The Dilemma of Artificial Intelligence in the European Union

Anastasia Glover
The America-Eurasia Center
www.eurasiacenter.org

The America-Eurasia Business Coalition
www.usebc.org
The Dilemma of Artificial Intelligence in the European Union

On Wednesday, June 14, 2023, members of the European Parliament adopted an official position concerning the highly anticipated Artificial Intelligence (AI) Act. This crucial development may become the first piece of international legislation that deals with regulating artificial intelligence, as the voting occurred with an overwhelming majority of 499 votes in favor, 28 votes in opposition, and 93 abstentions.¹ The European Union is now shifting its focus towards engaging in discussions centered around the official draft of the AI Act, aiming to reach a consensus among member states and enact it into EU law by the end of the year. Parliament’s ultimate objective is for

the legislation to effectively address the ethical, social, economic, and legal implications of AI and protect the interests of European citizens while simultaneously promoting innovation.²

The adoption of a negotiating position by the European Parliament serves as a crucial step towards establishing a comprehensive and future conscious framework for governing AI technologies. As discussions progress throughout the year, member states plan to work together to finalize details of the AI Act, balancing the need for innovation with responsible and accountable uses of AI systems.

The Artificial Intelligence (AI) Act

In respect to artificial intelligence, the European Parliament’s primary concern lies within the ethical usage of AI systems. Particularly, in the areas of biometric surveillance, emotion recognition, predictive policing, and the development of open-source AI systems such as ChatGPT. The AI Act establishes a ‘risk-based approach,’ outlining regulatory rules and practices that align

with EU rights and values, which will be applied to all AI technology developed and used throughout Europe. Three levels of risk have been outlined: limited risk, high risk, and unacceptable risk.

To ensure users can make informed choices, limited risk AI systems, or open-source generative AI systems like ChatGPT, will be required to comply with minimal transparency standards. These requirements will enable individuals to access essential information while empowering them to make educated decisions about their engagement with such systems. Following their interaction with these applications, users can then determine whether they wish to continue using them. The transparency requirement is crucial for users to be aware of when they are interacting with AI, particularly in the case of AI systems involved in generating or altering audio, image, or video content, including deepfakes.

AI systems that could jeopardize people’s health, physical safety, fundamental rights, or the environment will be classified as high-risk. This classification encompasses products falling under the purview of the EU’s product safety legislation, including cars, toys, and medical devices. Additionally, many types of AI system usage will be subject to varying degrees of the high-risk classification and will be required to register in an EU database. This includes any AI system utilized in critical infrastructure, educational institutions, employment, private and public services, law enforcement, migration, border control management, and legal interpretations and applications of the law. AI systems on social media platforms used to influence political campaigns or voting will also fall under high-risk classification.

Unacceptable risk AI systems – those that pose a threat to individuals and will thus be prohibited – include cognitive behavioral manipulation, like encouraging dangerous behavior in children, and social scoring, classifying people based on socio-economic status and personal characteristics.³

Biometric identification and categorization systems will be subject to varying degrees of classifying scrutiny. Certain forms of biometric identification, such as those used in predictive policing systems, remotely accessed systems in publicly accessible spaces, and those that use

---

profiling or sensitive characteristics (e.g., religion, gender, ethnicity, political orientation, citizenship status) will be prohibited and considered unacceptable risk. An exception, however, will be made for remote biometric identification systems, on condition of judicial authorization, to be used by law enforcement to persecute serious crimes.  

Dilemma in Regulating AI

With the initial framework for regulating AI systems, considerable debate remains within the EU regarding risk management, data governance, and the intricate technical aspects within the rapidly evolving field of AI technology. Discussions are ongoing about the potential success of the AI Act and future legislation in striking a balance between addressing potential risks and not impeding the value of technological innovation.

On one hand, AI systems have the potential to revolutionize various sectors, improve efficiency, and enhance the quality of life for individuals. It can automate tasks, facilitate decision-

---

making, and drive innovation in areas such as healthcare, transportation, and education. One of the key advantages of AI systems is their ability to process vast amounts of data and extract valuable insights. This has the potential to lead to significant advancements in fields like medical research, where AI can assist in diagnosing illnesses, drug discovery, and formulating personalized treatments. Similarly, in respect to transportation, AI can enable autonomous vehicles, reducing accidents and traffic congestion. In customer service, AI-powered chatbots can enhance response times and provide around the clock support.\(^5\)

Alongside the benefits, however, there are legitimate concerns about the scope of innovation of AI systems. One of these concerns includes the potential for biases and discrimination. AI systems learn from large datasets, which may contain biases that are either embedded in the data itself or introduced through the algorithms used. This can lead to discriminatory outcomes in areas like hiring practices, loan approvals, or criminal justice, perpetuating existing social inequalities. Additionally, privacy is another significant concern. AI systems often rely on collecting and analyzing personal data, raising questions about data protection and individuals' rights to privacy. The risk of data breaches and unauthorized access to sensitive information will be more pronounced as AI systems become more prevalent in various aspects of society.\(^6\) As AI systems become more sophisticated, questions arise about their accountability, transparency, and decision-making processes, and ethical considerations come into play. For example, the use of autonomous AI systems in critical areas like healthcare or automatic weapons raises ethical dilemmas and calls for responsible governance, which the AI Act hopes to achieve.

Ultimately, finding the right balance in regulating AI systems is crucial. Overregulation could stifle innovation and hinder the potential benefits of AI, while under regulation may lead to unchecked risks and potential harm to individuals. Striking a balance should require a multidisciplinary approach involving not just policymakers, but also industry leaders, researchers,


and ethicists to develop the frameworks that promote responsible development, deployment, and use of AI systems.

References


