EU Retains Role of Lead AI Regulator with Signing of EU AI Act

DECEMBER 18, 2023

PAMELA M. DEESE, EMILY B. LEWIS

It is no secret that European regulators are moving with greater speed in the regulation of artificial intelligence (AI) than their counterparts in the United States. In comparison, the United States, after months of hearings and discussions, continues to work toward the first piece of bipartisan legislation on the issue of AI regulation.

On December 8, after roughly 37 hours of talks and negotiations, the European Commission, European Council, and European Parliament announced the first-of-its-kind European Union (EU) AI Act. Recognizing the new risks and potential negative consequences that accompany the economic and societal benefits of AI, the Act aims to be "human centric," regulating AI technologies in ways that are intended to limit risk and provide for safe use, while also encouraging businesses to developing AI-based solutions.

The AI Act is expected take effect in 2026, though companies are being encouraged to begin implementing its requirements much sooner by updating their codes of conduct.

Goals and Scope of the AI Act

The priority of the AI Act is to foster a safer technological landscape, requiring human oversight of AI systems as opposed to automated systems. The implications of the AI Act are far-reaching, given who and what it aims to police. The scope of **the AI Act** is quite broad, with consequences extending beyond technological providers located in the EU. Indeed, the AI Act will apply to anyone or entity that offers AI system services in any market in the EU, regardless of whether they are established within the EU or a third country, including the United States. It will also apply to users of AI systems within the EU, and providers and users of AI systems located in a third country if any outputs produced by such systems are used in the EU.

Overall, the AI Act governs how AI systems and services will be able to be placed into the EU market and how they may be used following placement. Additionally, it will prohibit certain AI practices and impose transparency rules for systems intending to interact with "natural persons," as well as those generating or manipulating image, audio, or video content. Further, the AI Act will require compliance with certain rules involving market monitoring and surveillance. Importantly, the Act follows a risk-based approach, differentiating each use of AI by assessing whether there is an unacceptable, high, or low to minimal risk. Each type of risk will be subject to different levels of regulation.

A fulsome list of prohibited practices is included in an annex to the Act. Further, the Act chiefly bans practices that "contravene EU values" by violating certain fundamental rights delineated in the EU Charter of Fundamental Rights, including the right to human dignity, the rights to protection of personal data and non-discrimination, and equality among men and women.

Though critics have already voiced concern on what may be seen as controversial points, the Act explicitly states that it aims to ***prevent*** a chilling effect on the rights of free speech and expression. That being said, the Act also makes a clear admission that imposes some restrictions on other First Amendment-type provisions of the Charter, including those involving the freedom to conduct business and the freedom of art and science. To defend the decision to regulate in these spaces, the Act states that it has an overriding interest in protecting other fundamental rights threatened by high-risk AI technology, and **insists that** the restrictions are proportionate and limited to the minimum necessary to prevent and mitigate serious safety risks and infringements of other fundamental rights.

Tiers of Risk

Systems that are considered to have unacceptable risk, including those that threaten the safety and livelihoods of individuals, are **banned** outright under the Act. These systems include those involving cognitive behavioral manipulation of specific vulnerable groups, for instance, voice-activated toys that

encourage dangerous behaviors in children, those that involve any type of social scoring (***i.e.***, those that classify individuals based on socio-economic status or behaviors), and those using real-time biometric identification systems in public spaces for law enforcement. Such uses of biometric identification systems are considered particularly intrusive, as they may evoke a feeling of constant surveillance and dissuade the exercise of the freedom of assembly, along with the deployment of other fundamental rights.

High risk AI systems will be heavily regulated by the AI Act and will be required to comply with certain obligations before being made available for use. Such systems include those involving critical infrastructures, such as transportation, that could put at risk the health and safety of the citizenry, law enforcement, employment, and democratic processes. Before they can be offered on the market, high-risk AI systems must demonstrate that they have in place a number of safeguards, including, but not limited to, risk assessment and mitigation systems, maintenance of activity logs to ensure traceability of results, and human oversight measures to minimize risk. Upon satisfying stringent requirements mandated by the Act and being placed on the market, high-risk systems will still be subject to strict surveillance and human oversight to ensure potential threats are managed and human safety is being protected.

Finally, AI systems of limited risk are also covered by the Act. Examples of limited risk systems include generative AI (GenAI), deep fakes, and chatbots such as ChatGPT. Limited-risk systems will face only minimal transparency obligations, including the requirement to disclose AI-created content, implement a model to prevent illegal content generation, and publish summaries of copyrighted data used for AI training. Despite these minimal requirements, some businesses with limited-risk AI systems may choose to adopt a more intensive code of conduct in order to brand themselves as promoters of increased public safety and risk management. In fact, the AI Act encourages these systems to comply with restrictions imposed upon high-risk systems to further foster a safe AI landscape.

Next Steps

As referenced above, the United States is lagging behind the EU in terms of AI regulation, a gap that has only widened with the announcement of the EU AI Act. It will be interesting to see how companies that will face scrutiny under the AI Act respond and revise their codes of conduct and internal protective mechanisms, and whether this legislation will have the effect of expediting the bipartisan framework currently being developed in the United States at the federal level. While the United States may borrow some concepts from the EU's framework as it continues to draft its own, officials will need to exercise caution. Some of the restrictions implemented by the EU Act may run afoul of certain constitutional protections, including but not limited to the First Amendment.

The AI, Metaverse & Blockchain team at ArentFox Schiff will continue to monitor the EU AI Act and its repercussions as they unfold, as well as the impacts that the AI Act may have for legislators and thus businesses in the United States.

Please contact your AFS attorney or either author should you have questions or concerns.

Contacts

Pamela M. Deese
PARTNER

Emily B. Lewis
ASSOCIATE