EU Supervisory Digital Finance Academy

Digital Finance in the EU: Navigating new technological trends and the AI revolution

Editors

Lorenzo Moretti, Laura Rinaldi, Pierre Schlosser

Funded by the European Union

European Commission

EUI European University Institute

eba European Banking Authority

eiopa European Insurance

ESMA European Securities and Markets Authority

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

This e-book has received funding from the EU TSI Programme in the framework of the EU Supervisory Digital Finance Academy (EU-SDFA) project, grant agreement number 101092497.

Published by
European University Institute (EUI)
Via dei Roccettini 9, I-50014
San Domenico di Fiesole (FI)
Italy

ISBN:978-92-9466-637-6
doi:10.2870/8600400
QN:QM-01-24-186-EN-N

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.
This e-book has received funding from the EU TSI Programme in the framework of EU-SDFA project, grant agreement number 101092497

Digital Finance in the EU: Navigating New Technological Trends and the AI Revolution

The EU Supervisory Digital Finance Academy's Second Year e-Book

EDITED BY

Lorenzo Moretti, Florence School of Banking and Finance, European University Institute
Laura Rinaldi, European Commission DG REFORM
Pierre Schlosser, Florence School of Banking and Finance, European University Institute

European University Institute, Florence, Italy

Table of Contents

6. The EU AI Act: logic, content and implications for finance

Marco Almada

University of Luxembourg

The AI Act[1] is the cornerstone of the EU's approach to AI regulation. One of the first laws on artificial intelligence to be enacted worldwide,[2] it governs AI technologies with a risk-based approach. This approach aims to foster the adoption of AI systems in the EU by creating a legal framework that balances the economic opportunities created by AI with the need to address the risks that the use of AI might create in terms of protecting public values such as fundamental rights, democracy, and the rule of law.[3]

In general terms, the Act relies on an ex-ante assessment by the lawmaker of the risks associated with some AI technologies, which will determine the legal framework applicable to AI-based products and services. Each framework establishes different legal requirements drawn from different strands of EU product safety law (Almada & Petit, 2025) which address the perceived risks that AI creates in that context. In the following pages, we examine the core elements of the AI Act.

1 Regulation (EU) 2024/1689. All article, annex and recital numbers mentioned in the text come from this regulation, unless otherwise stated.

2 Even though the AI Act was the first major legislative initiative on AI, both the Council of Europe and the US state of Colorado approved AI-related regulations before the AI Act was published in the EU Official Journal on 12 July 2024.

3 Art. 1(1).

Because the AI Act is a long and complex legal instrument,[4] the following pages only offer a bird's-eye view of its legal framework. By doing this, they offer a glimpse of its relevance in financial supervision[5] and allow the reader to examine whether the AI Act succeeds in its ambition to foster innovation in AI, or whether, as feared by some commenters (Draghi, 2024, p. 26), it can be a roadblock in the European approach to AI.

First, Section 1 discusses the overall policy logic that underpins the EU's approach to AI regulation. Then, Section 2 sketches the main regulatory requirements established by the Act and Section 3 discusses the interplay between the Act and EU financial market regulation. Finally, the chapter concludes (Section 4) with a brief discussion of how and why the AI Act matters to financial institutions and supervisory authorities.

1. The EU's rationale for AI regulation

In April 2021, the Commission introduced its original proposal for an Artificial Intelligence Act. After many years of sustained progress in AI technologies, which were being applied in an ever-growing number of fields, this proposal was a reaction to substantial controversy regarding the opportunities and risks associated with AI (Bakiner, 2023). The Commission relied on various sources, such as the work of a High-Level Expert Group on AI that operated from 2018 to 2019, and the EU's experience with product safety law (Mazzini & Scalzo, 2022). This process resulted in a legislative proposal that built on existing product safety instruments but featured some fundamental changes which reflected the unique risks associated with AI technologies.[6]

During the AI Act legislative procedure, the original proposal evolved in several important ways. In particular, the final version of the Act reflected the need to address general-purpose models, such as large language models, which only became widespread after the proposal was introduced.[7] Nevertheless, the Act that is now in force largely follows the regulatory architecture proposed in 2021 by the Commission, even though many details underwent substantial adjustments.

