

**15TH
NETWORK EUROPE
CONFERENCE**

European Integration in Times of Security Challenges

**SPLIT / CROATIA
9–10 SEPTEMBER
2024**

**Editors:
Andreas Kellerhals
Tobias Baumgartner
Fatlum Ademi**

European Integration in Times of Security Challenges



European Integration in Times of Security Challenges Copyright © by Tobias Baumgartner; Andreas Kellerhals; and Fatlum Ademi is licensed under a [Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License](https://creativecommons.org/licenses/by-nc-nd/4.0/), except where otherwise noted.

© 2025 – CC BY-NC-ND (Book), CC-BY-SA (Text)

Editors: Prof. Dr. Andreas Kellerhals, Dr. Tobias Baumgartner, Fatlum Ademi – Europa Institut an der Universität Zürich

Publisher: EIZ Publishing (<https://eizpublishing.ch>)

Layout & Production: buch & netz (<https://buchundnetz.com>)

ISBN:

978-3-03805-784-0 (Print – Softcover)

978-3-03805-785-7 (PDF)

978-3-03805-786-4 (ePub)

DOI: <https://doi.org/10.36862/eiz-784>

Version: 1.01 – 20250310

This work is available in print and various digital formats in **OpenAccess**. Additional information is available at: <https://eizpublishing.ch/publikationen/european-integration-in-times-of-security-challenges/>.

Digital transformation: Regulation of Artificial Intelligence in the European Union

Jelena Ceranic Perisic

Table of Contents

I.	Introduction	147
II.	Causes for the slow progress of the AI industry in the European Union	150
1.	Lack of investments	151
2.	An incomplete European single market	152
3.	A shortage of data	152
4.	Low attractiveness for European talent	153
III.	Regulation on Artificial Intelligence – Artificial Intelligence Act	154
1.	Scope and definitions	155
2.	Regulation of AI systems	156
a)	Prohibited AI practices	157
b)	High-risk AI systems	158
c)	Limited risk AI systems	159
3.	Regulation of general purposes AI models (GPAI)	160
a)	Horizontal requirements for GPAI models	160
b)	Requirements for GPAI models with systematic risks	160
4.	Measures in support of innovation	161
5.	Governance and sanctions	161
6.	Implementation timeline	161
7.	Financial penalties	162
IV.	Concluding remarks	163
V.	Bibliography	164

I. Introduction

The Fourth Industrial Revolution is gradually transitioning into the Fifth, which is characterized by the diminishing boundaries between the physical, digital, and biological realms.¹ Although the forthcoming era will prioritize concepts such as sustainability, human-centeredness, and environmental concern, there is no doubt that it will be characterized by the use of artificial intelligence in almost all aspects of life.

¹ Howells, 145 et seq.

To date, there is no universally accepted definition of artificial intelligence (hereinafter: AI). However, a number of definitions do capture its fundamental aspects.

At the very beginning, it would be interesting to see what Artificial Intelligence says about itself. We have asked ChatGPT itself to give us a definition of AI in general. It has responded with the following text:

“AI, or Artificial Intelligence, refers to the simulation of human intelligence in machines that are programmed to think and learn like humans. These systems can perform tasks that typically require human intelligence, such as understanding natural language, recognizing patterns, solving problems, and making decisions.”

One of the most used definitions is the updated OECD definition, which is integrated into the EU legislation. The definition stipulates: “An AI system is one that is based on a machine that, for explicit or implicit purposes, deduces, from the inputs 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 adaptability once deployed.”²

Although this OECD definition draws a broad perimeter, which is useful for framing the largest number of existing AI technologies, it does not consider the human component. This definition ignores other essential elements of artificial intelligence. Nonetheless, it should be clarified that AI is neither intelligent nor artificial.³ “Due to great expectations and possibilities deriving from its use, the fact that artificial intelligence is also a product of human being is often neglected.”⁴ “The work and development of technologies that artificial intelligence is based on relies on previously entered information and parameters entered by humans.”⁵

The general public became familiar with AI through ChatGPT roughly a year and a half ago. “ChatGPT is a language model created by the San Francisco-based AI company OpenAI. ChatGPT can generate natural language responses to various end-user queries. Its main focus is on language modeling, which includes creating plausible models that can accurately predict the following word in a given sequence based on the previous words. Such a system can gen-

² <https://www.oecd.org/en/publications/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_623da898-en.html>.

³ Bianchiani/Ancona, 1.

⁴ Avramovic/Jovanov, 162.

