelligence-regulation/

On April 21, 2021, the EU Commission adopted a proposal for a regulation (the AI Regulation) on "artificial intelligence systems" (AI systems), which it describes as "the first-ever legal framework on AI." The AI Regulation will impose significant obligations impacting businesses across many, if not all, sectors of the economy. The AI Regulation will prove controversial, touching off a legislative battle lasting at least until 2022.

The proposed AI Regulation will join other ambitious EU initiatives in the digital sector, such as the Data Governance Act, Digital Services Act and Digital Markets Act, currently working their way through the EU legislative process, as well as the forthcoming Data Act and the ongoing reform of EU antitrust policy. Some of the AI Regulation provisions read across to related provisions in other measures; for example, the practices prohibited for all AI systems (see below) are related to the Digital Services Act measures to combat harmful content on the Internet.

The AI Regulation defines "AI systems" broadly and imposes tailored obligations on actors at different parts of the value chain, from "providers" of AI systems to manufacturers, importers, distributors and users. The AI Regulation imposes especially strict obligations in relation to "high-risk AI systems."

On the other hand, the AI Regulation includes a number of provisions intended to promote the development and uptake of AI systems in the European Union (EU). The AI Regulation also creates a new regulatory framework, with a European Artificial Intelligence Board overseeing and coordinating enforcement. The AI Regulation envisages a two-year period for application following adoption and publication of the final regulation, meaning that the new requirements could apply as early as 2024.

Scope

The AI Regulation defines AI systems as "software that is developed with one or more of [certain] approaches and techniques . . . 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." The definition is likely to be subject to close scrutiny and possible amendment, but the Commission clearly intends to cast a wide net, capturing not only AI systems offered as stand-alone software products but also products and services relying on AI services directly or indirectly.

The techniques and approaches leading to software being identified as an AI system (listed in Annex I) include machine learning (including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning); logic- and knowledge-based approaches (including knowledge representation, inductive (logic) programming, knowledge bases, inference/deductive engines, (symbolic) reasoning and expert systems); and statistical approaches, Bayesian estimation, search and optimization methods. Although this definition may be questioned from a technical perspective, again the intention seems to be to cast a wide net. Interestingly, the definition of AI systems presented in Annex I is limited to existing methods, and does not allow for future innovations in how AI systems operate (for example, by the use of methods analogous to non-human forms of intelligence).

AI systems identified as "high-risk AI systems" are those intended to be used as "safety components" of products, or which are themselves products, covered in EU legislation listed in Annex II (e.g., on machinery, toys, lifts/elevators, radio equipment, pressure equipment, marine equipment, cableways, gas-burning appliances, and medical devices), and AI systems listed in Annex III (those related to biometric identification and categorization of natural persons; management and operation of critical infrastructure; education and vocational training; employment, works 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; and administration of justice and democratic processes). "Safety components" are defined as components of a product or system that fulfil a safety function and whose failure and/or malfunctioning endangers the health and safety of persons and property.

Practices Prohibited for all AI Systems (Title II)

The AI Regulation will prohibit certain practices for all AI systems as violating EU values and fundamental rights. These include placing on the market or into service, or using, AI systems that:

- deploy subliminal techniques beyond a person's consciousness to materially distort a person's behaviour in a manner that causes or is likely to cause harm;
- exploit vulnerabilities of a group due to their age, physical or mental disability to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause harm; or
- evaluate or classify the trustworthiness of natural persons based on their social behaviour or known or predicted personal or personality characteristics, leading to detrimental or unfavourable treatment.

The use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement is permitted only insofar as strictly necessary for specified objectives, taking into account certain elements. Such uses must also comply with safeguards and conditions, in particular as regards temporal, geographic and personal limitations.

As mentioned, the practices prohibited in relation to all AI systems should be viewed in connection with proposed measures to address harmful content on the Internet, notably in the Digital Services Act proposal.

Obligations for High-Risk AI Systems, Providers and Users (Title III)

Requirements for high-risk AI systems include implementing a risk management system for the entire life cycle of a high-risk AI system to (among other things) eliminate or reduce risks through adequate design and development, implementing mitigation and control measures, providing information and training, and conducting testing. The AI Regulation further imposes extensive obligations in relation to data and data governance; technical documentation and record-keeping; transparency and provision of information; human oversight; and accuracy, robustness, and cybersecurity.

The obligations imposed on businesses distinguish between providers of high-risk AI systems, product manufacturers, authorized EU representatives appointed by non-EU providers, importers, distributors, users, and other third parties involved in the AI value chain. Providers of high-risk AI systems are responsible for ensuring the compliance of their systems with the AI Regulation, implementing a quality management system, drawing up the relevant technical documentation, keeping logs generated by their high-risk AI systems, complying with conformity assessment and registration obligations, taking corrective actions as required and cooperating with authorities. Manufacturers of products covered by EU legislation and including high-risk AI systems are responsible for compliance as if they were the provider of the high-risk AI system.

