An Introduction to Digital Data Law in the EU

Regulatory Framework and Future Perspectives

edited by

Cristina Schepisi, Valeria Capuano and Sarah Lattanzi

HANDBOOK

Giappichelli

An Introduction to Digital Data Law in the EU

Regulatory Framework and Future Perspectives


IUSTITIAM COLIMUS

An Introduction to Digital Data Law in the EU

Regulatory Framework and Future Perspectives

edited by

Cristina Schepisi, Valeria Capuano and Sarah Lattanzi

Giappichelli

VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it

ISBN/EAN 979-12-211-8296-5

This publication has been co-funded by the Erasmus + Programme of the European Union 'Jean Monnet Module' DIgital REvolution and the new European Union tools for services and markets (DI-RE) – Project: 101085366 – J_M MODULE PARTH – ERASMUS-JMO-2022-HEI-TCH-R-SCH.

Co-funded by the European Union

The European Commission's support for the production of this publication does not constitute and endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

G. Giappichelli Editore

Published November 2025

TABLE OF CONTENTS

Preface IX

Introductory Remarks: The Ongoing Revolution of the Digital Single Market 1

Part I
Data Protection and Fundamental Rights

The Protection and Free Movement of Personal Data in the EU: An Evolving Legal Framework
Anna Fiorentini 6

The Right to Be Forgotten
Daniela Messina 20

Data Governance Act, Data Act: Reuse and Altruism of Data Held by Public Administrations
Sabrina Tranquilli 31

The European Health Data Space: The New EHDS Regulation and its Interactions with the GDPR and the DGA
Federica Scialoia 42

The European Declaration on Digital Rights and Principles: Towards a Human-Centred Digital Constitutionalism
Patrizia De Pasquale 49

Part II
Data Regulation for Markets and Services

The Regulation of Digital Services in the European Union
Sarah K. Lattanzi 60

Digital Markets Act and Data
Valeria Capuano 77

The Artificial Intelligence Act: An Overview
Federico Ferri 96

Cloud Computing Services
Franco Trubiani 116

Online Content-Sharing Platforms and Copyright Protection in European Union Law
Francesco Trapani 128

Part III
Future Challenges for Digital Data Law

Blockchain and EU Law: Legal Tensions at the Intersections of Data Protection and Competition Law
Enza Cirone 143

The European Union and the Governance of the Metaverse: Competition Law, Sovereignty and Accountability in Virtual Worlds
Jonatán Cruz Ángeles 156

Linguistic Diversity and Multilingualism through the Analytical Lens of Conversational Agents
Silvia Domenica Zollo 170

Appendices 179

The Artificial Intelligence Act: An Overview

Federico Ferri [*]

SUMMARY: 1. Setting the Scene. – 2. Putting the Artificial Intelligence Act into Context: the Preparatory Works. – 3. First (General) Considerations on the Regulation. – 4. The Risk-Based Approach: Main Categories and Obligations. – 4.1. Unacceptable Risks. – 4.2. High Risks. – 4.3. Focus: General-Purpose AI Models and Systemic Risks. – 4.4. Lower Risks. – 5. The Governance System: Levels and Actors, Powers and Functions. – 5.1. The National Level. – 5.2. The Supranational Level. – 5.2.1. New Competent Bodies. – 5.2.2. The European Commission. – 5.3. Need for (Loyal) Cooperation. – 6. Beyond the Artificial Intelligence Act: the Framework Convention on Artificial Intelligence. – 7. After the Artificial Intelligence Act: Likely Issues and Main Questions.

1. Setting the Scene

When discussing Artificial Intelligence (hereinafter, AI) it must be borne in mind that interest in this topic has not emerged in the last few years. On the contrary, there are examples of anticipations of AI-related works even in the preceding decades and, perhaps, centuries. Seventeenth-century natural philosophers such as Descartes, Pascal, and Hobbes somehow pioneered this field, as they used to reflect on mechanical calculators. In the first half of the nineteenth century, Charles Babbage, an English mathematician, designed the "analytical engine", a proposed digital mechanical general-purpose computer. And who can forget the "Turing test" (or "imitation game") developed by Alan Turing in the mid-twentieth century to assess machines' ability to exhibit intelligent behavior equivalent to that of humans? Many other examples could be made.

Nowadays, as anyone knows, AI is no longer an imaginary vision; it is the very frontier towards which the world is moving. That of course determines numerous consequences at the global level.

The United Nations (UN) presented AI as a global issue (UN, Global Issues, Artificial Intelligence) and claimed that this sector brings with it lights and shadows: it could be more than a game-changer for sustainable development but also a root cause or a tool for severe human rights violations. It thus does not come as

[*] Assistant Professor of EU Law at Alma Mater Studiorum- University of Bologna.

a surprise if AI has become a key subject for policy, politics and geopolitics. As a matter of fact, the most influential States (and several Big Tech companies), especially in the face of the ongoing worldwide tensions, are in the middle of an "AI rush". For sure, this transition is having considerable legal implications (for a comprehensive overview, see M. ARTZT, N. LOELFING, S. HEMBT, O. BELITZ (eds), 2024).

Against this background, one crucial question concerning AI is whether – and, in the affirmative, to what extent – this subject should be regulated. Because of the incredible innovative potential of AI, many States preferred to adjust the scope of application of existing sectoral norms, instead of bringing about tailor-made legal regimes. Even the States that made the first move in regulating AI (the United States, for instance) avoided introducing many – or too detailed – rules.

With all this in mind, what about the legal approach of European Union (hereinafter Union or EU) towards AI? The answer is quite controversial. Bearing in mind that the Union is not a State, as opposed to many partners or competitors, the fact remains that this organisation is experiencing manifest gaps in terms of technical resources and economic investments, at least if confronted with some strategic countries, where AI is being much more developed (see, for instance, the European Court of Auditors' Special Report of 8 April 2024 on AI).

