NAVIGATING THE EU AI ACT: EXPLORING CHALLENGES AMIDST THE EVOLVING GLOBAL REGULATORY LANDSCAPE

GLORIA SHKURTI ÖZDEMİR

SETA | PERSPECTIVE DECEMBER 2023 · NUMBER 72

- What is the EU AI Act?
- What are the main challenges it may face?
- What is the impact of this regulation within the global regulatory landscape?

INTRODUCTION

Artificial Intelligence (AI) is not new. Indeed, it has quietly woven itself into the fabric of our daily lives over the years. Often, we engage with AI seamlessly without even realizing it. We rely on AI in our smartphones for music, movie, and book recommendations, have casual conversations with virtual assistants like Siri or Alexa, scroll through our social media feeds tailored by AI algorithms, navigate our routes using AI-powered GPS systems, and benefit from the subtle assistance of autocorrect on our devices, which helps us type more efficiently and corrects our spelling errors. We become so accustomed to these AI applications, often using them without even recognizing the underlying AI algorithms and taking them for granted.

However, today, AI has become a central topic of discussion like never before. Suddenly, everyone is engaged in conversations about the potential applications of AI and its far-reaching implications, both positive and negative, in our daily lives. While landmark events such as IBM's Deep Blue defeating world chess champion Garry Kasparov in 1997 and Google's AlphaGo defeating the world Go champion Lee Sedol in 2016 were significant milestones in AI development, they largely remained within the domain of tech experts.

In stark contrast, the introduction of Chat GPT-3 in November 2022 by OpenAI undeniably marked a turning point in the trajectory of AI. It widened the aperture of AI's reach, ushering in a wave of AI use and increased the awareness among the general public like never before.

Simply put, what Chat GPT-3 brought about was a transformative moment when AI ceased to be a tool exclusively in the hands of experts and engineers. Instead, it became accessible to the everyday person, even those with no technical knowledge. In a manner reminiscent of how Google Search revolutionized internet search in the early 2000s, Chat GPT-3 has ushered in a revolution in AI by democratizing access and making it open source for all.

This development ignited a fierce competition among tech companies, leading to a rush to launch similar chatbots, exemplified by the quick announcement of Google's Bard. The advent of these large language models, made openly accessible to all, fueled discussions about the implications of AI, triggering

GLORIA SHKURTI ÖZDEMİR

Gloria Shkurti Özdemir completed her BA in Political Science and International Relations in Al- bania. She finished her master's studies at Sakarya University with her thesis entitled "A Lethal Weapon that Became the Cure-all for Terrorism: Discursive Construction of the U.S. Dronified Warfare." She is a PhD can- didate at Ankara Yıldırım Beyazıt University and her thesis focuses on the application of artificial intelligence in the military by taking as a case the U.S.-China rivalry. Her main research interests include U.S. foreign policy, drone warfare, and artificial intelligence. Currently, she is a researcher in the Foreign Policy Directorate at SETA Foundation. She is also working as the Assistant Editor of Insight Turkey, a journal published by SETA Foundation.

debates over the need for regulations -whether on a global or national scale.

In this rapidly evolving technological landscape, the European Union (EU) AI Act has emerged as a notable regulatory framework. What sets it apart from other regulations is its comprehensiveness. While not the first AI regulation, it is arguably the most all-encompassing, positioning it as a potential global standard for AI governance. This journey began in 2021, and the EU AI Act has undergone significant revisions to adapt to evolving technology, especially with the launch of Chat GPT-3.

Now, as of December 8, 2023, the European Commission, Council, and Parliament have come to a consensus in a trilogue, bringing the EU AI Act closer to the conclusion of its legislative process. This perspective will offer a concise introduction to the EU AI Act, discuss potential ramifications, and, crucially, examine how this development will resonate in the international arena. Here, a dual rivalry unfolds—one characterized by the ongoing race in AI algorithm advancements and applications, and the other marked by the competition to establish AI standards. It's essential to recognize that both of these competitions carry profound implications for the distribution of power on the global stage. The introduction of the EU AI Act is poised to exert influence on both fronts, adding a significant dimension to the ongoing dynamics.

