Implementing the EU AI Act: How Soon Is Now?

by Anastas Punev

Summary

This paper reflects on the future implementation of the EU Artificial Intelligence (AI) Act and mainly focuses on its possible drawbacks, which could undermine the visionary idea of instituting the first comprehensive regulation on AI. Drawing on comparisons between the AI Act and similar legislative attempts at regulating global phenomena, recommendations are made as to how to adapt the AI Act to foster EU leadership.

Keywords AI Act – AI liability – GPAI

The future of the AI Act: GDPR déjà vu?

The Artificial Intelligence (AI) Act was a result of 3 years of discussion and exactly 3,312 proposed amendments. In the proud words of Thierry Breton, the former European Commissioner for Internal Market, the political deal that produced the Act made the EU 'the first continent to set clear rules for the use of AI'.[1] Some of the key messages used to portray the novelty of the AI Act, however, are instantly reminiscent of a similar 'global first' model legislation—the General Data Protection Regulation (GDPR). Among the main features of the AI Act are the 'robust enforcement framework', the tough penalties for non-compliant businesses and the establishment of a new institution: the EU AI Office at the European Commission. All these measures are instantly comparable to the GDPR, which was also aimed at balancing fundamental rights and innovation, thus fostering the EU's global role. Unfortunately, the GDPR's goals have been undermined to a large extent by poor enforcement. Therefore, comparing the two seems appropriate, as the enactment of the AI Act, in its definitional, substantive and institutional aspects, has already been labelled as 'GDPR mimesis'.[2]

Extensive research shows that millions of European small and medium-sized enterprises (SMEs) have not complied with the excessive burdens provided by the GDPR, and this has thrown into question the purpose and future impact of the regulation.[3] Additionally, there was a considerable lack of consistency among the member states in implementing the GDPR, which only exacerbated the bureaucracy and created the impression that the regulation was forcing numerous extraneous duties on companies. Such risks are, unfortunately, also attributable to the AI Act. Not only does it lack a preliminary analysis of its future implementation, but the whole design of the Act appears comparable to the GDPR. That is, it treats technology as something that merely needs better organisation: AI systems must be labelled and then monitored to reduce their negative effects.[4] This is confirmed by the lack of calculation of the financial burden companies face to comply with the legislation. This issue has already been raised by trade associations such as Digital Europe, which referred to the AI Act as 'uncharted territory'.[5]

1 T. Breton, 'The European AI Act Is Here!', *LinkedIn*, 9 December 2023.
2 V. Papakonstantinou and P. de Hert, 'Post GDPR EU Laws and Their GDPR Mimesis. DGA, DSA, DMA and the EU Regulation of AI', *European Law Blog*, 1 April 2024.
3 GDPR.EU, *2019 GDPR Small Business Survey* (May 2019).
4 V. Papakonstantinou, 'The AI Act and a (Sorely Missing!) Right to AI Individualization; Why Are We Building Skynet?', *European Law Blog*, 16 July 2024.
5 G. Kaur, 'Concerns Remain Even as the EU Reaches a Landmark Deal to Govern AI', *CIO*, 11 December 2023.

The future simultaneous application of the AI Act and the GDPR has also caused controversy even before the entry into force of the new regulation. The requirements of both acts can be interpreted in a mutually contradictory manner because their goals cannot be entirely reconciled. While the AI Act presupposes that AI systems need large amounts of data, it also allows limitless data processing, which can contravene the explicit consent required under Article 9 of the GDPR. And the Act does not contain any clear instructions on how personal data from publicly available sources will be collected for the mandatory self-training, validation and testing of AI systems, which are the main ways in which these systems can be improved.[6]

Furthermore, Article 6 of the AI Act expressly grants the Commission the power to classify AI systems as high-risk by providing a 'comprehensive list of practical examples'. Such an extensive power, without any further narrowing of its scope, could hinder the enforcement of the Act, considering the Commission's lack of sufficient technical expertise. Here the GDPR is once again a useful reference as its implementation has already shown that safeguarding the rationale of the law without straying into over-regulation is better achieved by activists with sector expertise. Yet, the voice of individual users is not heard in the Act. The legislation could provide, among other things, an ombudsperson or a similar body entrusted with directly representing users in situations involving enforcement.[7] No less important is that the AI office's powers could lead to a duplication of roles and, as a result, to inefficiency and a lack of clarity regarding responsibilities. The recent controversy related to the investigation into how X handled the Israel–Hamas conflict revealed how significant misapprehension arose out of the confusion over which body had authority for what: the Commission team overseeing the Digital Services Act or the separate unit in charge of a voluntary EU code to guard against disinformation.[8]

