Policy Analysis Paper 1 - EU Artificial Intelligence Act (2024) with a Cybersecurity Focus

India Henry

CYSE 425W: Cyber Strategy and Policy

Hamza Demirel

February 8, 2026

The European Artificial Intelligence (AI) Act was implemented in 2024, building off of past resolutions and regulations created about robotics and artificial intelligence (Sousa Silva, 2025, 3-4). Regulations regarding AI had been in the works since 2017 and built on over time to recognize both the "dangers and the opportunities" robotics and artificial intelligence can create for individuals and industries (Sousa Silva, 2025, 3-4). Although, the first regulatory act that actively addressed the future role of artificial intelligence didn't come until the AI Act's proposal in 2021 and its implementation in 2024. The AI Act was created with the goal of implementing AI without infringing on people's fundamental rights, which ranges from work and employment to environmental protections (Kusche, 2024, 4; Sousa Silva, 2025, 3). The AI Act seeks to regulate AI by defining its key parts, where AI is defined as "a machine based system with varying levels of autonomy" and the ability to make inferences given the data that it is previously trained on; although, when the first draft of the AI Act was created in 2021, generative AI like ChatGPT had not yet been released, so the adopted version had to create regulations that also included generative AI (Sousa Silva, 2025, 7-8; Kusche, 2024, 4).

The AI Act created a list of prohibited practices, with few exceptions, in order to safeguard people's fundamental rights; those practices include: "manipulation and exploitation of vulnerabilities, general social scoring, predictive policing, creation of facial recognition databases, emotion recognition systems in workplace or education, biometric classification of protected categories, and special cases of real-time biometric identification" (Sousa Silva, 2025, 14). These factors were prohibited based on the risk classification system that considers both the intended and unintended uses of an AI system; the list of prohibited practices are considered systems of intolerable risk, versus systems of high risk which aren't prohibited, but are still heavily regulated (Sousa Silva, 2025, 5). Systems of high risk can be used can be used in the

EU's jurisdiction, however, these systems have to be transparent about AI being used; for example, "chatbots and conversational systems" have to be designed in a way where people know they aren't talking to another person or systems that create audio or images need a watermark showing it is made by generative AI (Sousa Silva, 2025, 20).

I chose the European Artificial Intelligence Act because it may set the tone for later AI legislation in countries or other global organizations; furthermore, AI will continue to have broader cybersecurity implications as it continues to be implemented into new technologies, applications, and systems. However, like any legislation on technology, the AI Act has created some interpretation issues and faces becoming outdated in a matter of years. The AI Act is one of the first attempts to regulate AI, the risk-based approach has created issues for individuals, private industries, and countries developing AI (Kusche, 2024, 4). Predictive AI is trained using databases and algorithms that can be tainted by biases; these biases can harm individuals as predictive AI outputs are skewed and assumes past injustices are relevant in future contexts (Kusche, 2024, 4). A notably less serious repercussion is that only those who live within the EU's jurisdiction are subjected to the regulations in the AI Act; while the regulations are made for the protection of people within the EU's jurisdiction, countries outside of the EU are able to make quicker advancements in AI than countries within the EU. While this may entice companies or countries working to advance AI to work within the EU's parameters, this could also mean that countries within the EU are simply left behind in technological developments as the rest of the world progresses. From a cybersecurity standpoint, article 15 of the AI states that "high-risk systems must achieve an 'appropriate level of accuracy, robustness and cybersecurity' and must function consistently in this respect throughout their lifecycle (Nolte et al., 2025, 285). While this seems like a valid request, Article 15 does reveal inconsistency in terminology

between the law and cybersecurity experts; this in turn also creates an issue in how cybersecurity risks in the AI systems are handled (Nolte et al., 2025, 288-290).

References

Kusche, I. (2024, May 11). Possible Harms of artificial intelligence and the EU AI act: fundamental rights and risk. *Journal of Risk Research*, 1-14. https://doi.org/10.1080/13669877.2024.2350720

Nolte, H., Rateike, M., & Finck, M. (2025, June 23). Robustness and Cybersecurity in the EU Artificial Intelligence Act. *Association for Computing Machinery (ACM)*, 283-295. https://doi.org/10.1145/3715275.3732020

Sousa Silva, N. (2025, March 1). The artificial intelligence act: critical overview. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, *16*(1), 2-23. https://arxiv.org/abs/2409.00264