

Understanding EU's AI Act And Its Enforcement Mechanisms

By **Matthew Justus and Wade Barron** (September 22, 2023)

Until recently, businesses have employed artificial intelligence technology with few restrictions because AI has remained largely unregulated.

However, on June 14, the European Parliament — the main legislative branch of the European Union — passed a draft version of the Artificial Intelligence Act that would constitute the first major legislation to regulate AI.[1]

By enacting this legislation, the EU hopes to balance promotion of further innovations related to AI technologies and the various risks posed by AI.[2]

The AI Act could go into effect as early as 2024. As currently written, the act bans AI tools that pose unacceptable risk and regulates high-risk AI tools such as requiring the implementation of risk management systems.

Failure to comply with the act's regulations could result in fines of up to €40 million (\$42.8 million) or up to 7% of a company's worldwide annual revenue. The act reaches any organization that markets or uses AI tools in the EU or provides the output of AI tools in the EU.

The draft legislation is still subject to change as passage will require further negotiations among the EU's three major decision-making bodies.

However, once the act has been implemented, companies wishing to continue using or marketing AI technology in EU countries, or even providing output from AI systems in EU countries, will need to become familiar with these new rules or risk serious penalties.

This article begins with an overview of the act's risk-based regulatory framework and then discusses enforcement mechanisms, including financial penalties and how organizations can take steps now to avoid those penalties. Finally, the article looks at the next steps for the act as it moves closer to becoming law.

Regulatory Framework

As currently written, the act broadly defines the AI technologies that fall within its regulatory scheme. Specifically, the act defines artificial intelligence to mean a machine-based system that is designed to operate with varying levels of autonomy that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations or decisions that influence physical or virtual environments.[3]

The act also specifies that an AI system can be used as stand-alone software system, integrated into a physical product, used to serve the functionality of a physical product without being integrated therein or used as an AI component of a larger system.

In addition, the act considers any system that would not be able to function without an AI



Matthew Justus



Wade Barron

component to be one single AI system. This definition modifies the act's initial definition of AI to focus more on the machine learning and generative components of AI.

The EU Parliament intends for the current definition to ensure legal certainty, harmonization and wide acceptance, while providing the flexibility to accommodate the rapid technological developments in AI.

The act makes clear that its regulatory framework applies to EU and non-EU countries alike, stating that its regulations govern any organization placing on the market or putting into service AI systems in the union, irrespective of whether the organization is located within the EU.

Additionally, if the output of an AI system is intended to be used in the EU, the act also applies.

The act regulates AI using a risk-based system that differentiates between uses of AI that create:

- An unacceptable risk;
- A high risk; and
- Low or minimal risk.

The act provides extensive descriptions of what technologies fall within the unacceptable-risk and high-risk categories. AI deemed to pose an unacceptable risk is prohibited outright. AI that poses an unacceptable risk includes all those AI systems whose use is considered unacceptable as contravening EU values, for instance by violating fundamental rights.

In line with this broad definition, the act prohibits any AI system that uses subliminal techniques that would distort a person's behavior in such a way that it would likely cause that person or another person harm, as well as any AI systems that would exploit the vulnerabilities of any group due to their age or disability.

In addition, the act bans the use of real-time remote biometric identification in publicly accessible spaces for the purpose of law enforcement except under limited circumstances. The act also bans using AI for the social scoring evaluation or classification of natural persons or groups thereof over a certain period of time based on their social behavior.

The act defines social scoring as evaluating or classifying natural persons based on their social behavior, socio-economic status or known or predicted personal or personality characteristics.

Initially, the ban on social scoring only extended to public authorities or those acting on their behalf. However, the EU Parliament removed the "public authorities" language from the most recent version of the act, indicating that it would apply to private businesses as well.

The act also places several requirements on AI that present a high risk, defined to include AI technology that meets certain criteria and is intended to be used as a safety component of another product, or that otherwise falls under a discreet group of AI systems listed in Annex III of the act.

The AI systems listed in Annex III include:

- Biometric and biometrics-based systems;
- Management and operation of critical infrastructure;
- Educational and vocational training;
- Worker management and access to self-employment;
- Access to and enjoyment of essential private and public services;
- Law enforcement;
- Asylum and border control management; and
- Administration of justice and democratic processes.

In the most recent version of the act, the EU Parliament clarifies that the AI systems included in Annex III would only constitute a high risk if they posed a significant risk to a person's health, safety or individual rights.

It also added to the high-risk category AI systems that could influence voters or AI systems used by large social media companies to recommend user-generated content.