Balance of responsibilities, foundation models and fundamental rights

Another widely disputed issue surrounding the entry into force of the AI Act is that of responsibility, since the Act is intended as product safety legislation whose main aim is to reduce the risk of the potentially dangerous use of AI. In this regard the AI Act focuses mainly on the prohibitions and limitations to be applied to AI. It proceeds by adopting a detailed risk-based approach, placing AI systems into four risk categories depending on their use: unacceptable-risk, high-risk, limited-risk, and minimal- or no-risk. Conversely, there are specific requirements for foundation AI models[9] capable of performing a wide range of distinct tasks, irrespective of their risk categorisation.

According to the European Council's official statement, mirrored in the AI Act, the rules on high-risk systems apply to general purpose AI (GPAI) models that can be used in contexts involving significant risk unless such uses are explicitly excluded. This is further reflected in the vague language of the law, according to which a GPAI model can be classified as containing 'systemic risk' on the basis of criteria such as 'high-impact capabilities'. Therein lies the main challenge in implementing the AI Act without hindering innovation. One and the same AI model can simultaneously enable care robots and lethal weapons. Thus, many models can be placed in the high-risk category even if only one of their general uses turns out to involve a high degree of risk.[10] This seems even more dangerous for open-source foundation models as the description of their requirements is very generic compared to the intricate descriptions of the (various) risks set out in the AI Act. This could easily lead to ambiguous interpretations. For this reason, it has rightly been proposed that mitigation measures should focus solely on the potential future uses of the technologies so that continuous adaptation is allowed.[11]

---

6 S. Wadhwani, 'Last Mile Trouble: What Needs to Be Sorted in EU AI Act Before Next Week's Trilogue Talks', *Spiceworks*, 29 November 2023.
7 L. Edwards, *Regulating AI in Europe: Four Problems and Four Solutions*, Ada Lovelace Institute (March 2022), 11.
8 M. Scott, 'The EU's Online Content Rulebook Isn't Ready for Primetime', *Politico*, 14 February 2024.
9 A foundation model (also known as general-purpose AI or GPAI) is an AI model designed to produce a wide and general variety of outputs. As such, it differs from narrow AI systems which focus on a specific task.
10 C. Djeffal, 'The EU AI Act at a Crossroads: Generative AI as a Challenge for Regulation', *European Law Blog*, 24 July 2023.
11 Ibid.

Concerning innovation and liability, the one-size-fits-all approach of the AI Act is particularly impractical for providers of mostly decentralised open-source AI systems. This is especially true given the excessive regulatory burden, which could be difficult to comply with. For example, the requirement to maintain 10 years of documentation is practically impossible to implement as open-source systems by definition allow other agents to modify the software and thus break the chain of liability. A more reasonable approach would be to regulate specific high-risk AI applications and not the underlying GPAI models. This could balance the AI Act's goals with the threats and would not discourage new possible fields for the application of AI, especially for SMEs, which should not be faced with excessive costs and obstacles.[12] Furthermore, while the levels of risk are defined in the Act, the allocation of responsibility among the different providers throughout the various stages involved in the use of AI remains vague and thus unpredictable for businesses from the outset. In fact, 'AI' is even disputed as a meaningful term because it is neither a product in the traditional sense of the word (as expressly recognised by the AI Act) nor a one-off service but a dynamic system that moves through a series of stages which make up the AI life cycle.[13]

Even more importantly, there are large groups of people that are not sufficiently addressed in the Act, such as those mostly impacted by the AI models: consumers, data subjects and end users. They have been left in the dark as their role as rights-holders is not expressly guaranteed and protected. For example, users buying a system off the shelf will most certainly not regard themselves as responsible for the 'substantial modification' necessary for them to become regarded legally as providers, and so they could fall under the scope of the Act even without realising it.[14] Precisely for this reason, the product safety framework of the Act is not suitable for the possible violations of fundamental rights in an AI context. In product safety legislation any adverse risk can supposedly be calculated by measuring the likelihood of an event and its effects, but this is largely impossible when it comes to AI. A braver step in guaranteeing fundamental rights would have been, for example, to declare that every human being has property rights to their genetic data and personal identifiable information.[15]