⁵ Andonovic, 112

erate text in any language, in any format, and on any topic in a few seconds.”⁶ However, it’s important to note that generative AI, which underpins ChatGPT, is just one type of AI. In fact, various AI applications have long been part of our everyday lives. These include algorithms used by social networks to recommend content, predictive analytics in finance, and programs that diagnose and personalize therapies in healthcare.

The transformative nature of this technology is undeniable: AI has the potential to revolutionize various aspects of human experience and, more profoundly, to alter reality itself and the very role of humans within it.

Five years ago, the White Paper on Artificial Intelligence drafted by the European Commission recognized the significance of the AI for the improvement of healthcare, national security, industry, production, farming.⁷ However, “artificial intelligence posed a puzzle for lawyers and academia all over the world”⁸, as it remains an uncertain and unpredictable field, with its implementation potentially giving rise to various legal issues.⁹

The challenge of AI has recently been addressed by the international community, particularly at the regulatory level.¹⁰ Significant efforts are being made to implement legislative actions in light of the rapid evolution of AI technologies. While several recent initiatives demonstrate a growing awareness of this issue, the European Union is emerging as a leader in regulating this technology, as seen with its AI legislation. Such an approach of the European Union to the issue of AI will be particularly discussed and examined later in the paper.

Accordingly, it is not surprising that the industrial development of AI technologies is becoming a new arena of fierce confrontation between global players.

In terms of approach to artificial intelligence, three models stand out in today’s market:

- the market-led US model;
- the state-led Chinese model;
- the rights-led European model.

⁶ Zivkovic, 331.

⁷ White Paper on Artificial Intelligence: A European approach to excellence and trust of 19 February 2020, COM (2020) 65 final.

⁸ Glintic, 33.

⁹ Mihajlovic/Coric, 9 et seq.

¹⁰ For more on regulatory interventions at the level of the European continent see *Ibid.*, 17–19. On initiatives on broader international level see Stanic/Tintor, 171–174.

The European approach is clear, at least in its intentions: to enhance AI research and industrial capacity while guaranteeing fundamental rights. The guiding principles are equally clear: the technological sovereignty of the European Union for strategic economy and the central role of people in the digital transformation.¹¹

Despite the ambition underlying this approach, it must be acknowledged that the European Union is, at best, a secondary player in the development of AI. This is not surprising, as it reflects the historically slow progress of the European innovation sector.¹²

This paper aims to examine the current state of digital transformation and the regulation of artificial intelligence within the European Union, addressing both practical and legislative dimensions. To this end, the paper is structured into four main parts. Following a brief introductory remark dedicated to the concept and definitions of AI (Part I.), the paper analyses the challenges faced by the EU in the context of artificial intelligence, with particular emphasis on the underlying factors contributing to the slow progress of the AI industry (Part II.). The third part delves into the key features of the new AI Act (Part III.), highlighting its provisions and the categorization of use cases based on their level of risks to health, safety, and fundamental rights. Finally, the paper seeks to offer a preliminary assessment of whether the regulatory approach introduced by the AI Act effectively addresses the causes of the EU's slow progress in the AI sector (Part IV.).

II. Causes for the slow progress of the AI industry in the European Union

At the very beginning, the question arises as to the root causes of the slow progress of the AI industry in the EU. This part of the paper will briefly explore four primary factors contributing to the industry's stagnation and suggest potential solutions to address them. Those factors are:

1. Lack of investments → financing of the European AI
2. An incomplete European Single Market → Building an ecosystem of excellence: a Union tailored to AI
3. A shortage of data → Feeding AI: European data sovereignty?
4. Low attractiveness for European talent → Skills for AI: European expertise

¹¹ Bianchiani/Ancona, 2.

¹² *Ibid.*

I. Lack of investments

The limited availability of venture capital and a weak stock market are among the primary factors contributing to the slow progress of the AI industry, hindering the development of a dynamic technological innovation sector for start-ups in this field. The situation is even more concerning when compared to other global players: from 2012 to 2020, venture capital investments in the United States were ten times greater than those in the euro area. Furthermore, equity investment in AI within the European Union accounts for less than 10%, while China and the United States together hold approximately 80% of global AI investments. This gap is likely to continue expanding. Moreover, the power dynamics are striking: as illustrated in the table, only three European countries—Germany, France, and Spain—are among the top fifteen nations in terms of AI investment, and US private investment is thirty-five times greater than that of Germany, the largest investor in AI within Europe.¹³