Due to these limits, the EU is responding to AI's call with its legal arsenal, thereby fostering the approach applied over the last decade to many other sectors that make up its digital space. This choice is not only aimed at increasing the probability of achieving a level playing field internally, that is to say, among the Member States; it also expresses the Union's intention to fill the aforementioned lacunas by acting as a sort of **global regulator**, in an attempt to force foreign companies to comply with strict obligations when operating in the **internal market**.

As a result, a dense and complex network of acts and provisions constitutes (and is evolving within) the legal framework of the **Digital Single Market**. Among the main pieces of legislation are those concretising the new EU data law and those epitomising the new framework for goods and services (all discussed in this volume).

And here comes Regulation (EU) 2024/1689, also known as "AI Act" (there are many works on this measure: see P. VOIGT, N. HULLEN, 2024; C.N. PEHLIVAN, N. FORGÓ, P. VALCKE (eds), 2024; L. COTINO HUESO, D.U. GALETTA, 2025; A. HUERGO LORA, G.M. DÍAZ GONZÁLEZ (eds), 2025; D. WENDT, J. WENDT (eds), 2025). The AI Act was adopted on 13 June 2024 and most of its provisions will be applicable from 2 August 2026.

This Regulation is a recent and cumbersome piece in a growing mosaic. It is also an example of a "blank state" EU law, since it aspires to govern a subject that has never been regulated before. But there is more. Neither the Treaty on the European Union (TEU) nor the Treaty on the Functioning of the European Union (TFEU) contain specific provisions on AI. Likewise, there is no AI-related right in the Charter of Fundamental Rights of the EU (Charter, *infra*).

Working on a Regulation on AI was a tough challenge, particularly if one considers that this is the first example of wide-ranging legal measure on AI in the world. For the EU, the AI Act is a real **testing ground**. Arguably, the EU's legal framework on AI, as well as the way it will be applied, implemented and enforced, will make a remarkable impact on multiple layers of the European integration process.

That inevitably raises many questions. To list but a few, how was the AI Act conceived? What is its scope? How did the EU's legislator deal with risks and opportunities stemming from AI? What are the main obligations provided for in the AI Act? Will the Member States enjoy any leeway after the entry into force of all the Regulation's provisions? Who does what to make the Regulation work? Are there any other legal initiatives on AI at the regional level in Europe? In an attempt to offer an overview of the key points of Regulation 2024/1689, the present chapter will address these questions.

2. Putting the Artificial Intelligence Act into Context: the Preparatory Works

The narrative of the Union's political institutions started to cover AI in the second half of the 2010s. In the first place, the EU's approach was rather nuanced and characterised by scattered statements and documents. Then, the European Commission began to deal with this subject more frequently and from broader perspectives. Two major phases emerge from the overall activity of the European Commission.

The first phase, steered by the "Juncker" Commission, produced the main preliminary steps. An initial strategy, entitled "Artificial Intelligence for Europe", was adopted in 2018 to encourage the acceptance of the transformative revolution inevitably brought by AI. A few months later, the Commission published a Coordinated Plan on Artificial Intelligence identifying joint actions to increase investment and cooperation, especially through the exchange of good practices. Importantly, the main outcome of the early stages of the EU's action was the progressive consolidation of an anthropocentric approach to AI, which was also supposed to be crucial for building trust in the transition. In particular, it is worth recalling the publication of the Ethical Guidelines for Trustworthy AI, drafted by a group of **high-level independent experts** appointed by the Commission itself.

The second phase was led by the (first) "von der Leyen" Commission and refers to the years 2019-2024. Since the beginning of this period, it was clear that the EU intended to address AI from a different angle; the idea was to prepare a tailor-made regulatory framework, as shown by some ambitious soft law acts. The turning point was the launch, in February 2020, of the Commission's White Paper on AI, aimed at laying the ground to the crafting of a new supranational legal framework to adequately address the risks and opportunities associated with the development of AI. It was believed that regulating trustworthy AI was a suitable

option to ensure the protection of all European citizens, to avoid the flourishing of many different national markets, and to strengthen the EU's industrial base.

After just one year, on 21 April 2021, the Commission tabled its proposal for a Regulation on AI (the Proposal, *infra*). Here, the Commission confirmed the EU's basic approach to AI that, by the way, also underpins the final version of the AI Act. Regulation 2024/1689 was adopted by the European Parliament and the Council of the EU (Council) three years later. This time-frame is not very long, having account of the different nature of these institutions and the complexities that such an ambitious legislative procedure was destined to experience. Just to make a couple of examples, Regulation (EU) 2016/679 on the protection and free movement personal data (GDPR) was adopted five years after the Commission's proposal, and the draft Regulation concerning the respect for private life and the protection of personal data in electronic communications has not yet been adopted even if it was proposed at the beginning of 2017.

That being said, it is now time to capture the main points of the Regulation from a bird's eye view.

3. First (General) Considerations on the Regulation

The **AI Act** is a **massive, groundbreaking Regulation**, comprising 180 Recitals, 13 Chapters, 113 Articles and 13 Annexes. It is considerably longer than the Proposal. In particular, it differs widely from the initial draft, although the broad logic is more or less the same.

Art. 3 sets out numerous definitions, starting with that of "AI system", which means «a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness 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». The rationale behind these semantic qualifications is fostering as much as possible the emergence of unitary concepts, to prevent Member States and the operators concerned from giving rise to an uneven framework. However, the European Commission issued guidelines on the AI system definition to explain the practical application of this legal concept. It also anticipated that, where necessary, this document will be updated in light of practical experiences, new questions and use cases that may arise.

Like the Proposal, the Regulation embodies a compromise between **preventing the fragmentation of the internal market** and **protecting fundamental rights and founding values**. In a nutshell, the AI Act is hybrid-nature tool, a product safety instrument characterised by a rigid *ex ante* risk-based regulation framework. This is also why the Commission, the European Parliament and the Council chose a double legal basis: Art. 114 TFEU, concerning harmonisation in the internal market, and Art. 16 TFEU, on the protection of personal data. The former is undoubtedly the center of gravity, but this does not mean the latter is irrelevant.