Even if such ideas are not implemented in the future, some of the carve-outs and the broad definitions of the AI Act should at least be clarified as they constitute a clear threat to individual rights. For example, emotional recognition or biometric categorisation could still be used in law enforcement under somewhat murky circumstances.[16] Similarly, the EU AI Office will be empowered to explain fundamental categories such as transparency obligations 'when deemed necessary'—a dangerous and possibly far-reaching notion that only expands the regulatory space at the expense of individual rights.[17] Even organisations such as the Office of the United Nations High Commissioner for Human Rights have already underlined that the risk-dependent formula of the AI Act must be related to adverse impacts on human rights and not to mere technical specifications.[18]

12 A. Prabhakar, 'The EU AI Act Is a Cautionary Tale in Open-Source AI Regulation', *Center for Data Innovation*, 20 November 2023.
13 Edwards, *Regulating AI in Europe*, 6.
14 Ibid., 7.
15 Kaur, 'Concerns Remain'.
16 M. V. Bravo, 'What U.S. Regulators Can Learn From the EU AI Act', *Electronic Privacy Information Center*, 22 March 2024.
17 B. Martens, 'The European Union AI Act: Premature or Precocious Regulation?', *Bruegel*, 7 March 2024.
18 V. Türk, 'Open Letter From the United Nations High Commissioner for Human Rights to European Union Institutions on the European Union Artificial Intelligence Act', Office of the United Nations High Commissioner for Human Rights, 8 November 2023.

The political impact of the AI Act

As is evident from the above considerations, AI is another battlefield where the clash between market forces will have very clear implications for the overall exercise of power, especially in a geopolitical sense. From this perspective, the AI Act has a key role in establishing the EU's position as a pioneer in AI legislation. The Act is being adopted at a very critical point in time because China has already introduced its AI legislation, and the US is still considering its own approach. If two models have already been established, it is hard to imagine that US companies will opt for a third one that would differ considerably and increase the risk of non-compliance.[19] Thus, the EU AI Act represents one of the few opportunities for the Union to demonstrate the 'Brussels effect' and achieve a global first. Moreover, the nature of AI is decentralised and universal, so the area of impact of the AI Act is wider than the EU single market, thus leading to a possible first-mover advantage.[20] In this regard, the EU has a unique role, as the Sino-US tech rivalry is igniting, and the Union act as a bridge between the two superpowers since AI is a matter of global governance. An already established principle is that AI governance is only as good as the worst-governed country.[21]

However, the EU seems to rely on this 'universal' character of the EU AI Act too much, as if that renders the Act unavoidable for its global competitors, while stakeholders have already expressed their doubts about the Act, even before its entry into force. For instance, Sam Altman, OpenAI's CEO, admitted that if compliance proves unfeasible, OpenAI might cease its operations in the EU.[22] In light of this, the Brussels effect bears the parallel risk of a 'Brussels side effect': the shortcomings related to the EU regulatory approach might be accepted outside the EU but at the cost of their negative spread across the globe.[23] Thus, the AI Act model might be successful in imposing widely accepted standards, but the result would be a non-stringent regulation ill-suited to defend fundamental rights.

The Chinese model, on the other hand, does not aim for global supremacy but is mostly pragmatic in its aims, adhering to a 'vertical strategy' in which regulations are tailored to certain AI applications. Its main short-term advantage would be the more relaxed regulatory environment.[24] This is the opposite of the AI Act's horizontal model whereby a wide range of technological applications is encompassed under a single legislative framework. OpenAI's product ChatGPT offers a good illustration of the possible advantages of a vertical model of legislation—it has already demonstrated the promise of large language models and made many of the EU's earlier legislative efforts obsolete.[25] It would be a missed opportunity if the EU were to decide not to include more agility in its quest for future-proof regulation. This is even more concerning from a political standpoint because it is hardly imaginable that the Commission would reopen the AI Act for revision soon after its adoption. In sum, the EU should be strict only when it comes to measures that (1) offer real regulatory advantages over the Chinese model (or any other framework that may be developed in the future); and (2), if compliance with them cannot be guaranteed, at least cannot be easily circumvented.

19 G. S. Özdemir, 'Navigating the EU AI Act: Exploring Challenges Amidst the Evolving Global Regulatory Landscape', *SETA*, December 2023.
20 Edwards, Regulating AI in Europe, 2.
21 A. Zhang, 'The Promise and Perils of China's Regulation of Artificial Intelligence', *Columbia Journal of Transnational Law* (forthcoming), 36.
22 Özdemir, 'Navigating the EU AI Act'.
23 M. Almada and A. Radu, 'The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy', *German Law Journal 25/4 (2024), 647.*
24 Zhang, 'The Promise and Perils of China's Regulation', 7.
25 M. Mema, 'The EU AI Act: Two Steps Forward, One Step Back', *Global Governance Institute*, 19 March 2024.