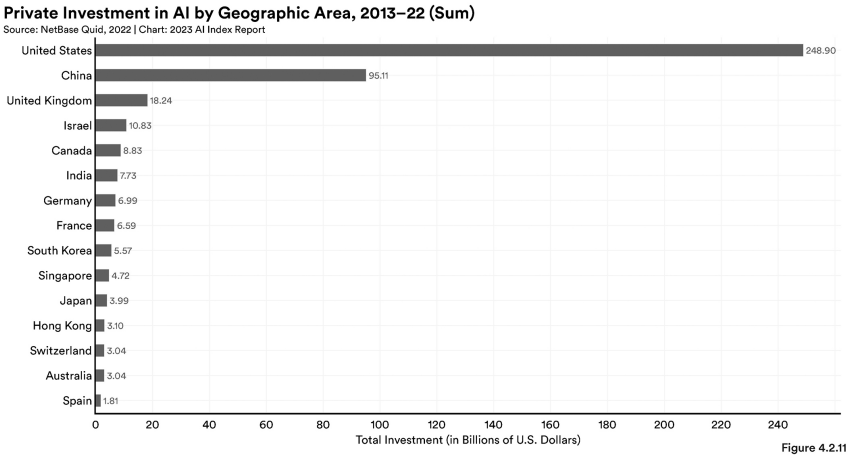


Fig. 1 HAI – [Artificial Intelligence Index Report 2023](#) – page 190

To address this issue, it would be necessary to revise the rules of the European financial framework to facilitate investment in start-ups, including the adoption of more flexible regulations for institutional investors.¹⁴

¹³ Bianchiani/Ancona, 2–4.

¹⁴ *Ibid.*, 3–4.

2. An incomplete European Single Market

The lack of an integrated innovation ecosystem represents a significant obstacle to the establishment of the European Union as a dynamic centre for innovation, with substantial repercussions for the burgeoning artificial intelligence sector. This deficiency not only constrains the development and growth of European excellence but also jeopardizes the EU's position in global competitive dynamics. Consequently, it is imperative to create conducive conditions for the establishment of an ecosystem of excellence in AI.¹⁵

In terms of fostering new AI ventures, the EU, and its Member States to an even lesser extent, have not effectively challenged the dominant positions held by the United States and, to a lesser degree, China. Key criticisms of the current situation include delays in data availability crucial for AI development, inefficient talent mobility, and insufficient funding for AI initiatives.

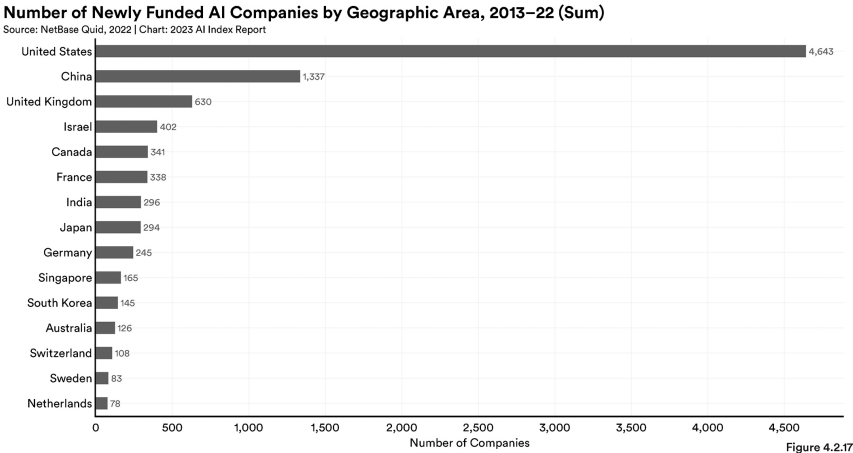


Fig. 2 HAI – [Artificial Intelligence Index Report 2023](#) – page 194

The main challenges are the geographical fragmentation of innovation and the still incomplete European digital market.

3. A shortage of data

Data are frequently described as the “new oil”, a characterization that is increasingly contested. Nevertheless, data remain a critical resource for artificial

¹⁵ *Ibid.*, 4–5.

intelligence (AI), both in terms of research and development and for facilitating its widespread adoption by non-specialist users and businesses. “The usage of data, data science, and analytic tools that enable extracting insights from a great amount of randomly collected data still remains a viable field in many commercial sectors due to the importance of collected information.”¹⁶ Therefore, it is urgent for Europe to address the significant delays in data availability and access to ensure strategic autonomy and technological sovereignty in AI.¹⁷