Organizations that employ high-risk AI systems must establish, implement and maintain a risk management system. The risk management system must be a continuous iterative process that runs throughout the entire lifecycle of the AI system.

Among other things, the risk management system must identify and analyze foreseeable risks associated with the AI systems and estimate and evaluate risks that may emerge from them. An organization intending to use or market a high-risk AI system must draw up technical documentation that demonstrates that the AI system will be subject to a risk management system.

AI systems classified as high risk must also make use of data sets that meet specific quality control criteria. The act outlines several specifications for training, validating and testing data sets implemented in models used by AI systems. These data sets must be tailored to the geographical, behavioral and functional setting where the high-risk AI systems are used.

The act further requires that high-risk AI systems be developed with appropriate human-machine interface tools so that they can be overseen by humans. The humans charged with oversight of high-risk AI systems must meet specific AI literacy requirements and must act to prevent or minimize risks posed by the AI system to both the environment and the health, safety and fundamental right of individuals.

AI systems that fall outside of the unacceptable or high-risk categories may remain subject to some regulations under the act, primarily concerning transparency. Specifically, any organizations that intends for its AI system to interact with humans must inform those individual users that they are interacting with an AI system if it is not readily apparent.

The act also requires disclosure concerning whether a human is overseeing the AI system's decision-making process as well as any potential rights users may have to object to the application of AI.

In addition, if an AI system is used to generate or manipulate text, audio or visual content that falsely presents someone doing or saying something then it must be disclosed that the content was created through the use of AI. All other AI systems — such as spam filters — are not subject to any regulations under the act.

Regulatory Penalties and Preparation for Compliance

To enforce its regulatory framework, the act comes with stiff penalties. The act initially provided for fines of up to €30 million (\$32 million) — or up to 6% of a company's worldwide annual revenue — for failure to comply with the ban on AI in the unacceptable-risk category.

However, the EU Parliament increased the maximum penalty to €40 million or up to 7% of a company's worldwide annual revenue, whichever is higher. The act requires all member nations to create regulatory agencies to implement their own rules to enforce these penalties.

Given these severe penalties, any organization that plans to make use of technology incorporating AI within the EU should become familiar with the act. Companies should monitor the language of the act as it proceeds through the final steps needed for implementation, especially to see whether the ban on using AI tools for social scoring will extend to private entities.

In addition, because the act places considerable emphasis on transparency, organizations using AI tools should begin preparing to label AI-generated content. Organizations should also begin examining whether any of their planned uses for AI fall within the act's high-risk category.

Importantly, because the act's regulatory framework is based on what the AI system is intended to do, organizations should keep in mind that their AI system might not initially be considered high risk but could become high risk if their plans for the AI system change.

As part of the act, all member nations are required to implement a regulatory sandbox that provides a space for organizations to test AI systems in a controlled environment under the guidance of EU authorities. For this reason, organizations intending to do business in the EU going forward should continually monitor and test how they use AI and whether those uses trigger certain obligations under the act.

Next Steps

Spain, which took over the presidency of the EU Council of Ministers on July 1, has indicated that final passage of the act is one of its top priorities.[4] However, passage will require negotiations between the EU Parliament, Council and Commission.

These negotiations could result in further changes to the definition of AI and what is included under the unacceptable and high-risk categories. If negotiations proceed smoothly, then the act's regulations could go into effect as early as the second half of 2024.[5]

Conclusion

While it is too early to say for sure, the act's risk-based regulatory framework is a promising development in balancing the risk of AI with further innovation in that space.

The act forecloses the riskiest outcomes for AI by banning them while still allowing for continued growth and change in other areas as long as appropriate checks are in place.

Through the act, the EU has taken steps to have Europe set the standard for the regulation of AI going forward.

Matthew Justus is assistant vice president, senior legal counsel at AT&T.

Wade Barron is an associate at Kilpatrick Townsend & Stockton LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] European Parliament, MEPS ready to negotiate first-ever rules for safe and transparent AI, (June 14, 2023), <https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai>.

[2] Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM (2023) 206 (April 21, 2021), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206>.

[3] European Parliament, Amendments Adopted by the European Parliament on 14 June 2023 on the Proposal for a Regulation of the European Parliament and of the Council on Laying Down Harmonised Rules on Artificial Intelligence, (June 14, 2023), https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html.

[4] Politico, Chaining the chatbots: Spain closes in on AI Act, (June 22, 2023), <https://www.politico.eu/article/spain-artificial-intelligence-ai-act-technology/>.

[5] European Commission, Regulatory Framework Proposal on Artificial Intelligence, (June 20, 2023), <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.