European Journal of Risk Regulation (2025), **16**, 63–75
doi:10.1017/err.2024.54

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

The AI Act from the Perspective of Administrative Law: Much Ado About Nothing?

Oriol Mir

Law Department, Pompeu Fabra University (UPF), Barcelona, Spain
E-mail: oriol.mir@upf.edu

Abstract

This paper examines the impact that the finally approved Artificial Intelligence Act (AIA) will have on European public authorities when developing, acquiring and using AI systems. It argues that, despite the initial disappointment that the Act may cause when approaching it from an administrative law perspective, and despite the fact that some of the solutions that have been finally chosen are questionable, it represents a remarkable step forward, duly addressing many of the problems raised in the literature in relation to the automation of administrative decisions and the use of AI systems by public authorities.

Keywords: adm-ADM; AIA; administrative law; public authorities

I. Introduction

The European Regulation on Artificial Intelligence (AI Act – AIA) has finally been published in the Official Journal of the European Union.[1] It is possibly the European secondary legislation that has generated the greatest expectation worldwide since the emergence of the European Economic Community in 1957, as it is the first binding regulation of general scope, in a large economic region, of a disruptive technology – or a set of technologies – that is destined to profoundly transform all productive sectors. The AIA has been several years in the making, it has been one of the most amended pieces of legislation in the history of the European Parliament,[2] and the marathon trialogues in December 2023 in which the final political agreement on its content was reached were broadcast and followed by many specialists as if they were a football match. Member States have also postponed their legislative initiatives in this area pending the adoption of the AIA, which is intended to establish the common regulatory framework across Europe. It is expected to unfold the well-known "Brussels effect"[3] and influence the regulation and practices of the

[1] 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, 12.7.2024).

[2] Javier Espinoza and Ian Johnston, "EU lawmakers agree tough measures over use of AI" *Financial Times* (London, 11 July 2023) <https://www.ft.com/content/da597e19-4d63-4d4d-b7d1-c3405302a1e3> accessed 8 June 2024. There is a very useful 681-page document comparing the Commission's April 2021 Proposal with the many changes suggested by the Council and the 771 amendments adopted by the European Parliament. It is available at: <https://www.kaizenner.eu/post/aiact-part3≥ accessed 8 June 2024.

[3] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).

software industry in other regions of the world, affecting a lucrative market and a huge quality data space of more than 450 million people.

The AIA applies to both the public and private sector, and many national and EU administrations have already begun to explore the use of artificial intelligence (AI) systems in many areas, eg for fraud detection, prediction of all types of risks, facial and object recognition, management of critical infrastructure, border control, preparation and automation of all types of decisions, interaction with citizens (chatbots, virtual assistants) or automatic translation of documents.[4]

This paper will examine the impact that the AIA will have on European public authorities when developing, acquiring and using AI systems. It will argue that, despite the initial disappointment that the Act may cause when approaching it from an administrative law perspective (section II), and despite the fact that some of the solutions that have been finally chosen are questionable, it represents a remarkable step forward, duly addressing many of the problems raised in the literature in relation to the automation of administrative decisions and the use of AI systems by public authorities (section III).

II. The initial disappointment when approaching the AIA from an administrative law perspective

After the high expectations generated by the media and the EU institutions themselves, it is quite possible that administrative lawyers approaching the text of the AIA for the first time may be disappointed.

The AIA does not adopt the usual administrative law approach, focused on public administrations, and does not contain a specific chapter on the use of AI systems by public authorities, comprehensively addressing the issues raised by such use and setting out in detail the rights of natural and legal persons affected by automated administrative action (section II.1). On the other hand, the obligations imposed by the AIA will affect only a quantitatively very small part of the automated systems used by public authorities (section II.2), and compliance with these obligations is subject to a *vacatio legis* that extends until 2030 (section II.3).

1. The approach of the AIA, based on product safety and data protection legislation

Although the AIA contains many provisions specifically applicable to public authorities, it does not contain a chapter dedicated to them, nor does it directly address many of the problematic issues that administrative law doctrine has identified in recent years, such as the legal basis required for automated administrative decision-making, the legal nature of the algorithms used by the public administration, the conditions required for external providers of AI systems, the use of such systems in the framework of administrative procedures and for the adoption of discretionary decisions, the difficulties of providing reasons for decisions derived from opaque machine learning systems, the human review of administrative decisions prior to judicial review, the effectiveness of such judicial review,

[4] On Member States' experiences see the reports by Gianluca Misuraca and Colin van Noordt, *Overview of the use and impact of AI in public services in the EU*, EUR 30255 EN (Publications Office of the European Union 2020), Luxembourg, doi:10.2760/039619, JRC120399; and Luca Tangi and others, *AI Watch. European Landscape on the Use of Artificial Intelligence by the Public Sector*, EUR 31088 EN (Publications Office of the European Union 2022), Luxembourg, doi:10.2760/39336, JRC129301. On the US federal agencies see David Freeman Engstrom and others, "Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies" [2020] Administrative Conference of the United States. On the EU Administration see Oriol Mir, "Algorithms, Automation and Administrative Procedure at EU Level" in Herwig C H Hofmann and Felix Pflücke (eds), *Governance of Automated Decision Making and EU Law* (OUP 2024) 69ff.

the right of access to algorithms and source code by interested parties and citizens in general, or the specific liability regime for damages caused by the use of such AI systems.[5] The AIA does not even contain a specific chapter dedicated to regulating these issues in relation to the Union's administration, as the European legislator could perfectly well have done under Article 298 of the Treaty on the Functioning of the European Union (TFEU).