The goals of the Regulation confirm this circumstance. Art. 1 of the AI Act reaffirms that the very purpose of the measure is twofold: improving the functioning of the internal market and promoting the uptake of human-centric and trustworthy AI, while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter. Art. 1 evidently expresses the need to balance often competing priorities. In particular, the pronounced attention to the protection of fundamental rights, further emphasised in the European Declaration on Digital Rights and Principles for the Digital Decade (solemnly proclaimed in 2023 by The European Parliament, the Council and the Commission), is one of the most characterising features of the EU's approach to AI. As for this last point, two further considerations can be made.

The first is that, even if Art. 16 TFEU refers to personal data protection and creates a link with Art. 8 of the Charter, the AI Act purports to protect many other fundamental rights. Recital 48 is emblematic, as it mentions human dignity, respect for private and family life, protection of personal data, freedom of expression and information, freedom of assembly and of association, non-discrimination, education, consumer protection, workers' rights, the rights of persons with disabilities, gender equality, intellectual property rights, effective remedy and fair trial, defence and presumption of innocence, good administration, the rights of children, and the high level of environmental protection.

The second observation is that Recitals 1 and 2 go beyond the fundamental right dimension, as they openly mention the founding values of the Union, enshrined in Art. 2 TEU and constituting the "DNA" of the organisation. This clarification mirrors the Commission's approach in the AI Act draft. Indeed, the Proposal was literally "based" on EU values, and its first specific objective was ensuring compliance of AI systems placed on the Union market and used with existing law on fundamental rights and Union values. Therefore, the AI Act is to be seen as a striking manifestation of what has been called "European Digital Constitutionalism" (see, among others, O. POLLICINO, F. PAOLUCCI, 2025).

These remarks are helpful to understand how the Union exercised its competence on AI. There were no particular issues in demonstrating the respect of the principle of subsidiarity, given that the AI Act's objectives cannot be sufficiently achieved by the Member States and, having regard of Art. 5(3) TEU, will be better achieved by the EU, due to the scale and effects of the proposed action. Instead, the implementation of the principle of proportionality was a little more complex, keeping in mind that, according to Art. 5(4) TFEU, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties. Drawing from the Proposal, the AI Act introduces a regulatory framework for the AI applications that are deemed more dangerous *vis à vis* the interests to protect, with the possibility for all other AI applications to follow a code of conduct (this will be discussed in Section 4).

That leads to another preliminary aspect: the subject of the Regulation. It can be questioned whether the label "Artificial Intelligence Act" is entirely accurate

because the Regulation was not designed as an "all-around" measure. Besides providing for variable intensity obligations on the basis of **selected risk categories**, the AI Act mainly regulates activities which complement the placing on the market, the putting into service, and the use of AI systems. Plus, it does not touch upon certain **particularly sensitive or strategic areas**: for instance, where AI systems are linked to military, defence or national security purposes, or scientific research and development. On a side note, the Regulation does not affect practices prohibited under EU law, including those covered by competition law. All in all, different legal regimes may apply, with an alternation of stringent limits, relatively prescriptive obligations and voluntary schemes; the basic criteria for determining the applicable regime are essentially the type and degree of the risk to address.

The AI Act applies in the Union, as is normal. However, it does not take long to realise that the EU's legislator was inclined to project the essence of the Regulation abroad. As long as targeted AI models are marketed or put into service in the EU, Art. 2 subjects to the Regulation all providers. The same goes for providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union. These circumstances, coupled with the EU's manifest ambition to benefit from a "first-move advantage" worldwide, contribute to consolidating the theory of the AI Acts' "Brussels effect" (see more extensively C. SIEGMANN, M. ANDERLJUNG, 2022) or, to use another expression, its "aterritoriality" (L. FLORIDI, 2021). It is expected that this Regulation will stimulate changes in production systems outside the Union and that it will also influence the definition of legal and judicial patterns in third countries. This should particularly be due to the attractive potential of the EU's internal market, as it comprises hundreds of millions of consumers with significant spending power.

Overall, the architecture of the AI Act is built around the following key points: **banning AI practices that pose unacceptable risks; identifying high-risk applications; establishing related requirements and specific obligations for operators and vendors; introducing specific discipline for general purpose AI models (GPAI models), including those with systemic risk; outlining measures to support innovation, with particular reference to regulatory experimentation spaces; setting up a multilayered governance framework and monitoring system for post-market interventions**.

4. The Risk-Based Approach: Main Categories and Obligations

4.1. Unacceptable Risks

As anticipated in the precious Section, one of the main features of Regulation 2024/1689 is the risk-based approach. Since AI is at the root of incredible opportunities and, at the same time, can become a **source of systemic damage**, the EU's

legislator decided to centralise risk management in a rather incisive manner. This choice applies right from the stage of identifying the risks to be countered. This has been a trend in EU digital law for some time. Legislative acts such as Regulations (EU) 2022/2065 (Digital Services Act – DSA, v. *supra*) and 2022/1925 (Digital Markets Act – DMA, v. *supra*) are exemplary in this respect. In particular, this represents a notable change from a milestone of the digital single market, namely the GDPR. Against this background, the AI Act refers to several risk categories, keeping in mind that the concept of "risk", according to Art. 3(2) means «the combination of the probability of an occurrence of harm and the severity of that harm».

The first category encompasses **unacceptable risks** (Chapter II). The main reason behind this category can be inferred by Recital 46 of the AI Act and refers to the urgency to shield important Union public interests as recognised and protected by EU law. Considering the Regulation as a whole, also in the light of the preparatory works and the legislation most relevant to the AI Act, it is clear that this degree of risk is extremely sensitive because it is likely to affect the values of the Union, the effectiveness of the Union's fundamental rights protection system, and the main supranational security requirements. The category of unacceptable risks is evidently a consequence of the human-centric approach to AI, which has settled in EU law at least since the publication of the Ethical Guidelines on Trustworthy AI.

