

Aysenur Alma* - 24 January 2024

The EU AI Act: State of Play and the Potential for Regulatory Globalisation

Introduction

After negotiating for 36 hours, a provisional agreement on the EU AI Act¹ was achieved on 8 December 2023 in the trilogue negotiations with some relevant amendments to the initial proposal. With that, the draft act for the world's first comprehensive regulation of Artificial Intelligence (AI) is politically set. At the same time, the EU is exercising its main political capital – its regulatory power. Though the EU has relatively few tech firms operating globally with substantial market shares, the EU's regulatory activism in digital policy has succeeded in limiting the overarching power of external global tech giants in the European market. For instance, a historical €1.2 billion fine was imposed on Meta on the grounds of (the non-adherence to) the General Data Protection Regulation² (GDPR)³. Thus, the question arises as to what potential the upcoming AI Act holds and whether the regulation will have an extra-territorial reach. The finalisation of the EU AI Act is eagerly awaited, both within and outside of Europe.

The EU Commission's Proposal for an AI Act

The EU AI Act was proposed by the Commission in April 2021 and aims at holding liable all providers and deployers who put high-risk AI systems into service in the EU, regardless of the origin of the providing entity, thus imposing an extra-territorial scope.⁴ Artificial intelligence systems are defined as “machine-based system[s] that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments”.⁵ The proposal establishes a legal framework based on a risk assessment of AI-based products or services for people's health, safety or fundamental rights.⁷ Unacceptable (and thus banned) risks are presumed in specific cases, e.g. AI systems that can enable social scoring. According to the Commission's impact assessment, around 5-15 % of all AI systems

would fall into the high-risk category. In these cases, providers need to comply with enhanced transparency reporting and documentation obligations.⁸ Moreover, deployers must label special interacting AI products (e.g., emotional intelligence or deep fake systems) and inform natural persons of their exposure to such products. With regard to enforcement mechanisms, member states are required to establish market surveillance authorities (MSAs). MSAs can impose fines in cases of non-compliance of up to €35 million or 7% of the company's annual turnover, whichever is higher, depending on the infringement and size of the company.⁹

The Trilogue Outcome

The institutions and member states managed to overcome major disagreements in regulating AI in the final stages of the legislative process. Not only had the European Parliament imposed disputed changes in its positioning, but individual member states also had contradicting views on the provisions of the AI Act. Compared to the Commission's initial proposal, the provisional agreement reached in the trilogue imposes five major amendments:

- *Rules on high-impact general-purpose AI models*

The issue here was that the draft act's risk-based approach did not initially apply to so-called general-purpose AI (GPAI) and foundation models like OpenAI's GPT series. Foundation models are large-scale models that build the basis of a wide range of further, more specialised technologies by being trained on massive amounts of data.¹⁰ The Parliament had called for including specific transparency and risk-management obligations for providers of such foundation models when designed for or used in generative AI applications, e.g., to design their models to prevent them from generating illegal content. Contrary to that, in the Council, Germany, France and Italy positioned themselves against foundation

* **Aysenur Alma** recently graduated from CIFE's Master in Advanced European and International Studies - European Integration and Global Studies. She has an academic background in law and political science. Her research interests cover Technology Policy, Geopolitics and International Transport Policy. She has worked as a trainee for the German Federal Foreign Office and in the private sector.

models falling under the scope, arguing this would inhibit innovation and fearing for the competitiveness of their fast-growing national AI startups like Mistral or Aleph Alpha. This had caused a setback during the many months of negotiations.¹¹ In the trilogue the parties finally agreed on a tiered approach as a compromise. GPAI systems will therefore be subject to differing obligations depending on whether they pose “systematic risks”. GPAI models, with respect to the first tier, will have to comply with transparency requirements such as technical documentation or content used for training. GPAI models that are assessed as being a systematic risk are subject to more stringent reporting and transparency obligations.¹²

· *Revised system of governance*

The institutions agreed on establishing three new bodies: (1) an AI Office within the Commission with an advisory scientific panel consisting of independent experts; (2) an AI Board consisting of member states’ representatives, serving as a coordination platform and advisory body to the Commission; and (3) an advisory forum for stakeholders from the industry, civil society and academia.

· *Remote biometric identification*

The subject of AI use for real-time remote biometric identification systems was heavily controversial. While member states such as Germany lobbied for a complete ban, the negotiators finally decided to add strict exceptions for the use of such AI systems in law enforcement when certain crimes or threats such as terrorist attacks are concerned.

· *Fundamental rights impact assessment*

Before a high-risk AI system is put onto the market, a fundamental rights impact assessment must be carried out.

· *Penalties*

The provisional agreement contains more proportionate caps for small and medium-sized companies (SMEs) and start-ups in cases of infringements of the AI Act, by way of derogation from the usual sanctioning system.