The AIA also does not set out a full catalogue of rights of citizens and businesses with regard to the use of AI systems by public authorities. The recitals of the AIA place great emphasis on the need to protect individuals from the significant risks posed by AI. However, the AIA is nothing close to a *Bill of Rights* for citizens and businesses affected by AI systems used by the public and private sector. In fact, the very term "affected person" did not even appear in the articles of the Commission's Proposal, and only after the European Parliament's amendments have they been granted a few rights such as the right to obtain an explanation or to lodge a complaint (Articles 85 and 86 AIA, discussed further below).

Rather than adopting this administrative law approach, the AIA regulates AI systems from the perspective of *product safety* legislation: AI systems, regardless of whether they are used by the public or private sector, are conceived as products potentially dangerous to health, safety, the environment, fundamental rights, democracy and the rule of law (Article 1(1) AIA), whose regulation must be harmonised at EU level, under Article 114 TFEU, to ensure the proper functioning of the internal market and to avoid restrictive national rules preventing their free movement throughout the EU.

This explains that the AIA is based on the *risk level* that the different AI systems pose to these legally protected interests and that it is founded on the same premises and principles as the general and sectoral European product safety legislation, to which it refers:[6]

- *Self-regulation*: Specification of the substantive requirements imposed on high-risk systems by Articles 8 to 15 AIA by means of technical standards drawn up by the European standardisation bodies – CEN, CENELEC, ETSI – with the participation of civil society (Article 40 and Recital 121 AIA), and, only in the absence of such self-regulation, by means of common technical specifications drawn up by the Commission through implementing acts under Article 291 TFEU (Article 41 AIA[7]).
- *Presumption of conformity* with such requirements in case of compliance with these technical standards and common specifications (Articles 40(1) and 41(3) AIA).
- *Self-control*: Conformity assessment of compliance with these requirements by the companies that develop the systems themselves (in the case of most of the systems in Annex III referred to below) or by the external private entities that are usually responsible for assessing product safety ('notified bodies', regulated in Articles 28 et seq. AIA), without prior administrative authorisation (Articles 16(f), 43 and 46 AIA).
- Ex-post supervision of compliance with these requirements and other obligations under the AIA by the national *market surveillance authorities* provided for in Regulation (EU) 2019/1020 (Articles 70 and 74 AIA), and the usual coordination mechanisms

[5] See, with further references, Mir, "Algorithms" (n 4) 54ff; Cary Coglianese, "A Framework for Governmental Use of Machine Learning" (2020) Report for the Administrative Conference of the United States 50ff; Albert Sanchez-Graells, *Digital Technologies and Public Procurement* (OUP 2024); Simona Demková, *Automated Decision-Making and Effective Remedies* (Elgar 2023); and the different national reports published in CERIDAP volume 1/2023, drafted respectively by Franz Merli, Ivo Pilving, Jens-Peter Schneider/Franka Enderlein, Diana-Urania Galetta/Giulia Pinotti, Eduardo Gamero and Jane Reichel, on the few provisions on administrative automated decision-making that currently exist in Austrian, Estonian, German, Italian, Spanish and Swedish administrative law.

[6] See in more detail Mark McFadden, Kate Jones, Emily Taylor and Georgia Osborn, "Harmonising Artificial Intelligence" (2021) Oxford Commission on AI & Good Governance Working paper 2021.5.

[7] This provision refers to the examination procedure, with veto power for Member State representatives, in Art 5 of the Comitology Regulation (Regulation (EU) 187/2011).

between national and European authorities in case a product needs to be withdrawn from the market (Articles 72–84 AIA).
- Coordination with harmonised *sectoral safety legislation* for dangerous products – such as machines, toys, lifts, radio equipment, medical devices, motor vehicles of all types, etc. – which may incorporate AI systems or have AI systems as safety components (high-risk AI systems as referred to in Article 6(1) and Annex I AIA: Articles 8(2) and 102 to 109 AIA).

The other main pillar of the AIA is the *protection of personal data*. Article 16 TFEU is the second legal basis for the AIA, as it contains rules restricting the use of certain AI systems that process personal data, such as, in particular, those allowing remote biometric identification of natural persons. The AIA makes *constant references* to the three main European data protection acts, which remain fully in force (Article 2(7) AIA), and focuses mainly on the negative effects that AI systems may have on *natural* persons (virtually all use cases of the stand-alone high-risk systems in Annex III concern only natural persons, except for those contained in points 2 – critical infrastructure –, 6(b) and 6(c) – polygraphs and assessed evidence can also be used in connection with a crime committed by a legal person –, and 8(a) – administration of justice –).