Art. 5 lists the unacceptable risks and **prohibits certain AI practices** accordingly, bearing in mind the general clause that excludes the lawfulness of any AI practice infringing other Union law. The main instances of prohibitions concerning the placing on the market, the putting into service or the use of AI systems can be summarised as follows: the deployment of subliminal, manipulative, or deceptive techniques aimed at distorting one or more persons' behavior to impair informed decision-making, and causing significant harm; the exploitation of individuals' vulnerabilities related to age, disability, or socio-economic circumstances to distort behavior, causing significant harm; the evaluation or classification of individuals or groups based on social behavior or personal traits, causing selected detrimental or unfavorable treatment (social scoring); the assessment of the risk related to individual criminal offenses solely based on profiling or personality traits, (unless this is used to augment human assessments based on objective, verifiable facts directly linked to criminal activity); the compilation of facial recognition databases by untargeted scraping of facial images from the internet or CCTV footage; inferring emotions in workplaces or educational institutions, except for medical or safety reasons; biometric categorisation systems designed to deduce or infer sensitive attributes, except labelling or filtering of lawfully acquired biometric datasets as well as categorising of biometric data in the area of law enforcement. In principle, also real-time remote biometric identification in publicly accessible spaces for law enforcement is prohibited; however, Art. 5 provides for numerous derogations and/or specifications.

Since prohibited practices represented one of the most debated issues during the legislative procedure, the application and enforcement of Art. 5 of the AI Act is supposed to be challenging. Hence, the European Commission published a set of guidelines on prohibited practices under the AI Act. The final goal is to increase legal certainty and the indications contained in the document are particularly detailed. Chiefly, the Commission strived to untangle the practices listed in Art. 5 by explaining their rationale and objective, the key concepts and contents, the scope of application, and the interplays with other Union law.

4.2. High Risks

The second category includes **"high-risk" AI systems** (Chapter III). This classification was elaborated taking into account the intended use of certain AI systems, **their relevance** in socio-economic sectors, and **their potential** to cause harm to health, security, fundamental rights, the environment, democracy and the rule of law.

Art. 6 of the Regulation clarifies that high-risk AI systems are, first of all, those used as a safety component or a product covered by EU harmonisation laws in Annex I (which lists 20 legislative acts) and required to undergo a third-party conformity assessment. Nevertheless, Art. 6 adds that further AI systems, referred to the numerous areas indicated in Annex III, are to be considered high-risk ones: permitted biometrics, critical infrastructure, educational and vocational training, workers' management and access to self-employment, access to and enjoyment of essential private services and essential public services and benefits, admissible law enforcement, migration, asylum and border control management, administration of justice and democratic processes. This presumption confirms the EU's intention to limit as much as possible the leeway of both Member States and operators concerned when it comes to the conceptualisation and construction of the risks to tackle.

The Regulation also provides for some detailed derogations, depending on the case. Besides that, it is important to recall that the Art. 7 of the AI Act gives the Commission the power to add or modify use-cases of high-risk; it can also downgrade a given AI system to a lower risk category. When taking such decisions, the Commission shall first carry out necessary assessments against the criteria put forward in Art. 7. In any event, the Commission understood that the rules concerning high-risk AI systems needed to be further elucidated. Therefore, it launched a consultation to collect practical examples, insights to clarify issues, and input on responsibilities along the AI value chain. This feedback shall serve to draft guidelines on classifying high-risk AI systems, and related requirements and obligations.

High-risk AI systems are not prohibited *per se*. However, they can only be placed on the Union market, put into service or used if they comply with certain mandatory conditions, provided that some flexibility is guaranteed with regard to operational decisions on how to ensure product compliance (Recital 46). Therefore, a thorough compliance assessment is required. Accordingly, the Regulation

establishes a multitude of requirements and obligations, especially at Arts. 8 to 27. Among the main constraints regarding this kind of AI systems are: establishing adequate risk management and mitigation systems throughout the high-risk AI system's lifecycle; conducting data governance, ensuring that training, validation and testing to achieve high-quality of the datasets that fuel the system; logging capabilities to ensure traceability of results; producing detailed documentation with all necessary information on the system; providing deployers with clear and adequate instructions to foster compliance requirements; ensuring appropriate human oversight measures; guaranteeing high level of robustness, cybersecurity and accuracy.

In this vein, Art. 27 prescribes the conduct a Fundamental Rights Impact Assessment (so called, FRIA) to be carried out by both public and private sector deployers, as they are in the best position to understand how the high-risk AI system will be used in practice; indeed, deployers have better chance to identify potential significant risks that may have not be foreseen in the development phase. The FRIA (see A. MONTALERO, 2024) is necessary in case of first use of the high-risk AI system. If, during the use of the system, the deployer considers that the main criteria to consider have changed or are no longer up to date, the Art. 27(2) requires the taking of the necessary steps to update the information. Needless to say, the FRIA's scope also includes the specific context where the AI system is to be used and the response strategies to put in place. Based on the AI Act, it is allowed to carry out a FRIA in conjunction with the data protection impact assessment required by Art. 35 of the GDPR.

The legal regime applicable to high-risk implies the fundamental role of certain companies. It is assumed that the operators targeted by relevant obligations will not only have to carry out compliance tests with respect to the standards established by the European standardisation bodies, but will also be called upon to strike, on an exclusive basis, a balance between the rights and/or the economic interests at stake.

4.3. Focus: General-Purpose AI Models and Systemic Risks

The high-risk category refers, at least to a certain extent, to the so-called **"general-purpose AI" (GPAI) models**. GPAI models constitute a new important content with respect to the Proposal.

Pursuant to Art. 3(63) of Regulation 2024/1689, a GPAI model is an AI model «that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market». Art. 3(66) defines general-purpose AI systems as AI systems that are based on general-purpose AI models and that have the capability to serve a variety of purposes, both for direct use and for integration in other AI systems. Recital 97 of the AI Act recognises the peculiar

nature of GPAI models; being essential components of AI systems, they do not constitute AI systems on their own.