The underlying causes of the data shortage are closely linked to the digital industry ecosystem within Europe. First, a few non-European “Big Tech” companies control the majority of global data, while European small and medium-sized enterprises (SMEs) typically lack comprehensive internal databases and have limited access to external ones. Additionally, the fragmentation of the European digital market hampers the creation of unified data sets, largely due to insufficient collaboration and data-sharing practices between private enterprises, institutions, and other stakeholders. This fragmentation also accounts for the disparity with the United States and China, which benefit from two distinct but equally powerful forces—private sector initiatives and central institutions—that facilitate the construction of extensive data sets.¹⁸

The Common European Data Spaces (CEDS) is an EU initiative designed to facilitate large-scale data collections at significantly lower upfront costs for European businesses. It aims to create a “level playing field” for data sharing and exchange, thereby reducing the dominance and dependency on large, quasi-monopolistic entities.¹⁹

4. Low attractiveness for European talent

The competitiveness of the European Union cannot be assessed without acknowledging the crucial role of talent. The artificial intelligence relies on the availability of natural intelligence, that is, skilled human capital, both for research and development (R&D) activities and for the widespread adoption of AI technologies.²⁰

The EU does not face a shortage in the production of talent, but rather an inability to retain it. In terms of R&D, European academic research in AI is increasingly threatened by the migration of human capital, particularly to the

¹⁶ Glintic, 102.

¹⁷ Bianchiani/Ancona, 5.

¹⁸ *Ibid.*

¹⁹ Ryan/Gürtler/Bogucki, 2 et seq.

²⁰ Bianchiani/Ancona, 6.

United States, where researchers are offered higher salaries, more flexible contracts, and more prestigious academic and entrepreneurial opportunities.²¹ To illustrate the scale of this brain drain, consider that one-third of AI talent in American universities originates from the EU.

It is therefore unsurprising that one of the primary obstacles cited by European companies in adopting AI is the scarcity of talent in the labour market.²²

Prioritizing AI expertise has become a recurring theme in European policy-makers' recent statements. EU Commission President has advocated for a concerted effort to tackle labour market challenges, highlighting critical issues such as skills and labour shortages. The European Commission aims to foster AI talent in Europe by providing the necessary infrastructure and public-private partnerships to support researchers.²³

The European Union's strategic objective must be to establish a hub for AI R&D that not only retains European talent but also attracts skilled professionals from other countries.²⁴

III. Regulation on Artificial Intelligence – Artificial Intelligence Act

The “Act” is a regulation based on Article 114 of the Treaty on the Functioning of the European Union (TFEU), which concerns the approximation of laws to improve the functioning of the internal market.²⁵

The AI Act²⁶ was adopted by EU co-legislators in May 2024 and came into force 20 days after its publication in the Official Journal of the European Union on July 12. It will be fully applicable starting August 2, 2026. In the meantime, the European Commission has introduced the AI Pact²⁷, a voluntary initiative that

²¹ <<https://www.stiftung-nv.de/publications/where-is-europes-ai-workforce-coming-from>>

²² Bianchiani/Ancona, 6.

²³ <https://commission.europa.eu/about/commission-2024-2029/president-elect-ursula-von-der-leyen_en>

²⁴ Bianchiani/Ancona, 7.

²⁵ Engel, 13 et seq.

²⁶ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689 of 12 July 2024.

²⁷ <<https://digital-strategy.ec.europa.eu/en/policies/ai-pact>>.

encourages AI providers to proactively adhere to the key obligations of the AI Act before its official enforcement.

One of the primary objectives of the AI Act is to regulate the deployment of AI technology across various sectors through a risk-based approach. In this context, the Act establishes tiered obligations for different stakeholders in the AI value chain, tailored to the level of risk associated with specific AI applications. As such, the AI Act should be regarded as a targeted regulatory intervention, rather than a broad, cross-cutting legislation like the General Data Protection Regulation (GDPR).²⁸

The AI Act can be regarded as one piece in a complex AI regulatory puzzle²⁹, i.e. the AI Act is also part of a broader regulatory framework, which consists of Data, Infrastructure and Algorithms.³⁰

Given the length and complexity of the AI Act, this chapter examines only its most significant provisions. The analysis of the AI Act will start by presenting the scope and definitions. Since the AI Act makes a distinction between AI systems and General-Purpose AI models (GPAI), provisions regulating both categories will be examined. Finally, the measures to support innovation outlined in the AI Act will be presented; afterwards, governance, sanctions, and the implementation timeline will be briefly outlined.