Data protection authorities retain important competences in the supervision of AI systems, in particular with regard to those used by Union authorities and national law enforcement and judicial authorities, where they assume the central role of *market surveillance authorities* (Article 74(8), (9) and (10) AIA; see also Article 77 AIA). Article 74(9) AIA confers on the European Data Protection Supervisor (EDPS) the status of market surveillance authority over Union institutions, bodies, offices and agencies developing or using AI systems, and Article 100 AIA allows the EDPS to impose administrative fines of up to EUR 1.5 million on them in case of breach of its provisions.[8] The joint opinion of the EDPS and the European Data Protection Board (EDPB) on the Commission's Proposal also had a strong influence on the European Parliament's amendments aimed at the protection of individuals affected by AI systems.[9]

Once again, the protection of personal data thus emerges as the main vector for the protection of European citizens with regard to information technologies. As important as the protection of personal data is, and as effective and laudable as the work of the independent data protection authorities is, it remains a *tangential* and *indirect* vector. The fundamental right to data protection is primarily aimed at ensuring (only) the informational self-determination of citizens, and it completely ignores the legal protection that *legal persons* also deserve in their relations with public authorities and other subjects.

2. *The limited number of systems subject to the most publicised provisions of the AIA*

As the administrative lawyer delves deeper into the AIA and understands its complex architecture, it is also possible that he or she will be somewhat disappointed by the small number of systems subject to its most publicised provisions.

From the outset, the AIA only applies to *AI* systems, not to any automated system used by public authorities. The finally adopted definition of AI system (Article 3(1) AIA), coming from the OECD,[10] is still very broad and includes not only machine learning systems, but

[8] This is three times the annual amount of administrative fines that the EDPS can impose on them for breaches of data protection law under Art 66 of Regulation (EU) 2018/1725.

[9] EDPB-EDPS, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021.

[10] OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449, as amended on 8 November 2023. See OECD, "Explanatory memorandum on the updated OECD definition of an AI system" (2024) 8 OECD Artificial Intelligence Papers.

also advanced symbolic or knowledge-based systems (expert systems). However, Recital 12 states that this definition excludes "systems that are based on the rules defined solely by natural persons to automatically execute operations." In any case, it is necessary to await the Commission's clarification of the concept of AI system in the *guidelines on the practical implementation* of the AIA to be drawn up in the coming months (Article 96(1)(f) AIA).

The AIA's flagship measure, the *prohibition* of certain AI systems, concerns *only* the *eight* types of AI systems or practices listed in Article 5 of the AIA (twice as many as before the European Parliament's intervention). And some of them are subject to quite a few exceptions.[11] This is particularly the case for the controversial *real-time remote biometric identification systems* in publicly accessible spaces, the use of which is allowed in many cases (Article 3(41), (42) and (44), Article 5(1)(f), (2) and (3), and Recitals 17, 19 and 32–41 AIA).

At the same time, *high-risk* AI systems (Article 6 and Annexes I and III), to which almost all of the AIA is devoted, represent a *very small part* of the systems that exist or will be developed in the future. Not only that.

On the one hand, high-risk AI systems linked to motor vehicles in Section B of Annex I (motorbikes, cars, aircraft, trains, etc.) are in fact *excluded* from the scope of application of the AIA, being governed solely by their specific rules, as provided for in Articles 102 to 109 AIA for each of them. These provisions merely amend the various pieces of legislation governing them by stating that, when technical rules relating to AI systems which are safety components of such products are adopted under these pieces of legislation, (only) the requirements which Articles 8 to 15 AIA impose on high-risk AI systems "shall be taken into account."

On the other hand, Article 6(3) of the AIA has included the controversial "*additional layer*" of classification of high-risk stand-alone AI systems proposed by the Council and maintained by the European Parliament.[12] It states that an Annex III system "shall not be considered to be high-risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons." It goes on to clarify that this is also the case where the system does "*not materially influenc[e] the outcome of decision making*" and lists four conditions that must be met in isolation or in combination.[13] The application of this exception is no longer subject to administrative authorisation, as proposed by Parliament, but is left to the assessment of the system provider. In return, the provider is required to document the assessment and also to register the system in the database of high-risk systems under Article 71 AIA, which will be referred to later (Article 6(4) AIA).

The *other AI systems* (the vast majority), those which are not prohibited or classified as high risk, are *also subject* to the AIA, as is clear from Articles 1(2), 2(1) and 3(1) of the AIA.

However, such systems *only* have to *comply*, where applicable, with the (important) *transparency obligations of Article 50 AIA* (information on *interaction* with AI systems – eg a chatbot –, on the *artificial* nature of the generated content – eg *deepfakes* – or on the exposure to an *emotion recognition* or *biometric categorisation* system).

Otherwise, only the *voluntary codes of conduct* of Article 95 AIA will apply to them. These codes do not necessarily exist and are obviously not binding.

The AIA has therefore not finally incorporated the Article 4a suggested by the European Parliament to be added to the Commission's Proposal, which listed and minimally specified a number of *general principles* applicable to *all* AI systems, regardless of their dangerousness

[11] This is criticised by EDRi et al., "EU's AI Act fails to set gold standard for human rights," 3 April 2024 <https://edri.org/our-work/eu-ai-act-fails-to-set-gold-standard-for-human-rights/> accessed 8 June 2024.

[12] This is criticised by EDRi et al., "AI Act fails" (n 11).