WHAT IS THE EU AI ACT?

The European Union has earned widespread recognition as a frontrunner in data regulation and governance. A prime illustration of this is the General Data Protection Regulation (GDPR),[1] which became enforceable in 2018 and set a significant precedent for the regulation of data not only within the EU but also as a model for other nations. The EU has also embarked on further initiatives, including the Digital Services Act,[2] which governs online platforms, and the Digital Market Act,[3] primarily focused on regulating online e-commerce. Within this framework, the EU has taken on an even more formidable challenge—regulating AI. This endeavor comes at a pivotal moment, as leaders of major tech companies themselves have been advocating for the necessity of AI regulations before it becomes an urgent concern.

The EU AI Act was initially introduced by the European Commission on April 21, 2021, with the primary objective of overseeing the deployment of AI in Europe. Originally crafted to address particular, high-risk AI applications, such as its usage in critical sectors like healthcare and finance—examples being medical equipment and loan approval processes or hiring decisions—its scope expanded in response to shifting perceptions.[4] As mentioned earlier, the introduction of Chat GPT-3 brought about a reevaluation of how AI was accessed and perceived. Consequently, the European Parliament introduced additional regulations to cover widely utilized AI systems with broad, general applications that extended beyond the initial target areas.

After several discussions, on December 8 an agreement was reached among the three main bodies of EU yet it is important to state that the final text of the regulation has not been available yet and it may takes several weeks upon its finalization. Yet, general specifics about it have become public.

First and foremost, the EU AI Act has decided upon a definition on AI, which indeed is quite important as not only have many states failed to do so but most importantly an exact definition of AI makes it easier the application of this regulation. Specifically, the EU AI Act is aligned with that of OECD which states that:

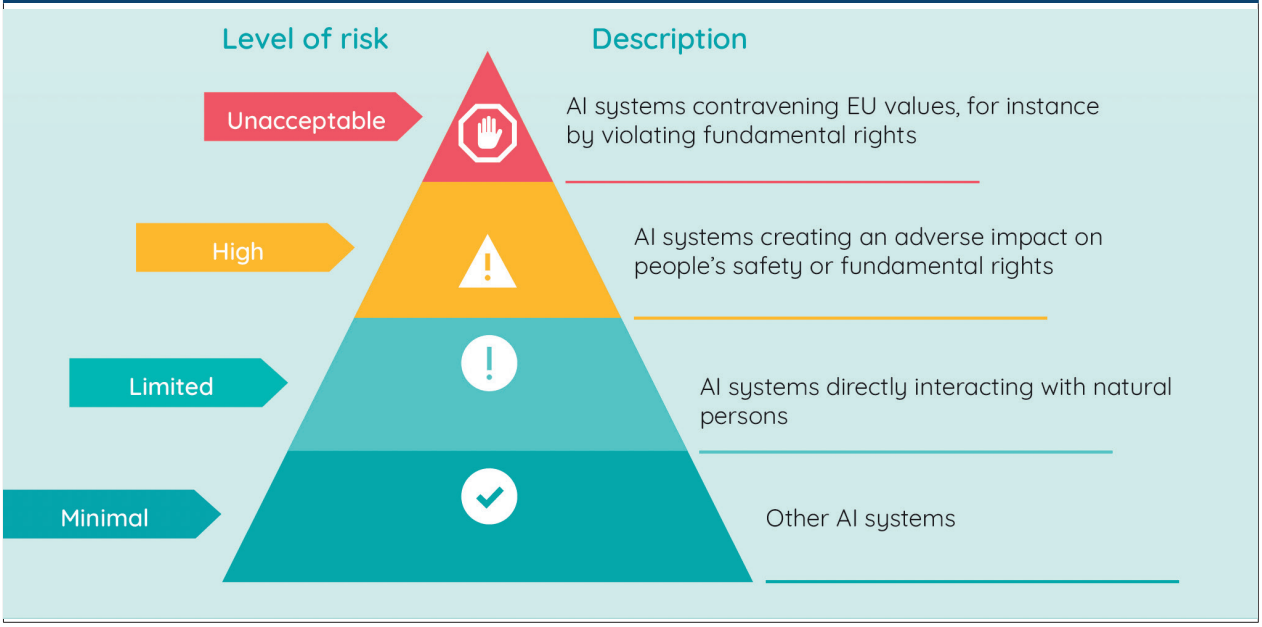
1 Ben Wolford, "What is GDPR, the EU's New Data Protection Law?", GDPR EU, https://gdpr.eu/what-is-gdpr/, (Accessed: December 13, 2023).