Distributors, importers, users and other third parties will also be subject to providers' obligations if they place a high-risk AI system on the market or into service under their name or trademark, modify the intended purpose of a high-risk AI system already on the market or in service or make a substantial modification to a high-risk AI system. In that case, the original provider is relieved of responsibility.

The AI Regulation also imposes obligations on users of high-risk AI systems. Users must use such systems in accordance with the instructions for use, ensure that input data is relevant, and monitor the operation of the high-risk AI system based on the instructions. Users also have various record-keeping and information requirements. Credit institutions using AI systems are singled out for specific obligations.

Title III also includes extensive procedural requirements relating to the bodies responsible for performing conformity assessments and possible challenges to their decisions. Products including AI systems as safety components, or AI system safety components that are themselves products, must undergo third-party testing known as a "conformity assessment" before being placed on the market or put into service. The use of harmonized technical standards is encouraged to facilitate conformity assessments.

High-risk AI systems will be registered, and the EU will maintain a database including information inputted by AI system providers. This information, as set out in an annex, includes information on the provider, the AI system trade name and any additional unambiguous reference allowing identification and traceability of the AI system; a description of the intended purpose of the AI system; the status of the AI system (on the market, no longer placed on the market, recalled); the type, number and expiry date of the certificate issued by the notified body and the name or identification number of that notified body; a copy of the conformity certificate (where required); Member States in which the AI system is to or has been placed on the market, put into service or made available; electronic instructions for use; and a URL for additional information (optional).

Transparency Obligations (Title IV)

Certain AI systems are subject to additional transparency obligations. These include AI systems intended to interact with natural persons, systems for emotion recognition or biometric categorization, and systems that generate "deep fakes."

Supporting Innovation (Title V)

In addition to the extensive obligations imposed on the development, distribution and use of AI systems, the AI Regulation contains a number of measures intended to support innovation in this area. These include support for regulatory sandbox schemes, reduction of regulatory burdens for small and medium-sized enterprises and startups, and the creation of digital hubs and testing facilities.

Governance and enforcement (Titles VI-X)

The AI Regulation creates a fully-fledged regulatory and enforcement regime overseen by a European Artificial Intelligence Board working with national supervisory authorities entrusted with ensuring the application and implementation of the regulation.

The AI Regulation also provides for an EU database for stand-alone high-risk AI systems. Information will be entered by high-risk AI system providers and accessible to the public. High-risk AI system providers will also be required to establish post-market monitoring systems to collect, document and analyze data on the performance of high-risk AI systems and their compliance with the regulation.

Providers of high-risk AI systems will be required to report on serious incidents and malfunctioning of those systems immediately after establishing a link between the system and the incident. National supervisory authorities will report to the Commission on their market surveillance activities and coordinate those activities. Member States objecting to a measure taken by another Member State, or the Commission can trigger a "Union safeguard procedure." National authorities can also require operators to take appropriate measures where an AI system presents a risk to health or safety or fundamental rights even though in

compliance with the regulation.

The Commission and Member States will encourage the creation of codes of conduct to foster the application of requirements applicable to high-risk AI systems to other AI systems based on appropriate specifications and solutions.

An elaborate system of penalties will be available for infringements of the AI Regulation. The highest fines may be up to 6% of total worldwide annual revenue for non-compliance with the prohibition of practices for all AI systems and data and data governance requirements.

Key Takeaways

The AI Regulation represents a major legislative initiative that may serve as a template for similar measures around the globe. It imposes broad obligations in relation to all AI systems from providers to users; prohibits certain AI practices entirely; imposes special obligations in relation to high-risk AI systems; and creates a new framework of regulators and testing, monitoring and compliance processes. The broad definition of AI systems ensures that the AI Regulation will have a significant impact in all sectors of the economy, not only digital.

Before it can be adopted, however, the AI Regulation will join an already crowded digital docket and must pass through a complex and contentious legislative process. The AI Regulation is consistent with the broad outlines of EU policy set out in the Commission's February 2020 AI strategy paper, so there are few if any complete surprises. However, the broad and potentially vague definitions highlight the difficulty of translating general principles into enforceable legislation.

Similarly, the extensive obligations imposed on providers, manufacturers, importers, distributors and users of AI systems will be daunting for all but the largest companies, and the new governance and enforcement regime will add to an increasingly dense regulatory forest in Europe. These obligations will likely shape regulatory expectations in relation to non-high-risk AI systems. As the AI Regulation and related measures move through the EU legislative process, hopefully, the EU institutions will streamline and rationalize the new regulatory frameworks to minimize duplication and clarify areas of responsibility.