[13] Recital 53 AIA provides many clarifying examples (systems for translation of documents, text and speech processing, detection of duplicate applications, improvement of drafting, detection of deviations from previous decisions, etc.). Art 6(5) AIA also provides that the Commission shall, within a maximum period of 18 months, provide guidelines on the practical implementation of this exception, together with an exhaustive list of practical examples of use cases of AI systems that are and are not high risk, in order to ensure adequate legal certainty.

(principles of human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, and social and environmental well-being). These principles and their brief description were very reasonable, but it is true that their practical implementation could give rise to doubts (even if Article 4a(2) indicated that they did not create "new obligations under this Regulation") and fuel all kinds of national restrictions on the free movement of any AI system.

The most important consequence of subjecting these systems, which do not merit a high risk rating, to the harmonised regulation of the AIA is precisely that they *cannot* be subject to *additional restrictions* by Member States. Member States may not subject their development to obligations restricting their *free movement* throughout the EU.[14] Therefore, in relation to this huge range of AI systems that exist and, above all, will be developed in the future, it is more important what the AIA does *not* say than what it says: by subjecting them only to voluntary codes of conduct, the AIA grants *complete freedom* to their development.

This "*regulatory shield*," designed not to hinder the development of AI in Europe, is arguably one of the most important effects of the AIA. It is paradoxical that the European legislator is accused of being over-regulatory when the AIA will serve, above all, to *prevent* the imposition of obligations on the providers of the vast majority of AI systems that will come onto the market.[15]

Finally, following the spectacular emergence of ChatGPT and its competitors at the end of 2022, the AIA has also incorporated some provisions applicable to *general-purpose AI models*. They are defined in Article 3(63) as those that display a significant generality and are capable of competently performing a wide range of distinct tasks. These provisions are found in Chapter V (Articles 51–56) and apply irrespective of the AI system into which the model is eventually incorporated, be it a general-purpose AI system (which can serve a variety of purposes, such as ChatGPT – Article 3(66) AIA) or a specific-purpose AI system. The AI system based on such a model must comply with the relevant rules of the AIA, depending on the risk it presents. The AIA imposes obligations only on *developers* ("providers") of general purpose AI models. While it cannot be excluded that public authorities will eventually develop such models,[16] it does not appear that they will do so very often, at least for the time being. Therefore, the following pages will not refer to Chapter V and will focus on the development and use of AI *systems* by public authorities.

3. The delayed entry into application of the AIA, which in the case of public authorities may be extended until 2030

Having noted the above, the administrative lawyer may also be disappointed that it will be a long time before the provisions of the AIA become fully applicable to the AI systems currently used by national and EU public authorities.

Except for banned systems, which can no longer be marketed and used in Europe as of 2 February 2025, all other systems benefit from a very generous *vacatio legis*, which runs until *2 August 2030* for high-risk systems aimed at public authorities in general, and until *31 December* of the same year for the crucial large-scale IT systems managed by the European

[14] See Recital 1 AIA.

[15] Member States may, however, impose additional obligations on public authorities *using* such systems (see section IV).

[16] A significant example is the ambitious and open source large language model being developed by the Spanish government for use by both the public and private sector <https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/transformacion-digital-y-funcion-publica/Paginas/2024/ia-inteligencia-artificial-estrategia-espana.aspx> accessed 8 June 2024.

agency *eu-LISA*, listed in Annex X. Moreover, this *vacatio legis* covers not only existing systems, but also those to be placed on the market or put into service before 2 August 2026 – public authorities in general – or 2 August 2027 – eu-LISA – (Art. 111(1) and (2) AIA).

This long and debatable adaptation period,[17] which is probably designed to allow for the amortisation of the substantial investments already made or committed by the various public authorities in AI systems (such investments have been very high, eg in the case of the large-scale systems managed by Eu-LISA),[18] is in any case stricter than for the *private sector*, where high-risk systems pre-existing or brought into service within this 24-month period only have to be adapted to the AIA when they are subject to significant changes in their design (Article 111(2) AIA).[19]

III. The great importance of the AIA for automated administrative decision making (adm-ADM) by European public authorities

Notwithstanding the above, a close examination reveals that the AIA will be of great importance for automated administrative decision-making ("adm-ADM"[20]) by European public authorities and their action in general. This is at least for the following reasons, which can only be briefly outlined here.

1. Prohibition of AI systems characteristic of authoritarian regimes

Although few in number, the systems prohibited by Article 5 AIA include practices currently common in the actions of police forces in authoritarian countries, such as the social assessment of citizens (*social scoring*, Article 5(1)(c) and Recital 31 AIA); *predictive policing* that determines the risk of a natural person committing a crime without being based on objective and verifiable facts directly linked to a criminal activity (Article 5(1)(d) and Recital 42 AIA, underlining its incompatibility with the presumption of innocence);[21] and systems that *massively scrap facial images* from the internet and surveillance cameras in order to identify natural persons through facial recognition (Article 5(1)(e) and Recital 43 AIA). The latter is a system that is also widely used by US and even European police forces.