2 "Digital Services Act", EUR-Lex, (October 27, 2022), https://eur-lex.europa.eu/eli/reg/2022/2065/oj, (Accessed: December 13, 2023).

3 "Digital Markets Act", EUR-Lex, (October 12, 2022), https://eur-lex.europa.eu/eli/reg/2022/1925/oj, (Accessed: December 13, 2023).

4 Richard Waters, Madhumita Murgia and Javier Espinoza, "OpenAI Warns Over Split With Europe as Regulation Advances", Financial Times, (May 25,2023) , https://www.ft.com/content/5814b408-8111-49a9-8885-8a8434022352, (Accessed: December 12, 2023).

FIGURE 1: CATEGORIZATION OF AI LEVELS OF RISK



Source: Elisar Bashir, New Cullen cheat sheet on the draft EU Artificial Intelligence Act, (July 12, 2021), Cullen International. https://www.cullen-international.com/news/2021/07/New-Cullen-cheat-sheet-on-the-draft-EU-Artificial-Intelligence-Act.html?gclid=Cj0KCQiA7OqrBhD9ARIsAK3UXh3-YtmR_X6D3_6VZqKArHVDg5xk9kfcjJh9_3kps-GjVf6yGig34xsaAtf9EALw_wcB

> An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.[5]

Secondly, it's crucial to recognize that the EU AI Act embodies a comprehensive and risk-focused framework, placing human rights at its core. From this vantage point, the regulation prohibits various AI applications, including: (i) biometric classification systems processing sensitive traits such as political, religious, or philosophical beliefs, sexual orientation, or racial attributes; (ii) indiscriminate harvesting of facial images from the internet or CCTV for facial recognition databases; (iii) the use of emotion detection technologies in workplaces and educational settings; (iv) social credit systems that assess individuals based on social conduct or personal traits; (v) AI tools designed to alter human behavior, undermining free will; (vi) AI solutions targeting the vulnerabilities of specific groups, including those defined by age, disability, or socio-economic status.[6]

Furthermore, the EU AI Act, differentiates between uses of AI that involve four levels of risk. To put it simply, the higher the risk, the tighter the restrictions (Figure 1).

5 Stuart Russell, Karine Perset, Marko Grobelnik, "Updates to the OECD's Definition of an AI System Explained", OECD, (November 29, 2023), https://oecd.ai/en/wonk/ai-system-definition-update, (Accessed: December 14, 2023).

6 It should also be noted that under certain conditions, the use of Remote Biometric Identification (RBI) systems, commonly known as automated facial recognition, in public spaces is permitted as an exception. This applies when there is prior judicial authorization or in response to specific criminal activities. These exceptions include targeted searches for victims of crimes such as abduction, human trafficking, or sexual exploitation, addressing immediate terrorist threats, and locating or identifying individuals suspected of committing crimes specified in the regulation. The listed crimes include terrorism, human trafficking, sexual exploitation, murder, kidnapping, rape, armed robbery, involvement in a criminal organization, and environmental crime. For more see, "Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI", Press Releases, European Parliament, (December 9,2023), https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai, (Accessed: December 13, 2023).