1. Scope and definitions

The AI Act has a very broad scope and a strong extraterritorial reach, as it applies to any AI system having an impact in the EU, regardless of the provider's place of establishment. Specifically, the AI Act would apply when the AI system *is placed on the market or put into service in the EU, when a user is located in the EU or when the output is used in the EU*.³¹

AI itself is defined in very broad terms in the AI Act. It covers “any machine-based system designed to operate with varying levels of autonomy and that

²⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 95/46/EC, OJ L 119 of 4 May 2016.

²⁹ Stanic/Tintor, 169 et seq.

³⁰ Samman/de Vanssay, 1.

³¹ Art. 2 of the Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

may exhibit addictiveness after deployment and 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.”³²

The AI Act distinguishes between AI systems and *General-Purpose AI models* (GPAI), which are AI models trained with a large amount of data, using self-supervision at scale and which can competently perform a wider range of distinct tasks.

AI Act Provides for several exceptions regarding its scope:

- “AI systems and models that are developed and used exclusively for military, defence and national security purposes;
- AI systems and models specifically developed and put into service for the sole purpose of scientific research and development;
- Any research, testing, or development activity regarding AI systems or models prior to their being placed on the market or put into service;
- AI systems released under free and open-source licenses, except where they fall under the prohibitions and except for the transparency requirements for generative AI.”³³

2. Regulation of AI systems

The AI Act distinguishes four categories of use cases based on their level of risk to health, safety, and fundamental rights. Specific requirements for providers and users of these systems are associated with each category. These categories are:

- Prohibited AI practices;
- High-risk AI systems;
- Limited risk AI systems; and
- Low- or minimal-risk AI systems.

The following sections will examine Prohibited AI practices, High-risk AI systems and limited-risk AI systems, except low or minimal risks, where Member States and Commission merely ‘encourage’ and ‘facilitate’ voluntary codes of conduct.³⁴

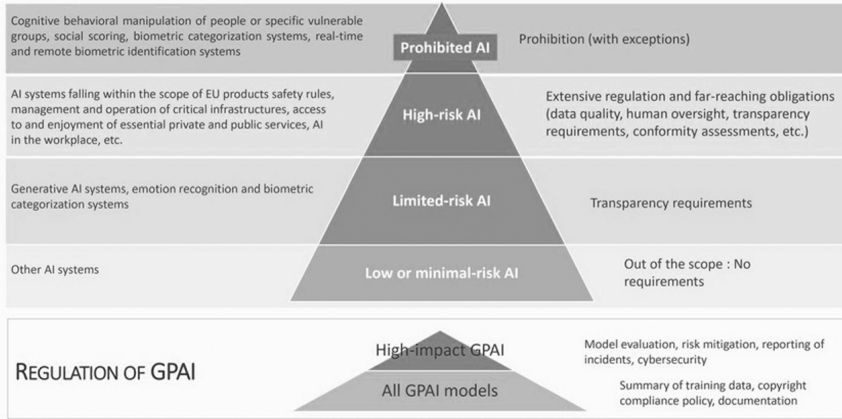
³² Art. 3 of the Regulation (EU) 2024/1689.

³³ Samman/de Vanssay, 2.

³⁴ Veale/Zuiderveen Borgesius, 98.

THE AI ACT ARCHITECTURE

SAMMAN



Source: What to take away from the European law on Artificial Intelligence, Schuman Paper 757/2024

a) Prohibited AI practices

The AI Act prohibits the placing on the market, the putting into service or the use of the following AI systems (with exceptions for certain cases):³⁵

- “AI systems that deploy subliminal techniques beyond a person’s consciousness or purposefully manipulative or deceptive techniques;
- AI systems that exploit any of the vulnerabilities of a person or specific group of persons due to their age, disability, or a specific social or economic situation;
- Biometric categorization systems that categorize individual natural persons based on their biometric data to deduce or infer some sensitive attributes;
- AI systems for social scoring purposes;
- Use of ‘real-time’ remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, with some important exceptions;
- AI systems for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence;
- AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;

³⁵ Art. 5 of the Regulation (EU) 2024/1689.

- AI systems that infer the emotions of a natural person in situations related to the workplace and education, with some exceptions.”

b) *High-risk AI systems*

The regulation of high-risk AI systems constitutes the core of the AI Act.³⁶ It outlines the criteria for classifying AI systems as high-risk, along with a series of obligations and requirements for these systems and the various stakeholders in the value chain, ranging from providers to deployers.