As for the aforementioned *real-time remote biometric identification systems* in publicly accessible spaces, their exceptional use by police forces is subject to *many safeguards*, which do not exist in authoritarian regimes, and which must serve to avoid the feeling of mass surveillance that they may provoke in citizens. These include the need for the use to be permitted and duly regulated by national law, the need for a fundamental rights impact assessment and registration of the use of the system in the EU database to be carried out (Article 5(2) AIA),[22] and the need for each specific use to be authorised (*ex ante* or, in urgent cases, within 24 hours) by an independent judicial or administrative authority (Article 5(3) AIA). *Post* remote biometric identification systems are themselves classified as high-risk (Annex III, point 1(a), Article 3(43) and Recitals 17 and 95 AIA), and their use by police

[17] The eu-LISA *vacatio legis* is criticised by EDRi et al., "AI Act fails" (n 11).

[18] See Mir, "Algorithms" (n 4) 74.

[19] A comprehensive timeline of the gradual and very complex entry into force ("into application," as is usual in EU law) of the AIA can be found at <https://fpf.org/fpf-resources-on-the-eu-ai-act/> accessed 8 June 2024.

[20] Oriol Mir, "The Impact of the AI Act on Public Authorities and on Administrative Procedures" (2023) 4 CERIDAP 238, 239.

[21] Other cases of predictive policing concerning natural persons are qualified as high risk by point 6(d) of Annex III of the AIA.

[22] On this impact assessment and this registration see section III.4.

forces is also subject to prior or subsequent judicial or administrative authorisation, with some exceptions and additional conditions (Article 26(10) AIA).[23]

2. The importance of high-risk AI systems used by public authorities

It has been shown above that high-risk AI systems represent only a small part of those that exist and will exist in the market. Particularly narrow is the list of *stand-alone* AI systems, which are those that are not linked to any product and relate to the use cases listed in *Annex III*. These are the types of AI systems that are usually in mind when discussing the risks of algorithms, in particular the risks of opacity, bias and discrimination on the basis of gender, race, income level, etc.

It is the case, however, that the vast majority of systems included in this list affect only or mainly *public authorities* and are or may be of *great importance* to *them* and to the *persons affected* by their use. From the latter's point of view, which is the most obvious, such systems can have a decisive impact on their lives by affecting their basic subsistence conditions (determining their possibilities for migration and asylum, access to education, vocational training, employment, loans, life and health insurance, essential public services and benefits, or the availability of critical infrastructure) and other relevant fundamental rights such as liberty, protection of personal data, effective remedy or to vote and to stand as a candidate. Seen from the perspective of public authorities, such systems may also become essential for the pursuit of public interests and the protection of the (other) persons and legal interests entrusted to them.

It is therefore imperative that such high-risk systems are well regulated and supervised, and that they function flawlessly, without bias or error.

To ensure that this is the case, the AIA even provides for a detailed regulation of *regulatory sandboxes*, which allow for the testing of innovative high-risk systems such as those that may eventually be used by public authorities in their day-to-day work (Articles 57–59 AIA).[24] It even makes it possible to authorise tests in real world conditions *outside* these sandboxes, with the informed consent of the persons concerned or – in police matters and other areas of law enforcement – without the results having any negative effect on them (Articles 60-61 AIA).

The AI systems included in Annex III may, moreover, *increase* (or decrease) over time. In order to provide adequate flexibility in the regulation of a set of technologies that will evolve significantly in the coming years, Article 97 AIA empowers the Commission to adopt *delegated acts* under Article 290 TFEU to amend some of its provisions and many of its annexes, subject to scrutiny by the Council and the European Parliament. These include Annex III, whose use cases the Commission may reduce, amend or extend (only in the framework of the eight existing areas) in accordance with the substantive criteria set out in Article 7 AIA. It can also modify the conditions of application of the *exception* of Article 6(3) AIA discussed above (Article 6(6), (7) and (8) AIA).

3. The imposition of detailed conditions for the development of high-risk systems by public authorities and their contractors

In order to ensure the proper functioning of these high-risk systems, the AIA subjects them to numerous detailed *technical requirements* in Articles 8 to 15, which, as mentioned above, are to be further specified by the European standardisation bodies.

[23] Both the regulation of real-time and post remote biometric identification systems are criticised by EDRi et al., "AI Act fails" (n 11).

[24] See Sofia Ranchordas and Valeria Vinci, "Regulatory Sandboxes and Innovation-friendly Regulation: Between Collaboration and Capture" (2024) 1 Italian Journal of Public Law 107.

These requirements must be fulfilled by the public authorities themselves when they are the ones developing these systems and therefore have the status of *providers* of these systems. Not only that. The broad concept of "provider" in Article 3(3) AIA implies that public authorities acquire such status not only when they develop the systems through their own IT services, but also when they commission an external party to develop them *tailor-made*, either against payment (as would be the case for a contractor with whom a service contract[25] is concluded) or free of charge (eg a university or a public research centre). The latter is important because it means that the *contracting authority*, and not the contractor, is then responsible for the fulfilment of the many obligations imposed on providers. Public authorities will only occupy the other major role provided for in the AIA, that of users ("*deployers*," Article 3(4) AIA) of the system, when they simply acquire AI systems available on the market (through a supply contract[26]) or released under free and open-source licences (Article 2(12) AIA)[27] and use them when performing their duties.[28] The AIA thus solves a major problem that can arise in the procurement of AI systems by public authorities, and avoids dilution of respective responsibilities.