4 It has 113 articles, accompanied by 180 recitals and 13 annexes.

5 For an in-depth analysis of this sector, see Passador (2025).

6 See Section 2.6.2 below.

7 On this point, see (Almada & Petit, 2025, sec. 4).

One crucial thing that remained unchanged is that the AI Act pursues a broad range of aims. Just like traditional product safety legislation, the provisions of the Act are meant to ensure a high level of health and safety protection of those affected by the use of AI. At the same time, as mentioned above, they also aim to protect other public values such as fundamental rights. These aims do not always align with one another. For example, Article 10(5) creates a new legal basis for processing sensitive personal data on the grounds that existing rules under EU data protection law[8] were not enough to enable measures to mitigate potential biases in data used to train algorithms in high-risk contexts. Thus the structure of the AI Act reflects a variety of compromises and trade-offs.

To address the risks associated with AI technologies, the AI Act controls access to the EU single market. It defines two AI-related products, the *AI system* and the *AI model*. It then stipulates that such products can only be placed on the EU single market if they meet certain requirements.[9]

An AI system is a machine-based system that infers from its input data how to generate outputs that can influence physical or virtual environments. These outputs can take various forms, such as predictions, recommendations or decisions.[10] For example, a system that uses a machine learning technique to detect outliers in financial transactions would meet this definition. An AI model, instead, is a component that allows an AI system to make such inferences.[11] For example, many uses of AI in 2024 are powered by large language models such as GPT-4 and Claude (OECD, 2023). To make an analogy with another branch of product safety law, the AI Act sets rules for both cars (AI systems) and engines (models).

Different types of systems and models are subject to different requirements, which are examined more closely in Subsection 2.6.2 below. Some of these requirements stipulate technical properties that an AI system or model must have. Others, instead, oblige actors involved in the AI supply chain to monitor incidents related to their systems or models, adopt measures to address hazards and cooperate with market surveillance authorities. These two sets of obligations aim to both mitigate risks and create a mechanism for responding to any harms that escape the initial measures.

8 See, in particular, Art. 9 Regulation (EU) 2016/679 (GDPR).

9 In addition, the AI Act lays down rules regarding how AI systems are put into service and used, as is discussed below.

10 Art. 3(1). Under this definition, an AI system may or may not rely on self-learning technologies, and it might be based on techniques other than machine learning.

11 Recital 97.

2. Risk regulation in the AI Act

The two kinds of products regulated by the AI Act – systems and models – involve different risks. When it comes to AI systems, the Act focuses on the purpose for which the system is developed and used:[12]

- Article 5 stipulates a closed list of practices in which AI poses an unacceptable risk. For each practice listed, placing on the market, putting into service and using an AI system to that end are prohibited.[13] For instance, one cannot use AI to download facial images from the internet or CCTV footage in order to create or expand facial recognition databases.[14]
- Article 6 defines a set of high-risk applications. Developing and using AI for such applications is only acceptable if done in conformity with a harmonised EU legal framework, as is detailed in Subsection 2.6.2.1 below.
- If the purpose of an AI system is not covered by either of the two lists, the AI Act considers that its risks are addressed by sector-specific regulation, either at the EU or at the national levels.

In addition, some rules apply regardless of the risk level of an activity. Providers[15] and deployers[16] of AI systems are required to foster AI literacy in their organisations.[17] Some systems are subject to transparency requirements.[18] For example, the provider of a chatbot must, in most cases, make sure that human users are aware they are interacting with an AI system.[19] For the most part, however, the legal framework applicable to an AI system is a function of its intended purpose.

For AI models, the AI Act follows a different approach. It creates cumulative layers of rules that apply to models. Most AI models are not subject to any special conditions to be placed on the EU market. If a model can be used

12 Recital 12.

13 Even if the practice itself remains lawful.

14 Art. 5(1)(e).

15 That is, an actor (regardless of its legal form) which either develops an AI system or commissions its development to market it under its own name or trademark: Art. 3(3).

16 That is, an actor (regardless of its legal form) using an AI system under its own authority: Art. 3(4).

17 Art. 4.

18 Art. 50.

19 Art. 50(1).

as a component of a broad range of AI systems, it is subject to a lightweight set of legal requirements that apply to all *general-purpose AI models*.[20] Additional rules apply to general-purpose models deemed to pose a systemic risk.[21] This framework is introduced in Subsection 2.2 below.