Qualification of high-risk AI systems

The AI Act qualifies as high-risk some AI systems that have a significant harmful impact on health, safety, fundamental rights, the environment, democracy and the rule of law. More specifically, the AI Act establishes two categories of high-risk AI systems:³⁷

AI systems are caught by the net of EU product safety rules (toys, cars, health, etc.), if *they are used as a safety component of the product or are themselves a product* (e.g. AI application in robot-assisted surgery).³⁸

AI systems are listed in an annex to the regulation, which outlines the use cases and sectors where the deployment of AI is deemed high-risk. In summary, the following areas and AI systems are included:³⁹

- Biometrics;
- Critical infrastructure;
- Education and workplace;
- Access to essential services;
- Law enforcement, justice, immigration, and the democratic process.

The AI Act also allows providers of high-risk AI systems to demonstrate that their systems do not qualify as high-risk (referred to as “the filter”) and do not significantly impact the decision-making process. To this end, providers must show that they meet at least one of the following conditions:

- “the AI system is intended to perform a narrow procedural task;
- the AI system is intended to improve the result of a previously completed human activity;

³⁶ Art. 6 of the Regulation (EU) 2024/1689.

³⁷ Samman/de Vanssay, 3.

³⁸ *Ibid.*

³⁹ Art. 7 of the Regulation (EU) 2024/1689.

- the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review;
- the AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III.”⁴⁰

*Main requirements for high-risk AI systems and obligations for parties in the AI value chain*⁴¹

First, the AI Act establishes a set of requirements for high-risk AI systems, including risk management, data governance, technical documentation, record-keeping, instructions for use, human oversight, as well as accuracy, robustness, and cybersecurity.

Second, the AI Act imposes a range of obligations on various stakeholders within the value chain, including providers, importers, distributors, and deployers. It also outlines the rules for determining the distribution of responsibility, particularly when one of these parties makes a substantial modification to an AI system. The majority of obligations are placed on providers, encompassing areas such as compliance and registration, quality management systems, documentation maintenance, logs, corrective actions, and the duty to inform.

c) *Limited risk AI systems*

The third category pertains to providers and deployers of generative AI systems, as well as deployers of emotion recognition or biometric categorization systems, who must, among other things, comply with the transparency requirements. When it comes to *chatbots* it is essential to inform individuals that they are engaging with an AI system, ensuring transparency regarding the nature of the interaction. In regard to *generative AI*, the obligation is to maintain clarity and prevent confusion. It is crucial to mark the outputs in a machine-readable format, ensuring they are identifiable as artificially generated or altered (e.g., through watermarking techniques). As for *deepfakes*, content must be clearly labelled as either artificially generated or altered. Additionally, it is important to notify users when such content is part of a work that is intentionally artistic, creative, satirical, or fictional. Regarding *Generated News Informa-*

⁴⁰ Samman/de Vanssay, 3.

⁴¹ Art. 16 of the Regulation (EU) 2024/1689.

tion, it is necessary to disclose when content has been artificially generated or manipulated, except in cases where the content has been subjected to human review or editorial oversight.⁴²

3. Regulation of general purpose AI models (GPAI)

The AI Act establishes a two-tier regulatory framework for General-Purpose AI (GPAI) models. The first layer of obligations applies to all GPAI models, while the second layer is reserved for those GPAI models that present systematic risks.⁴³

a) Horizontal requirements for GPAI models

Under the AI Act, some obligations are imposed on the providers of GPAI models, regardless of whether their models are used in high-risk areas. These obligations relate to:⁴⁴

- drawing up and keeping technical documentation (*inter alia* training, testing process and evaluation results);
- Providing documentation to users integrating the GPAI model in their own AI systems (including information about the limitations and capabilities of the model);
- Putting in place a policy to respect EU copyright law;
- Publishing a detailed summary of the content used for training of the model.

However, providers of non-systematic open-source models are exempt from the first two obligations. The definition of open source is narrow, as it only pertains to “models released under a free and open license that allows for the access, usage, modification, and distribution of the model, and whose parameters, including the weights, the information on the model architecture, and the information on model usage, are made publicly available”.⁴⁵

b) Requirements for GPAI models with systematic risks

The AI Act defines GPAI models with systematic risks as those with “high-impact capabilities”, or in other words, the most capable and powerful models.

⁴² Samman/de Vanssay, 4.

⁴³ Art. 51 of the Regulation (EU) 2024/1689.

⁴⁴ Samman/de Vanssay, 4–5.

⁴⁵ Samman/de Vanssay, 5.