GPAI systems **may be used as high-risk AI systems by themselves or be components of other high-risk AI systems**. Moreover, GPAI models are associated with a specific risk category, that is to say, "systemic risk". Art. 3(65) defines it as «a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain». Systemic risks include, but are not limited to, adverse effects of major accidents, disruptions of critical sectors and serious consequences to public health and safety, adverse effects on democratic processes, public and economic security, and the dissemination of illegal, false, or discriminatory content (Recital 110). Under Art. 51, an AI model shall be classified as a GPAI model with systemic risk if it has high impact capabilities evaluated on the basis of appropriate technical tools and methodologies; however, the Commission can make such a designation having regard to the criteria set out in Annex XIII (concerning technical documentation for providers of GPAI models to downstream providers that integrate the model into their AI system).

In order to ensure a fair **sharing of responsibilities along the AI value chain**, specific rules have been provided for GPAI models; the main ones are set forth in Chapter V of the AI Act. In particular, in light of Art. 53, providers of GPAI models must: draw up and update technical documentation, as well as information and documentation to supply to downstream providers that intend to integrate the GPAI model into their own AI systems; establish a policy to respect Union law on copyright and related rights; publish a sufficiently detailed summary about the content used for training the GPAI model.

Unless the GPAI model concerned is with systemic risk, these obligations do not apply to providers of AI models that are released under a free and open-source licence that allows for the access, usage, modification, and distribution of the model, and whose parameters are made publicly available. Art. 55 introduces additional obligations for providers of GPAI models with systemic risk: performing model evaluations in accordance with standardised protocols and tools reflecting the state-of-the-art, assessing and mitigating possible systemic risks; tracking, documenting and reporting without undue delay relevant information about serious incidents and possible corrective measures to address them; ensuring an adequate level of cybersecurity protection.

The obligations for providers of GPAI models entered into application on 2 August 2025, one year before the day the AI Act becomes applicable. Due to the complexity of this topic, in July 2025, a GPAI Code of Practice was published. The Code was drafted by independent experts in different fields. It constitutes an additional and voluntary tool to stimulate compliance with the AI Act's obligations on GPAI models. To make the Code more effective, Commission has

issued guidelines to clarify the scope of the obligations for providers of general-purpose AI models.

4.4. Lower Risks

The other risk categories include lower-risk AI systems. It is possible to distinguish between **limited and minimum-risk**. These two categories are dealt with in a less intrusive way by the EU's legislator, as they do not refer to alarming risk degrees with respect to the abovementioned interests to protect. So, based on the impact assessments carried out before the drafting of the Proposal, the proportionality principle was applied with the intent to reduce any burden for providers of these types of AI systems, thereby striving to stimulate innovation.

Examples of limited-risk systems are software that employs automatic artificial intelligence systems (such as chatbots) and those used to produce audio or video content and to identify emotions or detect biometric data without the intention of tracking the end user. These applications are subject to mere transparency and reporting obligations, especially to allow individuals to be aware that they are interacting with a machine and not a human being. Minimum-risk characterises the majority of AI applications, such as those used for machine translation, video games or spam filters. Given their nature, the AI Act does not establish restrictions or obligations for low-risk systems.

It can be said that the approach of the EU's legislator in the face of lower risk is mainly deferential. Recital 165 of the AI Act is particularly insightful from this point of view, as it points out that providers of AI systems that are not high-risk «should be encouraged to create codes of conduct». The aim of this recommendation is to foster the voluntary application of some or all of the mandatory requirements applicable to high-risk AI systems. It is also added that codes of conduct for lower-risk systems should be adapted to the intended purpose and the risk involved, also taking into account the available technical solutions and industry best practices.

5. The Governance System: Levels and Actors, Powers and Functions

5.1. The National Level

The overall governance system portraited in the AI Act has a **dual level**, **national and supranational**, with multiple actors involved.

Art. 70 of Regulation 2024/1689 requires Member States to establish or designate at least one notifying authority and one market surveillance authority. These bodies were designed to perform different functions. Under Art. 3(19) of the AI Act, notifying authorities are responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring. Differently, market surveillance

authorities basically carry out the activities indicated in Regulation (EU) 2019/1020, as can be inferred by Art. 3(26) of the AI Act.

Member States, in principle, can appoint any type of public entity in accordance with domestic law and with their organisational needs; they are also free to decide whether to create new *ad hoc* bodies or to entrust the relevant functions and responsibilities to existing independent authorities. The only few exceptions are indicated in Art. 74.

By virtue of Art. 70, it is clear that the bodies at hand must be in a position to exercise their powers independently, impartially and without bias. It is worth pointing out that these features are linked to the main objective of the AI Act, with an emphasis on the need to promote a high level of protection of fundamental rights, due to the likely impact that AI systems governed by the Regulation can have. Accordingly, it is necessary that national competent authorities own adequate technical, financial and human resources, and have infrastructure to fulfil their tasks effectively. The AI Act also provides for strict requirements in terms of personnel's knowledge and skills.

Moving to national authorities' attributions, one function is to provide guidance and advice on the implementation of the AI Act, especially in favour of SMEs. Market surveillance authorities are also tasked with taking measures in relation to all AI systems that present a risk in accordance with the Regulation. These authorities will thus be able to reach out to the operators concerned to ask for information, access documentation, request corrective action and withdrawal of the system from the market if it does not comply with the Regulation.

Based on Art. 85, the relevant market surveillance authorities are entitled to receive complaints from any natural or legal person having grounds to consider that one or more provisions of the Regulation have been breached. This is a remarkable outcome of the European Parliament's activity during the legislative procedure, and will hopefully complement the set of judicial and administrative remedies that concretise the right to an effective remedy laid down in Art. 47 of the Charter of Fundamental Rights.

A separate argument must be made for the adoption of effective, proportionate and dissuasive penalties or other enforcement measures (e.g., warnings and non-monetary measures) in case of infringements. According to Art. 99, Member States must lay down the baseline rules. These rules shall be notified to the European Commission, which is entitled to receive, on an annual basis, national reports on the administrative fines issued during each year. While there are no specifications as to the scope of potential non-pecuniary measures, thus leaving states free to lay down detailed rules, the Regulation is more ambivalent with respect to the conditions for authorities to impose administrative fines. On the one hand, Art. 99(9) allows the Member States, depending on their legal systems, to assign the power to impose fines to competent national courts or «other bodies».