This is not the appropriate place to study these requirements in depth, and they do not present particularities when the system is developed by or for an Administration. The most important obligations imposed – somewhat softened with respect to the Commission's initial Proposal – are the following: to establish a *risk management* system (to assess and minimise the risks that the system may entail – Article 9 AIA –); to use *quality data sets* for the training, validation and testing of the system (Article 10 AIA); to prepare the mandatory *technical documentation* (Article 11 AIA); to configure the system so that it *automatically records* the events that occur during its operation ("logs," Article 12 AIA) and that it operates with a *sufficient level of transparency* in order to allow the deployers to appropriately interpret and use the output of the system (Article 13 AIA, requiring this transparency to be reflected in clear and detailed instructions for use); to design the system so that it can be effectively *overseen by humans* during operation (Article 14 AIA) and achieve an *adequate level of accuracy, robustness and cybersecurity* (Article 15 AIA).

In addition to ensuring that their high-risk systems comply with the above requirements, providers must also observe the numerous *additional obligations* specifically imposed on them by Articles 16 to 21 AIA. These include the obligations to have a *quality management* system (Article 17 AIA), to *keep documentation* (Article 18 AIA) and automatically generated *logs* under their control (Article 19 AIA), to carry out the above mentioned *conformity assessment*, to draw up an *EU declaration* of conformity (Article 47 AIA), to affix the *CE marking* on the system (Article 48 AIA), to take the necessary *corrective measures* and to *inform* the competent authorities and operators in case of malfunctioning of the system (Article 20 AIA).

Special mention should be made of the obligation imposed on them by Articles 16(i) and 49(1) AIA to *register* the AI system in the *database* of Article 71 AIA, a database managed centrally by the Commission, which will be publicly accessible, and which must contain the information detailed in Annex VIII. This is an important and widely demanded *transparency* measure, which concerns *only Annex III* high-risk systems (not Annex I), and which will allow the public to know the basic aspects of the independent high-risk systems in place in the Union. As mentioned above, providers are also required to register in this database

[25] Directive 2014/24/EU, Art 2(1)(9).

[26] Directive 2014/24/EU, Art 2(1)(8).

[27] Although Art 2(12) AIA begins by stating that "this Regulation does not apply to AI systems released under free and open-source licences," it immediately clarifies that they are subject to the rules on prohibited, high-risk and Art 50 systems. As has been seen, these rules constitute the core of the AIA regulation.

[28] In these cases, public authorities may also assume the role of provider when they substantially modify the purchased system or its purpose, or put their name or trademark on it, as provided for in Art 25 AIA.

those systems which, in their view, do not merit a high-risk status even though they fall within one of the Annex III areas.

The finally adopted version of the AIA has *reduced* the scope of such transparency by creating a *non-public section* of the database in which the systems of points 1, 6 and 7 of Annex III, in the areas of law enforcement, migration, asylum and border control (Article 49(4) AIA), will be registered.[29] This section will only be available for consultation by the Commission and the competent national (data protection) authorities, and contains less information than the public part of the database. Article 49(5) AIA has also ended up stating that the systems in *point 2* of Annex III shall be registered at *national* level and no longer in the European database, which makes sense given the national-territorial basis of the critical infrastructure concerned.

4. The imposition of detailed conditions for the use of high-risk systems by public authorities

Particularly important for the purposes of automated administrative action are the many obligations imposed on public authorities when they *use* high-risk systems and are therefore in the role of deployers. These obligations are set out in Articles 26 and 27 AIA and are particularly intense in the case of Annex III systems. Some of them are only or almost exclusively required of public authorities (Article 26(8) and (10), Article 27 AIA).

The obligations apply whenever a high-risk system is used, irrespective of whether this is done in the context of a *formalised administrative procedure* aimed at producing a decision having legal effects (e.g. granting, refusing or revoking social benefits – Annex III, point 5(a) – or granting or refusing an asylum, visa or residence permit application – point 7(c) –), or in the context of a *merely factual administrative action*[30] (eg when the dispatch of an ambulance or health care in the emergency department of a public hospital is refused – point 5(d) of Annex III – or the police are investigating a crime – point 6 –). In fact, the substantive approach of the AIA has the advantage that it is *not necessary to qualify* the type of administrative action in question, so that its provisions are applicable even if doubts may arise as to the legal or factual nature of that action (eg when a border control officer refuses entry to a foreign national).

On the other hand, the obligations of Articles 26 and 27 AIA must be observed both when the administrative action is *fully automated* and when it is *only partially automated*. As has been seen, the – correct – criterion used by the AIA (Article 6(3)) is that the AI system used *materially influences* the decisions referred to in Annex III, irrespective of whether they are taken by a human or a machine. This is crucial and deserves to be viewed positively, in view of the numerous studies confirming the tendency of humans to rely excessively on the results suggested by machines (*automation bias*).[31] By the way, Recital 61 states, in relation to the systems in point 8(a) of Annex III, that judicial decision-making "must remain a *human-driven activity*."