Policy recommendations

The above considerations show that the EU AI Act should be treated cautiously at this initial stage of implementation. Although comprehensive regulation is needed, AI policy should be more concise and angled slightly differently. Whether these adjustments will happen depends largely not only on the Act's future application and interpretation by courts and the executive, but also on the interaction between it and its US and Chinese counterparts, and the upcoming supplementary acts detailing important aspects of the regulation. This is why there is still room for progress if the EU can demonstrate that the AI regulation will be adopted not against but in support of innovation.

The most important point is that the use of AI demands not only detailed regulation but also a workable solution that can be reasonably implemented. Therefore, the AI Act should address the capacity of SMEs to comply with the Act in terms of costs and organisational measures. This needs to be done before it is too late, because otherwise these companies will be forced to reckon with its far-reaching requirements. This necessitates minimal political intrusion from the EU authorities, mostly in labelling the risks posed by the various AI models, but also in avoiding making sudden and abrupt amendments to the regulatory framework. Here responsibility should be distributed between institutions at the EU and national levels after researching their potential interplay.

Considering the predictability of the AI Act, which is key to its success, the issue of liability should be treated more clearly, and the main strategy should be to shift the risk profile of an AI system away from its intended application. The distribution of liability between the service providers should be delineated so that there are no doubts about who is responsible for what during the AI life cycle. The most important reference point is that liability will be related to the use of the AI product and not to its foundation model. This implies that the focus of the AI Act will be shifted away from threatening and imposing large sanctions on companies and to consumers and their fundamental rights.

AI will in any case play an important part in the global role of the EU and its relationship with the US and China. Therefore, the AI Act is a matter not only of law but also diplomacy and leadership, which are even more important when it comes to global topics such as AI. For this reason, the enforcement of the AI Act should be supplemented by deepening EU–US cooperation and should use all the necessary instruments, including the transatlantic Trade and Technology Council and the G7 Hiroshima AI Process on priority risks.

Conclusion

The future is never certain. Nobody can be entirely prepared for the rapid technological progress of AI models and the unimaginable risks arising from their use. However, a good first step is to consider AI in its ever-changing nature: not as a danger to be reckoned with but as a necessary step in technological development. This step should be guided less by inflexible institutions than by free-market initiative and guarantees for individual rights. In any case, the EU AI Act might be one of the last chances for the Union to lead the way, and its success or failure will most certainly have a major impact on European policy.

	Programme 1	Programme 2	Programme 3
	Enforcing the EU AI Act	**Reducing unpredictability and the excessive burden for businesses**	**Ensuring Europe's leading role globally**
Project 1	Evaluate the capacity of SMEs to comply with the Act before its entry into force. Limit the political intrusion of EU authorities into approving which organisations will review and certify high-risk AI systems.	Consider exempting from certain obligations open-source models which are decentralised and can vary in their purposes. Evaluate the fines imposed by the AI Act. Focus on how adequate they are and whether they might have a stifling effect, taking into account the amount of money involved and the stringency with which they are to be imposed.	Deepen EU–US cooperation on mitigating the global risks of AI proliferation and the nefarious use of advanced biotechnologies. Make use of the transatlantic Trade and Technology Council to expand joint work on risk taxonomies, common standards and aligning key policies. Reinforce the EU's role in expanding the G7 Hiroshima AI Process on priority risks, guiding principles for AI systems and responsible AI tools.
Project 2	Analyse the interplay between the AI Act and the GDPR so that they can be applied systematically to the collection of data by AI systems.	Promote legislation which outlines the distribution of liability between different service providers. Develop a genuine assessment of risk which is grounded in clear renewable criteria that mirror technological developments. Analyse the established case law on the GDPR concerning the allocation of responsibility and adapt it to the needs of AI providers.	Promote the EU model as a 'global first' by emphasising the AI Act's advantages, without highlighting the tough penalties to businesses as the major selling point. Expand international agreements on data and digital cooperation with like-minded countries and attempt to 'export' some of the main provisions of the AI Act.
Project 3	Evaluate the scope of powers of the EU-level authority in light of the budget required and the distribution of responsibility between the EU and the national institutions.	Safeguard the fundamental rights of users by focusing on their freedoms (e.g. from property rights to genetic data) instead of treating AI only in terms of product safety. Provide inviolable individual rights and efficient procedures for the protection of consumer rights, e.g. by consolidating patterns of complaints.	Adopt a more vertical approach to AI applications and groups, especially in comparison to the pragmatic Chinese model.