Apart from these critical changes, further modifications to the general framework were made. For instance, the definition of AI systems was aligned with the approach proposed by the OECD. Additionally, it

has been clarified that the Act does not affect member states’ competences in national security matters. Moreover, the exceptions for AI systems in the area of research and innovation were expanded. To counter critical voices claiming that the AI Act is innovation-inhibiting, regulatory sandboxes were further strengthened and new provisions for testing AI systems in real-world conditions were created, all for the benefit of smaller companies.¹³ The provisional agreement now has to be formally adopted by the Parliament and the Council. The Act then becomes applicable two years after it enters into force, except for prohibitions, which will already apply after six months, and the rules on General Purpose AI which will apply after 12 months. In the transition period, the Commission will provide an AI Pact which will convene AI developers who voluntarily commit to implement the obligations of the AI Act prior to legal deadlines.¹⁴

Regulating the EU Market and Beyond?

Many recent EU regulations in digital policy have generated an extra-territorial reach. The kick-off that drew global attention was made in 2016 with the GDPR. The GDPR is considered to be an export hit and has become a global standard in data protection. The EU managed to unilaterally regulate the global marketplace with its data protection standards. The success of the GDPR was pushed forward by the peculiarities of the data economy and a profound extra-territorial scope within the legal design of the regulation. Not only have global companies adjusted their conduct to the stringent EU regulations, but other jurisdictions have also adopted “EU-style” regulations in the field of data protection (the so-called Brussels Effect)¹⁵. In addition to that, the Commission has lately been making headlines with its Digital Services Act (DSA) and Digital Markets Act (DMA) to further regulate and hold accountable large online platforms.¹⁶ Similarly, the proposal of an AI Act gained momentum, particularly due to the comprehensiveness of the EU’s approach and the international consensus of a regulatory vacuum. One can observe an emerging external regulatory agenda where the EU is actively promoting its human-centric regulation narrative in the digital sphere.¹⁷ In the AI Act’s explanatory memorandum, an external regulatory agenda is explicitly mentioned. It is stressed that the proposal aims at strengthening the Union’s role in setting global norms and standards, as well as

promoting its values and approach to digital policy and AI regulation. Thus, the EU proactively fosters its regulatory power as its political capital. Many factors accommodate this potential for an extra-territorial reach of the EU AI Act. Firstly, the affluence of the European market (450 million consumers) for the AI sector draws the attention of globally operating companies towards the Act. In 2023 the European Union spent \$34.2 billion (annual growth of approx. 29,6% from 2022 to 2027) on the AI industry. Globally, the EU's share of AI spending amounts to about 20,6%.¹⁸ Typical for the digital sector, the AI industry is (mostly) dominated by multinational firms and accordingly, the market has a globalised and oligopolistic structure.¹⁹ These companies cannot usually substitute the large consumer market of the EU and thus need to comply with EU laws for market access.

Another important factor is the EU's high regulatory capacity. In the provisional agreement on the AI Act, the parties determined different advisory bodies that would add expertise to the AI Office.

In addition to this, the Act sets out enforcement authorities that will impose fines in cases of non-compliance.

An important economic criterion within the assessment of extra-territorial reach is the so-called non-divisibility factor, i.e., the cost of maintaining two separate products (one for the EU market and another general product) that favours the regulatory globalisation of a more stringent standard.²⁰ Especially for global firms in the AI sector that provide high-risk systems, maintaining two products would require an early separation (a so-called forking) in the extensive production process of systems (design phase, data selection, data collection, data generation and training, system deployment and evaluation phase). Early forking brings with it increasing costs and decreasing economies of scale. Moreover, standardising global production to comply with EU rules can also be beneficial for a company to safeguard its reputation with regard to consumer protection, particularly in sensitive policy areas and high-risk AI systems.²¹ To make an analogy with the GDPR, for instance, many global companies such as Google have standardised their global privacy policies (complying with EU data protection laws) to signal to non-EU users that their data is as equally protected as EU users' data.

Lastly, the general principles of the AI Act, such as the general risk-based approach or fundamental rights assessments, have a high potential to develop an extra-territorial reach through a consensus on normative desirability. In these areas, the EU can profit from its first-mover advantage.²²

However, despite these examples of beneficial factors that favour the AI Act becoming a global standard *de facto* and legally, it is important to keep in mind the need to differentiate between industries or systems that make use of AI-based technologies, as well as particular parts or legal concepts of the Act. As Siegmann and Anderljung put it, "[What] holds for AI, in general, might not hold for the specific industries and AI systems that the EU AI regulation will apply to".²³ The AI Act is rather broad since AI use is potentially limitless. Thus, the potential for an external regulatory reach cannot be generalised. Furthermore, there are increasingly more technological means for economically viable early forking.²⁴ Lastly, the efficiency of the Act's enforcement methods and organs cannot be predicted for the time being. The case of the GDPR has shown that enforcement authorities in member states such as Ireland which hosts the European headquarters of global tech firms, can be systematically underfunded.²⁵ Another risk is the regionalisation of the markets when it comes to AI use in sensitive policy areas such as financial services.²⁶