1. **Minimal or No Risk**: This category includes AI applications like video games or spam filters, which are freely used. The majority of AI systems in the EU currently fall under this category. After an AI system is marketed, authorities monitor the market, users ensure human oversight, and providers maintain post-market surveillance. Both providers and users are required to report serious incidents and malfunctions.
2. **Limited Risk**: AI systems with limited risk have specific transparency obligations. For instance, users interacting with chatbots should be aware they are communicating with a machine, allowing them to make informed decisions about continuing the interaction.
3. **High Risk**: All remote biometric identification systems are considered high risk and face strict requirements. As stated above, their use in public spaces for law enforcement is generally prohibited, with narrow exceptions. High-risk AI systems also include those used in critical infrastructures, education, product safety, employment, essential services, law enforcement, immigration, and justice. These systems must undergo strict compliance assessments, including risk mitigation, high-quality datasets to minimize bias, activity logging, comprehensive documentation, clear user information, human oversight, and robust security measures.
4. **Unacceptable Risk**: AI systems posing clear threats to safety, livelihoods, and rights are banned. This includes AI used for social scoring by governments and voice-assisted toys promoting dangerous behavior (such as in the example of children).[7]

Another important point in the regulation is related to General Purpose AI (GPAI). As state above, the emergence of Chat GPT-3 had a great impact on the drafting of this regulation. For this reason, a section focusing on GPAI is included in the EU AI Act. Specifically, GPAI models are trained on a large amount of data and are able to perform a wide range of distinct tasks and can be integrated into a variety of downstream AI. Generative AI – that is a model used by Chat GPT- falls within this category.

Within this perspective, the EU AI Act introduces two obligation levels for general purpose AI, overseen by a new AI Office that will be created within the Commission:

1. **Level One - General Purpose AI:** Obligations for all providers include maintaining technical documentation, providing detailed model information for downstream compliance, adhering to EU copyright rules (especially concerning data opt-outs for text and data mining), and publishing statements about training data. Open-source general purpose AI is exempt from documentation and downstream information requirements but must comply with copyright policies and training data disclosure.
2. **Level Two - High Impact and Systemic Risk AI:** This tier applies to general purpose AI models that pose systemic risks, characterized by extensive training data and computational complexity. A model is considered a systemic risk if its training involves more than 10^25 floating point operations. Providers of such AI models must undertake additional obligations like model evaluation, adversarial testing, monitoring and reporting serious incidents, ensuring cybersecurity, and reporting on energy consumption. The AI Office can also designate AI systems as having systemic risk based on various factors.[8]

At this point, what is mainly discussed is that under the new regulation, companies like OpenAI and Google, which develop GPAI models, are partially ac-

7 "Regulatory Framework Proposal on Artificial Intelligence", European Commission, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai, (Accessed: December 14, 2023).

8 Osborne Clarke, "The EU's AI Act: What Do We Know So Far About the Agreed Text?", Lexology, (December 12, 2023), https://www.lexology.com/library/detail.aspx?g=813bdbdc-c265-4f45-b512-c4622fffec9c, (Accessed: December 13, 2023); "Artificial Intelligence – Questions and Answers", Questions and Answers, European Commission, (December 12, 2023), https://ec.europa.eu/commission/presscorner/detail/en/QA-NDA_21_1683

countable for the usage of their AI systems, regardless of their control over specific applications where the technology is implemented. Additionally, as stated tech companies are required to disclose summaries of copyrighted data used in training their AI models which in result can enable artists and other content creators to potentially seek compensation for the use of their material.[9]

Finally, it's worth noting that this legislation will not encroach upon the deployment of AI for national security purposes, making it clear that the regulations won't be applied to systems exclusively designated for defense and military applications.[10] However, a crucial aspect to highlight is that AI systems possess a unique characteristic of dual-use capability, meaning they can serve both civilian and military functions, as exemplified by technologies like facial recognition. Given that the legislation covers dual-use technologies, it is evident that it will exert a direct influence on the development and application of AI in the realm of defense within the EU.