Hence, national competent authorities set up or empowered to comply with the AI Act may be of relevance in this respect. As for pre-established limits to

sanctioning powers, Art. 99(7) requires taking due account of all the relevant circumstances of the specific situation and, where appropriate, of further criteria mentioned therein. The Regulation also provides for ceilings set on the basis of two alternative references: a predetermined amount or a percentage of the global annual turnover in the previous financial year. These would be, quantitatively, €35 million or 7% of turnover for violations concerning the application of prohibited AI systems; €15 million or 3% of turnover for violations of the obligations laid down in the Regulation; and, finally, €7.5 million or 1.5% of turnover for the communication of incorrect information.

In any event, sanctioning powers under the AI Act must be subject to the procedural safeguards provided by EU and national law, including the right to an effective judicial remedy and due process.

5.2. The Supranational Level

5.2.1. New Competent Bodies

Further innovative aspects can be grasped from an analysis of the provisions concerning the supranational level of the AI Act's governance system. The most evident fact, following a first reading of the Regulation, is the co-presence of several new bodies: Section I of Chapter VII mentions the AI Office (Art. 64), the **European Artificial Intelligence Board** (Board, Arts. 65 and 66), the **Advisory Forum** (Art. 67) and **the Scientific Panel of Independent Experts** (Scientific Panel, Art. 68).

It is interesting to note that only the Board was originally contemplated in the Proposal, although it had different features. Nor should it be forgotten that the AI Office, first mentioned by the European Parliament during the process, was the subject of subsequent interventions that modified its essential aspects.

It is also emphasised that the nature of these bodies is profoundly different. The AI Office was established within the European Commission, thereby expressing some sort of "Community" essence. In contrast, the Board is composed of one representative per Member State, thereby reflecting a typical feature of the intergovernmental dimension. The Advisory Forum and the Scientific Panel, instead, bring together representatives of categories of stakeholders and civil society, as well as qualified individuals: the composition of the former, which involves figures with different profiles, must ensure a balance between commercial and non-commercial interests, while the latter includes personalities with proven expertise and technical-scientific knowledge in the field of AI.

The functions exercised by these bodies are also different. It is true that all of them support the implementation and enforcement of the Regulation by providing assistance and advice. However, the scope of action of the Advisory Forum and the Scientific Panel is more circumscribed than that of the Board and, above all, the AI Office; specifically, the AI Office is presented as the cornerstone of the entire system.

There is, however, an obvious link between these bodies and the European Commission. The most striking case is that of the AI Office. Besides being part of the Commission, it is regulated by a Decision adopted by this institution even before the AI Act. This circumstance is peculiar and symptomatic of the Commission's powers in the framework of the Regulation's governance. As regards the Board, which also serves – to some extent – as a liaison point for the competent national authorities, it is chaired by one of the Member States' representatives. However, the AI Office attends the Board's meetings and acts as its secretary. The influence exercised by the Commission over the Advisory Forum and the Scientific Panel is more direct. It is, in fact, the Commission that appoints or selects the members of both bodies; when it comes to the Scientific Panel, the Commission is even empowered to establish it by means of an implementing act.

Against this background, the role played by the **European Data Protection Supervisor** (EDPS) should not be overlooked. The EDPS has been designated as the competent market surveillance authority for Union institutions, bodies, offices and agencies. It will monitor the application of the AI Act from this perspective and can exercise powers similar to those attributed to national supervisory authorities. Under Art. 85 of the AI Act, the EDPS can also take complaints from natural or legal persons, without prejudice to other possible administrative or judicial remedies, such as those referring to the jurisdiction of Court of the Justice. The EDPS can even impose administrative fines on Union institutions, bodies, offices and agencies. Art. 100 fine-tunes this power, specifying the conditions that must be met. Quite surprisingly, the mechanism provided by Art. 100 is slightly different from the one of Art. 99; the former only provides for the possibility of imposing pecuniary measures, and these fines are considerably lower compared to those referred to by the latter.

5.2.2. The European Commission

Regulation 2024/1689 stands out for the assignment to the European Commission of quite unusual powers. Essentially, the greater the risk raised by the AI model or system concerned, the more intense the powers that the Commission can deploy. This legislative technique confirms the consolidation of a trend, which has been fostered by other recent Regulations: indeed, under the DSA and the DMA the Commission can exercise significant powers against, respectively, very large online platforms (and search engines) and the gatekeepers.

In the first place, the AI Act enables the Commission to **adopt delegated and implementing acts**, in accordance with Arts. 290 and 291 TFEU. It can exercise these regulatory powers in a wide range of situations; in some cases, this regulatory power seems to be destined to impact sensitive contents of the Regulation.

The rationale behind the delegation of power is to make the management of high or systemic risks more efficient. The Commission can proceed after assessing specific conditions, sometimes predefined criteria. As stated above, the Commission may adopt delegated acts to amend Annex III of the Regulation, as established

by Arts. 6(6) and 7(1)(3); in this way, the Commission is at the front line when it comes to reshaping the categories of high-risk AI systems referred to in Art. 6(2). By delegated acts the Commission may also decide to review the conformity assessment of high-risk AI systems, updating conditions and procedures. Similar considerations apply to Art. 51's rules on GPAI models with systemic risk; for example, the Commission may review substantive criteria and indicators for the designation of such models, as well as the burdens that providers must meet for technical documentation and information to be provided.

In this vein, multiple provisions of the AI Act entrust the Commission with the power to adopt implementing acts. One example is Art. 41(1), on the elaboration, in certain circumstances, common specifications for requirements applicable to high-risk AI systems (Arts. 8-15). Pursuant to Art. 56, Commission's implementing acts may serve to approve the codes of practices, also in order to give them general validity within the Union. Where the codes have not been made available in due time, the Commission can adopt implementing acts to establish common rules on the implementation of the requirements for providers of GPAI models. Moreover, the Commission must craft the post-market monitoring plan for high-risk AI systems through an implementing act (Art. 72(3)).