Nevertheless, even the claim or expectation to produce such an extra-territorial effect benefits the regulatory power of the EU in the field of AI regulation. Most importantly it provides the EU with a strong basis to negotiate with external partners. The emerging policy field of AI regulation is on the agenda of most legislators globally. Thus, it is crucial that the EU has built a uniform approach. For instance, in last month's AI summit in London, Commission President Ursula von der Leyen entered the debates in a strong position for the Union.²⁷ This merging of the AI Act's internal dimension (the benefit of harmonisation of rules in the common market) and the external regulatory agenda increases the potential for individual areas of the EU AI Act to serve as a blueprint for AI regulation and to influence the global marketplace.

Conclusion

Taking into consideration the political sensitivity of regulating Artificial Intelligence, the trilogue results

are an important step forward towards the adoption of the world's first comprehensive AI regulation. The EU has established an extensive framework for safe and human-centric AI systems that has the potential to create a spillover to the global market space. This is particularly the case for the obligations regarding "high-risk" AI systems and fundamental concepts in sensitive policy areas. Nevertheless, it is important to keep in mind that the factors benefiting the regu-

latory power of the EU in digital and AI policy are not a given. For instance, the EU consumer market and access to it can – in the long run – lose its affluence as the importance of large consumer markets in emerging economies rises. Thus, simultaneous investments in future technologies in the AI sector remain indispensable for a global standard-setting and regulatory pioneering role of the EU.

References

- 1 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 2021/0106 (COD) [EU AI Act]
- 2 Bendiek, A. /Stürzer, I. (2023). "The Brussels Effect, European Regulatory Power and Political Capital: Evidence for Mutually Reinforcing Internal and External Dimensions of the Brussels Effect from the European Digital Policy Debate". *Digital Society* 2:5.
- 3 Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/EC, 2016 O.J. (L119) 1.
- 4 Satariano, A. (2023). *Meta fined \$ 1.3 Billion for Violating EU Data Privacy Laws*. New York Times.
- 5 Art. 2 (1) EU AI Act.
- 6 OECD. (2022). AI Policy Observatory. *The OECD Artificial Intelligence (AI) Principles*.
- 7 EU AI Act. Explanatory Memorandum. 1.1.
- 8 Commission Staff Working Document. Impact Assessment accompanying the AI Act. Art. 71.
- 9 European Parliament (2023). Press Release. *Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI*.
- 10 OECD. (2023). AI Policy Observatory. *A law for foundation models: the EU AI Act can improve regulation for fairer competition*.
- 11 Volpicelli, G. (2023). "Power grab by France, Germany and Italy threatens to kill EU's AI bill". Politico.
- 12 Council of the European Union (2023). Press Conference. "Part 8 – Q&A".
- 13 Council of the European Union (2023). Press Release. *Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world*.
- 14 European Commission (2023). Press Release. *Commission welcomes political agreement on AI Act*.
- 15 Bradford, A. (2019). *The Brussels Effect. How the European Union Rules the World*. New York 2020; online edn; Oxford Academic, 19. Dec. 2019.
- 16 Goujard, C./ Scott, M. (2023). *X vs. EU: Elon Musk hit with probe over spread of toxic content*. Politico.
- 17 see note 15 above, 21.
- 18 International Data Corporation (2023). *European Artificial Intelligence Market Driven by the Need for More Efficient Operations and Enhanced Security, Says IDC*.
- 19 Siegmann, C. /Anderljung, M. (2022). *The Brussels Effect and Artificial Intelligence. How EU regulation will impact the global AI market*. [Report], 3.
- 20 see note 15 above, 58.
- 21 see note 15 above, 61, 144.
- 22 Christakis, T. (2020). *European Digital Sovereignty. Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy*. Multidisciplinary Institute on Artificial Intelligence/ Grenoble Alpes Data Institute, e-book.
- 23 see note 19 above, 49.
- 24 Bradford, A. (2021). "The European Union in a globalized world: the 'Brussels Effect'". *Governing Globalization Issue #2. Revue Européenne du droit*.
- 25 Satariano, A. (2018). *New Privacy Rules Could Make This Woman One of Tech's Most Important Regulators: With Europe's sweeping new data privacy law, Ireland is in the middle of a standoff between regulators and tech companies*. New York Times.
- 26 See note 19 above, 31.
- 27 European Commission (2023). *Remarks of President von der Leyen at the Bletchley Park AI Safety Summit*.