In addition to the first layer of obligations, providers of GPAI models with systematic risks are required to:⁴⁶

- “Perform model evaluation with standardized protocols and tools;
- Assess and mitigate possible systematic risk at EU level;
- Report serious incidents and corrective measures to the European Commission and national authorities;
- Ensure an adequate level of cyber security protection.”

4. Measures in support of innovation

The primary measure outlined in the Commission’s proposal is the mandatory establishment of at least one AI regulatory sandbox in each member state.⁴⁷ A sandbox is a framework created by a regulator that enables businesses, particularly start-ups, to conduct live experiments with their products or services in a controlled environment under the supervision of the regulator.⁴⁸

5. Governance and sanctions

The AI Act establishes a complex and hybrid governance framework, with the implementation and enforcement powers shared between the EU and national levels.

The European Commission will play a central role in the governance and implementation of the AI Act. In summary, it will be responsible for enforcing provisions related to GPAI models, ensuring the harmonization of the AI Act’s application across the EU, defining compliance with the AI Act, and updating key aspects of the regulation. At the national level, regulators will be tasked with enforcing all provisions related to prohibited and high-risk AI practices.⁴⁹

6. Implementation timeline

The AI Act was published in the EU Official Journal on 12 July 2024. It entered into force 20 days after the publication and will be applied gradually.

The rules governing prohibited AI practices are expected to come into effect in early 2025 – six months after the regulation’s entry into force.

⁴⁶ Art. 55 of the Regulation (EU) 2024/1689.

⁴⁷ Art. 58 of the Regulation (EU) 2024/1689.

⁴⁸ Samman/de Vanssay, 5.

⁴⁹ Samman/de Vanssay, 5.

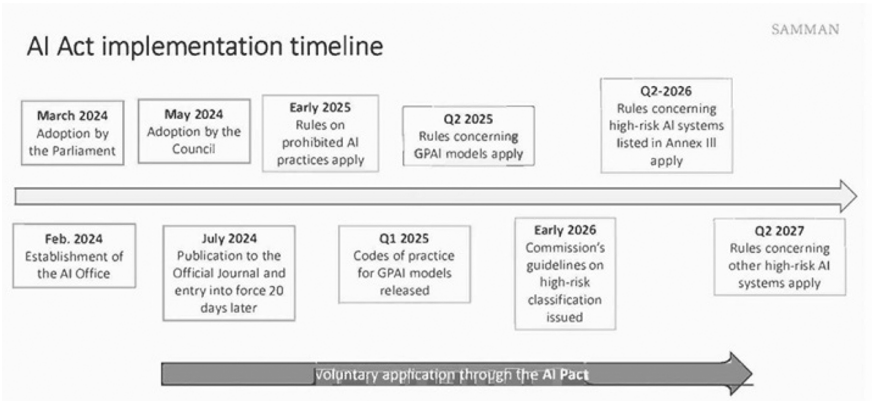
Codes of practice for General Purpose AI (GPAI) models must be issued by the Commission no later than nine months after the regulation's entry into force, which is anticipated for the first quarter of 2025.

Rules related to GPAI models will apply 12 months after the regulation enters into force, around mid-2025. This will also mark the deadline for designating national market surveillance authorities and issuing guidelines on high-risk AI systems by the Commission.

The Commission is required to issue guidelines on the classification of high-risk AI systems no later than 18 months after the regulation's entry into force, expected in early 2026.

Rules concerning high-risk AI systems listed in Annex III will come into effect 24 months after the regulation's entry into force, which is projected for mid-2026.

Rules regarding other high-risk AI systems will apply 36 months after the regulation's entry into force, anticipated for mid-2027.



Source: What to take away from the European law on Artificial Intelligence, Schuman Paper 757/2024

7. Financial penalties

In addition to being able to request corrective actions, national authorities and the Commission will have the authority to impose fines, the amount of which will vary depending on the nature of the infringements.⁵⁰

⁵⁰ Art. 99 of the Regulation (EU) 2024/1689.

IV. Concluding remarks

We live in an era where it is evident that innovations are progressing at a pace that outstrips the capacity of legislators to keep up. Therefore, the question arises as to how to approach the regulation of AI in a manner that avoids the waste of time and resources.

When it comes to the regulation of AI, three approaches have emerged in comparative law: the market-led US model, the state-led Chinese model, and the rights-led European model. It is undisputed that the EU's approach is inspired by the principles of technological sovereignty and the central role of humans in digital transformation. This approach is completely in line with the EU's fundamental objective of advancing research in the field of AI and protecting human rights. The recently introduced AI Act has been developed entirely in accordance with these principles.