Bibliography

Almada, M. and Radu, A., 'The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy', *German Law Journal* 25/4 (2024), 646–63

Bravo, M. V., 'What U.S. Regulators Can Learn From the EU AI Act', *Electronic Privacy Information Center*, 22 March 2024, accessed at https://epic.org/what-u-s-regulators-can-learn-from-the-eu-ai-act/ on 25 August 2024.

Breton, T., 'The European AI Act Is Here!', *LinkedIn*, 9 December 2023, accessed at https://www.linkedin.com/pulse/european-ai-act-here-thierry-breton-gcnre/ on 25 August 2024.

Djeffal, C., 'The EU AI Act at a Crossroads: Generative AI as a Challenge for Regulation', *European Law Blog*, 24 July 2023, accessed at https://www.europeanlawblog.eu/pub/the-eu-ai-act-at-a-crossroads-generative-ai-as-a-challenge-for-regulation/release/1?readingCollection=65b658d5 on 10 October 2024.

Edwards, L., *Regulating AI in Europe: Four Problems and Four Solutions*, Ada Lovelace Institute (March 2022), accessed at https://www.adalovelaceinstitute.org/wp-content/uploads/2022/03/Expert-opinion-Lilian-Edwards-Regulating-AI-in-Europe.pdf on 25 August 2024.

GDPR.EU, *2019 GDPR Small Business Survey* (May 2019), accessed at https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf on 24 August 2024.

Kaur, G., 'Concerns Remain Even as the EU Reaches a Landmark Deal to Govern AI', *CIO*, 11 December 2023, accessed at https://www.cio.com/article/1255863/concerns-remain-even-as-the-eu-reaches-a-landmark-deal-to-govern-ai.html on 24 August 2024.

Martens, B., 'The European Union AI Act: Premature or Precocious Regulation?', *Bruegel*, 7 March 2024, accessed at https://www.bruegel.org/analysis/european-union-ai-act-premature-or-precocious-regulation on 26 August 2024.

Mema, M., 'The EU AI Act: Two Steps Forward, One Step Back', *Global Governance Institute*, 19 March 2024, accessed at https://www.globalgovernance.eu/publications/the-eu-ai-act-two-steps-forward-one-step-back on 25 August 2024.

Özdemir, G. S., 'Navigating the EU AI Act: Exploring Challenges Amidst the Evolving Global Regulatory Landscape', *SETA* (December 2023), accessed at https://www.setav.org/en/assets/uploads/2023/12/P72En.pdf on 25 August 2024.

Papakonstantinou, V., 'The AI Act and a (Sorely Missing!) Right to AI Individualization; Why Are We Building Skynet?', *European Law Blog*, 16 July 2024, accessed at https://www.europeanlawblog.eu/pub/04y8qbam/release/1 on 10 October 2024.

Papakonstantinou, V. and de Hert, P., 'Post GDPR EU Laws and Their GDPR Mimesis. DGA, DSA, DMA and the EU Regulation of AI', *European Law Blog*, 1 April 2024, accessed at https://www.europeanlawblog.eu/pub/post-gdpr-eu-laws-and-their-gdpr-mimesis-dga-dsa-dma-and-the-eu-regulation-of-ai/release/1 on 10 October 2024.

Prabhakar, A., 'The EU AI Act Is a Cautionary Tale in Open-Source AI Regulation', *Center for Data Innovation,* 20 November 2023, accessed at https://datainnovation.org/2023/11/the-eu-ai-act-is-a-cautionary-tale-in-open-source-ai-regulation/ on 24 August 2024.

Scott, M., 'The EU's Online Content Rulebook Isn't Ready for Primetime', *Politico*, 14 February 2024, accessed at https://www.politico.eu/article/european-union-digital-services-act-dsa-thierry-breton/ on 25 August 2024.

Türk, V., 'Open Letter From the United Nations High Commissioner for Human Rights to European Union Institutions on the European Union Artificial Intelligence Act', Office of the United Nations High Commissioner for Human Rights, 8 November 2023, accessed at https://www.ohchr.org/en/open-letters/2023/11/turk-open-letter-european-union-highlights-issues-ai-act on 24 August 2024.

Wadhwani, S., 'Last Mile Trouble: What Needs To Be Sorted in EU AI Act Before Next Week's Trilogue Talks', *Spiceworks*, 29 November 2023, accessed at https://www.spiceworks.com/tech/artificial-intelligence/articles/eu-ai-act-in-trouble/ on 25 August 2024.

Zhang, A., 'The Promise and Perils of China's Regulation of Artificial Intelligence', *Columbia Journal of Transnational Law* (forthcoming), accessed at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4708676 on 27 August 2024.