2.1 The legal framework(s) for high-risk AI systems

Under the AI Act, high-risk AI systems are subject to harmonised rules at the EU level.[22] Like a traditional product safety instrument, the Act establishes requirements that the provider of an AI system must meet before the system can be placed on the market.[23] However, it also creates obligations for other actors in the AI supply chain, in particular by stipulating requirements that deployers must observe when putting into service or using AI systems.[24]

These requirements can be categorised in three sets. The first set obliges the provider to ensure that the system is designed in a way that mitigates risks. For example, a financial institution designing a credit scoring system[25] must ensure that the data it uses are sufficiently representative of the group of persons it covers,[26] and take into account contextual factors that might be relevant for its operation, such as geographical or behavioural attributes of the population assessed.[27] Providers must also incorporate safeguards in their technical designs, such as functionalities for automated logging[28] and human oversight.[29] Furthermore, they must ensure that the system is transparent enough for deployers to understand its outputs and how to use it.[30] Last but not least, providers must ensure that systems have appropriate levels of accuracy, robustness and

20 Art. 3(63).

21 Art. 3(65).

22 Art. 1(2)(c).

23 Art. 16(a).

24 Art. 26.

25 Point 5(b), Annex III.

26 Art. 10(3).

27 Art. 10(4).

28 Art. 12.

29 Art. 14.

30 Art. 13(1).

cybersecurity.[31] For instance, the credit scoring system mentioned above would need to show that its outputs are good enough to guide credit decisions, and that the results can stand up to changes in the data about the population, and also against potential cyberattacks that might manipulate one's score or extract sensitive information.

The second set of requirements establishes disclosure duties. Providers must draw up and update detailed technical documentation which enforcement authorities can use to assess the conformity of a system with legal requirements.[32] They must also supply the deployers of their system with instructions to use it.[33] In the case of the credit scoring system, this would involve, for instance, information about how to interpret the outputs and what safeguards to use when running the system. Providers of high-risk AI are also required to register themselves and their systems in an EU-wide database.[34]

Finally, the third set of requirements consists of behavioural obligations. Providers must adopt a system of quality management practices[35] including practices aimed at detecting and managing risks throughout the life cycle of the system.[36] Deployers must follow the instructions for use[37] and perform various other duties. In particular, some deployers must conduct a fundamental rights impact assessment before certain AI systems are used.[38] This obligation covers any high-risk system used by public bodies, and, *inter alia*, systems used to assess creditworthiness (including credit scores) and risk assessment and pricing systems for life and health insurance. In addition to these duties, providers and deployers must cooperate with one another and with enforcement authorities to detect and address AI-related risks.

---

31 Art. 15(1). This obligation applies not only at the moment of initial deployment but also during the entire life cycle of the system. That is, from its initial conception to its deactivation.

32 Art. 11.

33 Art. 13(2).

34 Art. 49.

35 Art. 17.

36 Art. 9.

37 Art. 26(1).

38 Art. 27.

2.2 The governance of general-purpose AI models

General-purpose AI models are governed by two cumulative layers of obligations for providers. For every general-purpose AI model, its provider must put in place a policy to comply with the law on copyright and related rights,[39] draw up technical documentation and keep it up to date,[40] make available information and documentation to providers who want to incorporate the model in their own systems[41] and make public a summary of the content used to train the model.[42] These obligations do not require any technical intervention in the model but are meant to ensure that actors which integrate the model in their products can discharge their own legal duties.[43]

Some models are deemed to pose systemic risk due to their technical sophistication and widespread impact on the EU market.[44] A model is considered a general-purpose AI model with systemic risk if it meets certain technical thresholds.[45] If it does, its provider is subject to additional rules which oblige it to identify and mitigate risks proactively.[46] In this way, providers contribute to the safe(r) incorporation of such models in other AI-based products. However, this approach has been criticised for creating heavy burdens for cutting-edge innovation (Draghi, 2024) and failing to capture relevant sources of risk stemming from AI (Hooker, 2024). Its effects therefore remain to be seen in practice.

3. Implications for financial supervision

One of the distinctive properties of the AI Act is its horizontality. It applies in all domains covered by EU law, with few exceptions.[47] Therefore, AI systems used by financial institutions and by the financial sector are covered by the Act. In particular, systems used to assess creditworthiness or credit scores and those

39 Art. 53(1)(c).

40 Art. 53(1)(a).

41 Art. 53(1)(b).

42 Art. 53(1)(d).

43 Recital 101.

44 Art. 3(65).

45 Art. 51.

46 Art. 55.

47 Art. 2.

used for risk assessments and pricing life and health insurance fall in the high-risk category.[48] This means that a decision to use AI in a financial context is often bound by AI-specific legal requirements, in addition to the usually applicable legal framework.