Considering the causes of slower progress in the EU's AI industry, the question arises whether the new AI Act will contribute to addressing these causes, which should certainly be one of its goals. However, even before the beginning of its implementation, part of the academic and professional community has expressed concerns that the regulation may have gone too far and that various types of challenges may arise during its enforcement.⁵¹ Moreover, there is a well-founded fear that this regulatory approach could further weaken the EU's position relative to the United States and China.

In this regard, it is often heard in both academic and professional circles that the AI revolution represents a unique opportunity that Europe cannot afford to overlook.⁵² Over the past fifteen years, during which it has fallen behind the United States and, to a lesser extent, China, Europe often seemed to be the "continent of the old". This perception is not so much demographic but, more importantly, stems from widespread mistrust of innovation, reluctance to embrace risk, and a tendency to emphasize the dangers of the unknown rather than the opportunities for progress. Ultimately, innovation is measured in the marketplace, where the European Union, at best, plays a supportive role.

It is clear that the EU has chosen an approach based on rights. However, it may be necessary to find the right balance in this regard, in terms of regulation, but not over-regulation.

⁵¹ Veale/Zuiderveen Borgesius, 97 97 et seq., Samman/de Vanssay , 1 et seq.

⁵² Bianchiani/Ancona.

Bibliography

- Andonovic Stefan, Stratesko-pravni okvir vestacke inteligencije u uporednom pravu [Strategic-legal framework of Artificial Intelligence in comparative law], *Strani pravni zivot* [Foreign Legal Life], 3/2020, 111 et seq, <https://doi.org/10.5937/spz64-28166>
- Avramovic Dragutin/Jovanov Ilija, Sudijska (ne)pristrasnost i vestacka inteligencija [(Im)partiality of a judge and Artificial Intelligence], *Strani pravni zivot* [Foreign Legal Life], 2/2023, 161 et seqq, https://doi.org/10.56461/SPZ_23201KJ
- Bianchiani Niccolo/Ancona Lorenzo, Artificial Intelligence: Europe must start dreaming again, *Schuman Paper* 728/2023, 1 et seq.
- Glintic Mirjana, The impact of digitalization on insurance contract and insured's rights, in: D. Celic (ed.), *The dynamics of modern legal order*, Faculty of Law at the University of Pristina, Institute of Criminological and Sociological Studies, Institute of Comparative Law, 2024, 101 et seq.
- Glintic Mirjana, Insurance market response to challenges imposed by Artificial Intelligence, in: Glintic, Obradovic (ed.), *Causation of Damages, Damage Compensation and Insurance*, Institute of Comparative Law, Association for Tort Law, Judicial Academy, Belgrade 2024, 33 et seq.
- Engel Annegret, Licence to Regulate: Article 114 TFEU as Choice of Legal Basis in the Digital Single Market, in: Engel, Groussot, Petursson (ed.), *New directions in digitalization*, Springer, 2025, 13 et seq.
- Howells Geraint, Protecting Consumer Protection Values in the Fourth Industrial Revolution, *Journal of Consumer Policy*, 43/2020, 145 et seq.
- Mihajlovic Aleksandar/Coric Vesna, Artificial Intelligence and discrimination – strengths and weaknesses of the current European anti-discrimination legal framework, in: Kostic/Rodina/Russo (ed.), *Regional Law Review*, 2024, 9 et seq, https://doi.org/10.56461/iup_rlr.2024.5.ch2
- Ryan Mark/Gürtler Paula/Bogucki Artur, Will the real data sovereign please stand up? An EU policy response to sovereignty in data spaces?, *International Journal of Law and Information Technology*, Vol. 32, 1/2024, <https://doi.org/10.1093/ijlit/eaee006>
- Samman Thaima/de Vanssay Benjam, in: What to take away from the European law on Artificial Intelligence, *Schuman Paper* 757/2024, 1 et seq.
- Stanic Milos/Tintor Ljubomir, Human rights and Artificial Intelligence – International Public Law and Constitutional Aspects, in: Kostic/Rodina/Russo (ed.), *Regional Law Review*, 2024, 169 et seq, https://doi.org/10.56461/iup_rlr.2024.5.ch2
- Veale Michael/Zuiderveen Borgesius Frederik, Demystifying the Draft EU Artificial Intelligence Act, *Cri* 4/2021, 97 et seq.
- Zivkovic Antonije, Computer programs legal protection framework with special reference to Artificial Intelligence ChatGPT, *Foreign Legal Life*, 3/2024, 317 et seq, https://doi.org/10.56461/SPZ_24301KJ