The examination of such obligations, which raise many issues of interest, deserves a specific paper.[32] Here they will only be listed and minimally commented upon following the typical sequence of administrative decision-making.

Before using for the *first time* an AI system listed in Annex III (except those relating to critical infrastructure), the public authority must carry out an *assessment of the impact* that its *use* may have on *fundamental rights* (Article 27 AIA). This obligation, widely called for as a

[29] This is criticised by EDRi et al., "AI Act fails" (n 11).

[30] *Realakte* or *actividad administrativa material* in German and Spanish administrative law.

[31] Art 14(4)(b) AIA expressly refers to this bias.

[32] In Mir, "Algorithms" (n 4) 61ff I suggested and justified including some of them (information to affected persons and the public, impact assessment) before the European Parliament approved the amendments that have led to their incorporation – with relevant changes – in the finally approved version of the AIA.

measure to prevent algorithmic discrimination, has been introduced at the request of the European Parliament, but with a *much reduced* scope compared to amendment 413 it adopted. In addition to greatly simplifying the content of the assessment to be carried out, the obligation to consult, for a period of six weeks, the competent authorities and representatives of persons or groups of persons likely to be affected by the system in question has been removed.[33]

Then, also *before* the *first use* of these same Annex III systems, public authorities (only public authorities) are obliged to *register* such *use* in the *European database* of Article 71 mentioned above (Article 26(8) AIA). This obligation also derives from the European Parliament's amendments, although it has again been watered down. It is still necessary to include in the database a summary of the conclusions of the fundamental rights impact assessment previously carried out, but no longer to describe the aspects relating to the use of the system as required by the Parliament. The publicity of the systems of points 1, 6 and 7 of Annex III is also restricted here, in the same terms as set out above in relation to the registration to be carried out by their providers.

During the use of any high-risk system, public authorities, like any other deployers, must use it in accordance with the instructions for use and inform the provider and the competent authority about episodes of malfunctioning (Article 26(1) and (5) AIA). They must also entrust the necessary *human oversight* of the system to natural persons who "have the necessary competence, training and authority" (Article 26(2) AIA), which is particularly important in the case of public authorities – which have significant shortcomings on this point – and links to the essential *AI literacy duty* imposed on them by Article 4 AIA. They must also ensure that the system's input *data* are "relevant and sufficiently representative," *keep* the *logs* generated automatically by the system for at least six months, and *inform workers* that they will be exposed to an AI system, where this is the case (Article 26(4), (6) and (7) AIA).

It is particularly relevant that the version finally approved has also incorporated the obligation proposed by the European Parliament to *inform* in general *natural persons exposed* to *Annex III* systems that take or assist in taking decisions affecting them (Article 26(11) AIA). Although Article 26(11), unlike the provision proposed by the Parliament, does not specify the information to be provided, Recital 93 does: such information should include the intended *purpose* of the system and the *type of decisions* it takes or assists in taking, as well as the right to obtain a more detailed *explanation*.[34]

The latter *right to explanation* is contained in Article 86 AIA, in the section on remedies, and has also been included at the request of the European Parliament. According to paragraph 1 of this provision, any person who is affected by a decision which produces *legal effects* or *significantly* affects that person in a similar way (by having an adverse impact on their health, safety or fundamental rights), and which is based on the output of any of the systems in *Annex III* (except, again, those relating to critical infrastructure), has the right to obtain from the deployer "*clear and meaningful explanations* about the role of the AI system in the decision-making procedure and the main elements of the decision taken."

Unlike the right to information, this right exists only in relation to *particularly important* individual decisions, similar to those which Article 22(1) of the General Data Protection Regulation (GDPR)[35] prohibits (with many exceptions) from being taken in a fully automated manner. However, the fact that both the right to information and the right to explanation are linked to individual decisions taken in relation to Annex III use cases will

[33] This is criticised by EDRi et al., "AI Act fails" (n 11).

[34] The reference that Art 26(11) AIA makes to Art 13 of Directive (EU) 2016/680 allows Member States to limit, delay or omit such information in order to protect criminal investigations and for the other purposes indicated in this Art 13(3).

[35] Regulation (EU) 2016/679. On Art 22 GDPR see the important Case C-634/21 *OQ v Land Hessen (Schufa)* [2023].

mean that both rights will *normally exist together*, since most such use cases have a significant impact, as seen above, on the health, safety or fundamental rights of persons. Unlike the right to information, the right to explanation is no longer limited to natural persons and also applies to *legal persons*.[36] Another important difference between the version of the provision proposed by the European Parliament and the version finally approved is that the latter no longer refers to the "right to request," but to the "right to *obtain*" the explanation. The nuance is important and implies that Article 86 AIA obliges to provide the corresponding explanations "*ex officio*," and not only when requested by the person exposed to the AI system.

Importantly, this right to explanation has to be related to the *duty to state reasons* for administrative decisions deriving from the fundamental right to good administration in Article 41(2)(c) of the Charter of Fundamental Rights of the EU (CFREU), from Article 296(2) TFEU and from the case law of the Court of Justice. When the public authority adopts a decision in one of the areas listed in Annex III, fully or partially automated, using an AI system, it will have to include in the obligatory statement of reasons for the decision a "*clear and meaningful explanation*" of the role that the AI system has played in that decision. This shall be the case whether or not the person concerned so requests.