In addition to the above, the Commission may exercise other important prerogatives. Among the main ones is deciding that a GPAI model should be classified as a systemic-risk one under Art. 51(1)(b). Based on Art. 46(5)-(6), the Commission can also establish whether or not national authorisation to market or put into service specific high-risk AI systems is justified for exceptional reasons concerning public safety or the protection of human life and health and the protection of the environment or major industrial and infrastructural assets. What is more, it is up to the Commission to trigger the so-called "Union safeguard procedure" (Art. 81), to decide in an autonomous way on the conformity of internal measures with the apex protection standards against the risks tackled by the AI Act.

Reference should also be made to the supervisory, investigative, enforcement and monitoring powers in relation to providers of GPAI models, which lie exclusively with the Commission. Arts. 88-94 confer the Commission the power – *inter alia* – to request documents and information, carry out investigations, and order the implementation of measures.

Finally, the Commission can impose fines. This power is regulated by Art. 101, and the Commission may exercise it if there has been an intentional or negligent breach of the Regulation's provisions applicable to providers of GPAI models. And even if the procedure provides for obvious guarantees in favour of the persons concerned, such as the right to be heard, the Commission's obligation to respect the principle of proportionality and the possibility that the Court of Justice may also review the merits of the decisions imposing fines, it should not be forgotten that Art. 101 sets quite high maximum thresholds: provided that any sanction must be effective and dissuasive, the Commission may require payments of up to 3% of the total annual worldwide turnover in the preceding business year or €15 million, whichever is higher.

It follows from the foregoing that the Commission's supervisory function partly goes beyond the direct or mediated sanctioning powers expressly provided for by the EU's founding Treaties: this refers especially to pecuniary sums that Member States may be forced to pay as a result of infringement procedures under Art. 260 TFEU, as well as Art. 279 *interim* measures, or fines imposed on undertakings in the framework of EU competition policy.

5.3. Need for (Loyal) Cooperation

The governance structure outlined above requires the actors involved to interact with each other and ensure a high level of cooperation. Specifically, two scenarios are worth dwelling on.

The first one refers to horizontal cooperation between different authorities in a given Member State (internal dimension). The potential allocation of supervisory powers to different authorities will entail the search for sound coordination patterns in order to ensure the effective and efficient enforcement of the Regulation at the national level.

The Court of Justice partly shed light on this issue in its recent ruling in the *Meta Platforms and Others* case (2023). In that case, it was complained that, within a single Member State, the antitrust authorities' interpretation of the GDPR provisions in order to find an infringement of competition law would have resulted in a potential encroachment on the competences of the privacy authorities. The Court recognised the possibility for the administrative authorities to exercise a shared (although not substitutive) competence, inferring a series of obligations directly from a structural principle of EU law, namely the principle of loyal cooperation, enshrined in Art. 4(3) TEU.

It seems fair to assume that this reasoning should apply to the relationships between a Member State's authorities expressly empowered to oversee the implementation of the AI Act. Loyal cooperation shall constitute a sort of "umbrella principle" to guarantee, on the one hand, the effective application of sectoral law and, on the other, the coherence of the protection system established by Regulation 2024/1689.

This conclusion can also be deduced from that Court's case law according to which the administrative authorities of the Member States must respect and assist each other in the performance of their tasks under the Treaties, take all necessary measures to ensure the fulfilment of the obligations arising from EU lar, and avoid taking any measure which could jeopardise the attainment of the objectives of the Union (see in particular the 2013 judgment, case *UPC Nederland BV*, point 59).

Since the AI Act does not exhaustively regulate this aspect, it is likely that the Court of Justice will be asked to add further clarifications – without prejudice to certain Member States' exclusive prerogatives in terms of internal organisation – to exclude, or at least mitigate, the risk of divergences between the various national authorities with regard to the control of the implementation of the Regulation.

The second scenario covers the cooperation between the national supervisory authorities of different Member States and the cooperation of these authorities with the competent EU bodies. The very aim is to guarantee the correct application of the Regulation everywhere and to draw up guidelines on AI, especially in relation to foundation and GPAI models. Some manifestations of this multi-layered cooperation are listed as follows.

A case in point is the situation regulated by Art. 74(11). This provision specifies that national market surveillance authorities and the Commission should be able to propose joint activities, including joint investigations, designed to promote compliance, identify non-compliance, raise awareness or provide guidance on specific categories of high-risk AI systems that are found to present a serious risk across two or more Member States. The AI Office is tasked with coordinating support for joint investigations. In addition, any market surveillance authority can request assistance from the AI Office if it is unable to conclude an investigation of a high-risk system because it cannot access certain information about the GPAI model on which the system under investigation is built. Furthermore, pursuant to Art. 79(3) of the Regulation, if the supervisory authority of a Member State considers that the infringement is not limited to its national territory but may have a transnational impact, it must inform the Commission and the other Member States of the results of the assessment conducted as well as the actions required to the operator concerned.

Despite these rules, the risk that the authorities of a single Member State claim competence, leading to fragmentation of enforcement and possibly conflicting decisions, is not negligible. Once again, it will be necessary for the authorities' initiatives to be based on the principle of loyal cooperation. The caselaw of the Court of Justice could also be of help in this case. Particularly important could be the requirements and modalities of cooperation already identified in the well-known 2021 *Facebook Ireland* judgment. On that occasion, in fact, the Luxembourg judges had confirmed the division of competences between the supervisory authorities of different Member States, emphasising the importance of effective (as expressly provided for in the GDPR) and – more importantly – sincere cooperation between them. With regard to Regulation 2024/1689, this approach is likely to be strengthened and further investigated in order to ensure consistent and homogeneous implementation of key rules as well as greater predictability for the operators involved in the provision and use of AI systems.