Regarding the timing, the political agreement on the AI Act awaits formal approval by the European Parliament and the Council. Once published in the Official Journal, it will come into force 20 days later, with general applicability two years after. Specific provisions vary: prohibitions will be effective in 6 months, while General Purpose AI rules will apply after 12 months. During the transition, the Commission will launch an AI Pact, encouraging AI developers globally to voluntarily adhere to key AI Act obligations before the legal deadlines.[11]

CHALLENGES OF EU AI ACT

Regulating technology, particularly AI, is a delicate balancing act. On one side, there's the need to protect the rights of civilians and tech users; on the other, it's vital to foster innovation and investment. This equilibrium is particularly challenging in the AI sector due to its broad range of applications. The EU's regulations have drawn significant criticism, mainly from major American tech firms impacted by these rules. A prime illustration is OpenAI's chief, Sam Altman, who expressed their intent to adhere to these regulations. However, he also stated that if compliance proves unfeasible, OpenAI might cease its operations in the EU. Similarly, Google's launch of its updated AI chatbot Bard, which was conspicuously not made available in the EU, highlights the regional variations in tech deployment, underscoring the complex interplay between global tech developments and regional regulatory environments.

The EU AI Act faces a another significant challenge due to the nascent state of AI. We've only seen a fraction of AI's potential applications and capabilities. This was evident when the introduction of Chat GPT-3, during the regulation's drafting phase, shifted the context of the discussions, necessitating further revisions.

Indeed, the Act is often praised for being the first extensive AI law, setting a precedent in comprehensive AI regulation. In other words, the EU's approach is a horizontal regulatory framework, encompassing a wide range of technological applications under a single legislative framework. This contrasts with China's vertical regulatory strategy, where regulations are tailored to specific AI applications or groups. This method allows for more agile adaptation to new technological advancements, ensuring regulations remain current.

In simpler terms, our world today is vastly different from just a few months ago, primarily due to rapid technological advancements. While the current EU AI Act seems comprehensive now, the fast-paced emergence of new technologies or novel uses of existing ones may soon render it outdated. This will necessitate either updates to the existing regulation or the creation of new regulatory frameworks to keep pace with these advancements.

9 https://www.ft.com/content/5814b408-8111-49a9-8885-8a8434022352, (Accessed: December 23, 2023).

10 Osborne Clarke, "The EU's AI Act: What Do We Know So Far About the Agreed Text?".

11 "Commission Welcomes Political Agreement on Artificial Intelligence Act", Press Release, European Commission, (December 9, 2023), https://ec.europa.eu/commission/presscorner/detail/%20en/ip_23_6473, (Accessed: December 13, 2023).

A GLOBAL COMPETITION IN TERMS OF AI REGULATIONS

The realm of AI regulation is witnessing a global competition, with nations leveraging AI to enhance their national interests and international standing. This has led to diverse regulatory approaches. The EU is a leader in establishing regulations, but other major players like China, the US, and the UK are adopting different strategies.

China's vertical regulatory framework aligns company operations with the interests of the Chinese leadership, offering more operational freedom compared to the EU's approach. In contrast, the US has historically adopted a laissez-faire stance, allowing companies significant self-regulation. This approach, centered on economic profit maximization, shares similarities with China's but differs markedly from the EU's.

However, this hands-off approach in the US is evolving, with major tech companies now advocating for regulations, including a federal AI oversight agency. Despite this shift, they resist regulations akin to the EU AI Act.

The global AI landscape shows that leading AI nations also set regulatory standards. This is due to the 'first mover advantage' in regulation, where the initial standard-setter influences subsequent global discussions and policies, leaving others to adapt.

Currently, two dominant regulatory models have emerged: the EU's and China's. The critical question is where the US will position itself. Aligning with the EU could impact its competitiveness in the AI race against China. Conversely, creating a third model poses challenges, as US companies might resist adhering to vastly different standards across markets. Therefore, some convergence between the US and EU approaches seems necessary.

In conclusion, it's premature to judge the effectiveness of the EU AI Act. The undisclosed specifics of the regulation, combined with the rapid evolution of technology, make it hard to foresee the future landscape of AI technologies and their governance. Nevertheless, the diverging approaches of the US and EU highlight a fundamental split in the broader AI competition.

SETA
SİYASET, EKONOMİ VE TOPLUM ARAŞTIRMALARI VAKFI
FOUNDATION FOR POLITICAL, ECONOMIC AND SOCIAL RESEARCH
مركز الدراسات السياسية والاقتصادية والاجتماعية

www.setav.org | info@setav.org | @setavakfi

ANKARA • İSTANBUL • WASHINGTON D.C. • BERLIN • BRUSSELS