To a large extent, the AI Act incorporates its new requirements in existing procedures for financial supervision. For example, the monitoring duties that apply to deployers of high-risk AI systems are deemed fulfilled if the deployer complies with the existing internal governance requirements in relevant financial services law.[49] In addition, financial supervisory authorities are designated as the market surveillance authorities for high-risk AI systems directly connected with the provision of regulated financial services.[50] Financial supervisors therefore become enforcers of AI regulation, but they must themselves comply with the requirements of the Act when they use AI.

As AI enforcers, financial supervisory authorities are granted additional powers to deal with technology-specific issues. They can carry out joint investigations with other market surveillance authorities,[51] and request access to documentation and to data sets used during development,[52] and even to the system's source code.[53] If they detect any risks in the course of these investigations (e.g. as a result of reports by providers or deployers, or from complaints lodged by natural or legal persons),[54] the Act empowers the authorities to request corrective measures, restrict or remove market access,[55] or impose fines and other sanctions.[56]

Keeping in line with the dual ambition of the Act to foster the use of AI while safeguarding public values, it also obliges national authorities to adopt measures to support innovation. For instance, each member state is required to have at least one regulatory sandbox in operation by 2 August 2026,[57] in which

48 Point 5, Annex III.

49 Art. 26(5).

50 Art. 74(6).

51 Art. 74(11).

52 Art. 74(12).

53 Art. 74(13).

54 Art. 85.

55 Art. 79.

56 Art. 99.

57 Art. 57(1).

the competent authorities are required to supply providers and prospective providers with guidance on regulatory expectations[58] in a controlled environment in which systems can be tested before being put on the market, put into service or used.[59] In particular, these sandboxes facilitate the reuse of personal data for the development of AI systems in the public interest,[60] potentially favouring the construction of systems to support the operation of financial authorities. Therefore, financial supervisors will be actively involved in governing the sandbox while their own use of AI technologies might benefit from it.

4. Conclusions

The AI Act creates a series of legal frameworks targeted at AI systems and models. Many uses of AI in the financial sector – both by regulators and by regulated actors – are not subject to additional requirements. Nevertheless, some important uses of AI, such as credit scoring and some law enforcement applications, are singled out as posing a particularly high risk to fundamental rights and other public interests protected by law. Therefore, the AI Act is an additional regulatory layer to be considered both by financial institutions and financial supervisors.[61]

In order to carry out their duties in the age of AI, financial supervisory authorities need to develop additional capabilities. They need to foster technical competencies in AI, and the legal expertise required to navigate risks to fundamental rights that fall outside their traditional remit. Therefore, the AI Act is likely to have tangible operational implications for the authorities responsible for financial markets, especially at first. If properly wielded, however, these new competences will be powerful tools to address the specific impacts of technological change in the financial sector.

58 Art. 57(6).

59 Art. 57(5).

60 Art. 69.

61 In fact, various provisions in the Act specify that its compliance requirements should be integrated in existing requirements under EU financial services law rather than duplicating information. See, e.g, Art. 72.

References

Almada M., and Petit N. (2025). The EU AI Act: A medley of product safety and fundamental rights? *Common Market Law Review*. Issue 62(1) forthcoming.

Bakiner O. (2023). Pluralistic sociotechnical imaginaries in Artificial Intelligence (AI) law: The case of the European Union's AI Act. *Law, Innovation and Technology*. 15(2), 558–582. Available here.

Draghi M. (2024). The future of European competitiveness, Part A – A competitiveness strategy for Europe. *European Commission*. Available here.

Hooker S. (2024). On the Limitations of Compute Thresholds as a Governance Strategy. *arXiv*. Available here.

Mazzini G., and Scalzo S. (2022). The Proposal for the Artificial Intelligence Act: Considerations around Some Key Concepts. In C. Camardi (ed.), *La via europea per l'Intelligenza artificiale*. Cedam.

OECD. (2023). AI language models: Technological, socio-economic and policy considerations (DSTI/CDEP/AIGO(2022)1/FINAL). *Organisation for Economic Co-operation and Development*. Available here.

Passador M. L. (2025). AI in the Vault: AI Act's Impact on Financial Regulation. *Loyola University of Chicago Law Review*. Available here.

Publications Office
of the European Union

ISBN: 978-92-9466-637-6
doi: 10.2870/8600400
QN: QM-01-24-186-EN-N

Funded by
the European Union