6. Beyond the Artificial Intelligence Act: The Framework Convention on Artificial Intelligence

Right after the adoption of Regulation 2024/1689, an additional instrument on AI was approved at the regional level: the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (the Convention),

signed within the framework of the Council of Europe (CoE), in Vilnius, in September 2024. The group of signatories includes non-members of the CoE too, and the Convention is potentially open to every State of the international Community (the state-of-the-art of signatures and ratifications is accessible on the website of the CoE).

Obviously, there is a **strong connection** between this Convention and the AI Act. Yet, some caveats must be made to better understand the synergies between both instruments.

The Convention has the typical features of a framework agreement. As specified in the Preamble, the Convention aspires to foster cooperation between its Parties and, where possible, with other States that share the same values. Moreover, the Parties agreed that the Convention might be supplemented by further instruments addressing specific issues about the activities within the lifecycle of AI systems. The framework character of the Convention is also visible in some provisions that may limit its scope of application and the strictness of multiple obligations.

Starting from the end of the text of the Convention, Art. 27 allows the Parties to apply international and regional mutually agreed-upon rules on the matters dealt with by the Convention, unless this results in failing to comply with its object and purpose. Of course, this also applies to EU Law obligations that Union Member States must respect in the field of AI.

Although under Art. 34, reservations to the Convention are basically prohibited, Art. 32 enables any State of the EU to specify the territory or territories to which the Convention shall apply; this choice can be made at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession. In addition, Art. 32 provides that any Party may, at a later date, by a declaration addressed to the Secretary General of the CoE, extend the application of the Convention to any other territory. However, in both cases, the State concerned can revoke any territorial selection concerning the application of the Convention; it is enough to notify the Secretary General.

This high degree of flexibility underpins the obligations laid down in the Convention. Substantially, the Parties agreed to adopt or maintain measures concerning general common principles that reflect, at least in part, those enshrined in the European Declaration on Digital Rights and Principles for the Digital Decade (see *supra*, Section 3): protecting, safeguarding or respecting – depending on the case – human rights, the integrity of democratic processes, the rule of law, human dignity and individual autonomy, transparency and oversight requirements, accountability and responsibility, equality and non-discrimination, privacy and personal data, reliability of AI systems. Similar considerations apply to the provision of accessible and effective remedies or to procedural safeguards. It goes without saying that the Convention does not add specific conditions to detail its generic obligations; this means that the Parties are likely to carve out significant operating spaces. The only (minor) exception is Art. 16, on risk and impact management. This provision puts forward some requirements to guide the Parties in the adoption of all necessary measures. Interestingly, it openly

refers to the need to consider, where necessary, the perspectives of relevant stakeholders; Art. 19 reinforces to a certain extent the duty to conduct public discussion and multistakeholder consultation.

The weakness of the Convention's obligations goes hand in hand with soft follow-up and enforcement schemes. The main body in this respect is the Conference of the Parties (CoP). The fact that Art. 23 simply refers to «representatives of the Parties» to explain how the CoP is composed suggests that the role of this body will mainly revolve around fostering cooperation, issuing recommendations, or facilitating the exchange of best practices. Indeed, the main oversight powers lay in the hands of the Parties (Art. 26), since the CoP was not empowered to issue binding decisions against any State – even as regards dispute settlement – except for restricting the participation to its works with respect to Parties that cease to be members of the CoE, as prescribed by Art. 23(8).

In conclusion, the Convention does not constitute a breakthrough in terms of rule-making, but it might pave the way for the definition of new and sufficiently accepted standards in Europe and in the relationships between EU Member States and third European and non-European countries.

7. After the Artificial Intelligence Act: Likely Issues and Main Questions

The AI Act is a revolutionary initiative, good or bad, at least from a theoretical perspective. At the time of writing, we are halfway through its implementation: the most important insights from the practice are expected to be visible after 2026.

However, it is not difficult to guess that the AI Act will represent a major **turning point** for the European integration process. Indeed, the way it will be **put into practice** will determine significant consequences on many constitutional layers of the EU legal order. Moreover (and not to mention the innovations and threats coming from outside the EU), the startup of the Regulation will depend on a number of subjects: the European Commission and national authorities, the Court of Justice and domestic judiciaries, the bodies representing relevant stakeholders and civil society organisations.

Put briefly, the AI Act is a new point of departure. AI runs fast, so for now the Regulation just answers some questions. Nevertheless, other questions remain, others change, and others rise. Will the AI Act keep pace with technical development? Will it be ancillary to the internal market, or will it hinder innovation? Will it succeed in protecting fundamental rights, or will it be counterproductive in this respect? Will the Commission produce secondary law to the point that the AI Act will end up encompassing different and fast-changing legal frameworks? How will the Court of Justice use EU law general principles to interpret the AI Act? How will the AI Act interact with sectoral pieces of legislation at the EU level? Will it influence the evolution of AI law in third countries, or will external factors influence its implementation? These and other questions are destined to keep the attention on the AI Act high.

References

ARTZT M., LOELFING N., HEMBT S., BELITZ O. (eds), *International Handbook of AI Law: A Guide to Understanding and Resolving the Legal Challenges of Artificial Intelligence*, Wolters-Kluwer, 2024.

COTINO HUESO L., GALETTA D.U., *The European Union Artificial Intelligence Act: A Systematic Commentary*, Napoli, Editoriale Scientifica, 2025.

HUERGO LORA A., DÍAZ GONZÁLEZ G.M. (eds), *The EU Regulation on Artificial Intelligence: a Commentary*, Milano, Wolters Kluwer – CEDAM, 2025.

PEHLIVAN C.N., FORGÓ N., VALCKE P. (eds), *The EU Artificial Intelligence (AI) Act: A Commentary*, Wolters Kluwer, 2024.

SMUHA N.A., YEUNG K., *The European Union's AI Act: Beyond Motherhood and Apple Pie?*, in SMUHA N.A. (ed.), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, Cambridge, Cambridge University Press, 2025, p. 228.

VOIGT P., HULLEN N., *The EU AI Act Answers to Frequently Asked Questions*, Berlin, Springer, 2024.

WENDT D., WENDT J. (eds), *New Artificial Intelligence Act: A Practitioner's Guide*, Nomos, 2025.