The most relevant aspect of Article 86 AIA is, in general, that it presupposes that the high-risk AI systems used by deployers (in our case, public authorities) in the areas listed in Annex III *must be properly explainable*. This requirement, which already derives in general from Article 13 AIA – in particular from subparagraphs 3(b)(iv) and (vii) –, is very important and prevents or at least limits the use of *opaque* machine learning systems (known as "black box" systems), whose operation is not understood even by their own programmers, and which are the ones that have raised the most objections due to their lack of transparency.

Finally, Article 85 AIA, again introduced at the initiative of the European Parliament, recognises the *right of any natural or legal person to lodge a complaint* with the relevant market surveillance authority. This right is recognised "without prejudice to other administrative or judicial remedies," such as the administrative and judicial remedies available at national and EU level against administrative action. This right of complaint is thus conceived as a complementary means of monitoring compliance with the AIA, which can be used by persons other than those affected by the use of the system, and which seeks the control of such systems and not the legal protection of the latter. It should be stressed that the version of the AIA finally adopted has not extended the high-risk qualification to AI systems used in the resolution of *administrative appeals*, as Parliament intended by including them in point 8(a) of Annex III (amendments 71 and 738).

5. Other relevant issues

Other aspects of the AIA that will also exert a powerful influence on adm-ADM include the following:

- The *definition* of the key concepts in this matter (Article 3 AIA, with 68 points).
- The design of the *governance system* responsible for ensuring the proper functioning of AI systems and models, merging the control system for product safety with that of data protection, and adding new specialised bodies at EU level such as the new *European AI Office*, already created within the Commission[37] (and lacking the independence demanded by the European Parliament), the *European Artificial*

[36] The expression "any affected person" is still used in the final English version of Art 86, but Art 3 AIA no longer contains the definition of the term "affected person" proposed by the European Parliament, which limited it to natural persons only. In other language versions, this term is no longer even used in Art 86 (eg the Spanish version refers to "*toda persona*" – "any person").

[37] Commission Decision of 24 January 2024 establishing the European Artificial Intelligence Office C/2024/390.

Intelligence Board made up of representatives of the Member States, the *Advisory Forum* and the *Scientific panel of independent experts* (Chapter VII AIA).
- The establishment of *supervisory mechanisms* (Chapter IX AIA).
- The delimitation of the significant *penalties* that may be imposed in this matter, of up to EUR 35 million or, if the offender is an undertaking, 7 per cent of its total worldwide turnover for the previous financial year[38] (Chapter XII AIA).
- The great importance given to the *duty of confidentiality*, for the protection of both public and private interests (Articles 74(13) and 78 AIA, limiting access to the source code even vis-à-vis market surveillance authorities and thereby conditioning the application of European and national rules on access to public documents).

IV. Conclusion

As the preceding pages have shown, the AIA, despite what may appear at first glance, will have a *major impact* on administrative action in general and on automated administrative action in particular. It duly addresses – although some of the solutions it offers may be disputed[39] – many of the *problematic issues* that European and non-European administrative law scholarship has identified in relation to the use of AI systems by public authorities, such as the lack of knowledge of the systems they use, the quality of the data with which they train them, the risk of discrimination and errors, opacity, lack of transparency and explainability, the need for human oversight, automation bias, outsourcing of system development, protection of confidentiality, lack of technical qualification of public employees or the very definition of what is to be understood by AI.

The AIA's provisions on the use of AI systems by public authorities are not detailed and do not take an administrative law approach, but it does not seem that it could have gone much further within the *Union's competences*, at least in relation to national authorities. In any case, and this is very important, *the AIA does not prevent Member States* from subjecting the *use* of AI systems by their public authorities to *additional safeguards*, as I have argued in a previous paper[40] and as Article 26(3) AIA confirms. Member States (and their regional and local authorities) can increase – not reduce – the minimum safeguards required by the AIA and, eg: prohibit certain decisions to be taken in a fully automated way, the use of machine learning systems in cases where the law predetermines the criteria for the administrative decision, the use of systems that do not have a certain degree of reliability, or the use of AI systems in the framework of certain discretionary powers; subject the use of high-risk systems to more detailed impact assessments or explanations; extend the requirements of the AIA to the use of non-high-risk systems (such as the obligation to register such use in national or local databases); extend the guarantees of the AIA to *legal* persons affected by AI systems, etc.

The AIA, with a regulation duly conditioned by the principle of proportionality (Article 52(1) CDFUE), thus lays the foundations for the development of a robust market that offers the various public authorities innovative, reliable and secure AI systems, which can make a significant contribution to improving administrative performance and the lives of citizens.

[38] As is the case, for example, with the GDPR (Art 83(7)), Member States are free to decide whether or not to impose administrative fines on national authorities that infringe the provisions of the AIA (Art 99(8) AIA).

[39] Especially in the area of law enforcement and border control.

[40] Mir, "The Impact" (n 20) 246ff.

Cite this article: O Mir (2025). "The AI Act from the Perspective of Administrative Law: Much Ado About Nothing?" *European Journal of Risk Regulation* **16**, 63–75. https://doi.org/10.1017/err.2024.54