EJLT European Journal of Law and Technology

Fundamental Rights Impact Assessments in the EU's AI Act: A teleological and contextual analysis of the obligations of deployers

Eduardo Gill-Pedro*

Abstract:

This article examines the obligation for public-sector deployers to conduct Fundamental Rights Impact Assessments (FRIAs) under Article 27 of the EU Artificial Intelligence Act (AI Act). The article argues that the FRIA obligation functions as a minimum harmonisation standard, granting Member State authorities discretion to go beyond the AI Act's baseline and conduct more rigorous fundamental rights scrutiny prior to deployment. In contrast, the AI Act's obligations on providers of high-risk AI systems are fully harmonised, primarily structured around internal market objectives and designed to facilitate the free circulation of AI technologies across the EU. By drawing a distinction between these two regulatory logics, the article demonstrates that decisions by public authorities not to deploy AI, or to conduct broader or deeper FRIA impact assessments than required by Article 27, fall outside the scope of EU law. Drawing a parallel with free movement of goods caselaw, the article argues that such decisions are akin to 'selling arrangements'. Consequently, they are not subject to challenge under internal market or fundamental rights provisions of EU law by affected providers. The article concludes that the FRIA mechanism offers Member States a critical lever to secure fundamental rights and foster human-centric and trustworthy AI.

Keywords: AI; EU Law, AI Act, Fundamental Rights Impact Assessment, scope of EU law, harmonisation

* Faculty of Law, Lund University.

1. Introduction

The obligation to conduct a Fundamental Rights Impact Assessment (FRIA) was one of the most contentious elements in the legislative processes that gave rise to the AI Act.[1] It was not in the original proposal of the Commission, much to the consternation of civil society.[2] It was then introduced by an amendment proposed by the European Parliament, but this in turn was contested by the member states in the Council. Even after coming into force, the final version has been criticised for not requiring meaningful engagement with relevant stakeholders.[3] It has also been the subject of some debate about what the correct methodology for conducting such an assessment should be, with the general view in the scholarship seeming to be that there is unclarity about what a FRIA requires.[4]

This paper aims to provide greater clarity about the nature of the FRIA. Through a teleological and contextual analysis of the obligations that the AI Act places on deployers and providers, the paper will highlight the distinctive nature of the FRIA process as the primary tool available to the member states to ensure that the deployment of AI does not unduly undermine fundamental rights protections within their legal orders. The analysis proceeds in four steps:

The first step entails a textual analysis of the obligation of the deployer to conduct a FRIA, as set out in Article 27 of the AI Act. Deployers are one of the two key categories of operators regulated by the AI Act. A deployer is defined as a 'person, public authority, agency or other body using an AI system under its authority'.[5] This obligation will be compared with the obligations placed on providers[6] to assess the impact of AI systems on fundamental rights prior to placing the system on the market or into use. This textual analysis suggests that these obligations are similar in nature, and that, while Article 27 imposes an explicit FRIA requirement on deployers, other provisions appear to impose an implicit obligation to providers to conduct a process that appears very similar to a FRIA.

---

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (The AI Act) OJ L, 2024/1689 12.7.2024.
[2] See for example ECNL 'The EU AI Act must have a standardised methodology for impact assessments' 4 April 2022, <https://ecnl.org/news/eu-ai-act-must-have-standardised-methodology-impact-assessments> accessed 18 November 2025.
[3] European Disability Forum 'EU's AI Act fails to set gold standard for human rights', Statement of 3 April 2024 <http://edf-feph.org/publications/eus-ai-act-fails-to-set-gold-standard-for-human-rights/> accessed 18 November 2025..
[4] Alessandro Mantelero 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template' (2024) 54 *Computer Law & Security Review*,
[5] AI Act, Article 3(4)
[6] A provider is 'a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark'

The second step will explain how the objectives of the AI Act fit within the broader structure and objectives of EU law.

The third step will provide a teleological and contextual analysis of the two obligations. The central issue at stake is the extent to which EU law harmonises the obligations of providers and deployers.

The key finding in this section is that, whilst the AI Act fully harmonises the obligations of providers, and leaves very little room for member states to impose additional obligations on providers, in respect of the obligations on deployers to conduct a FRIA, the AI Act functions as an instrument of minimum harmonisation. Member states, and their public authorities, can conduct more extensive FRIAs than required by the AI Act, and can choose to conduct FRIAs even in situations where they are not required to do so by the AI Act.

The central argument in this paper is that the decision of a deployer not to deploy an AI system does not constitute a barrier to free movement. Rather, borrowing from the terminology of free movement of goods, this paper argues that decisions by deployers to conduct a FRIA should be seen as equivalent to a 'selling arrangement'.[7] Such 'selling arrangements' fall outside the scope of EU law, with the proviso that, if the deployer does decide to deploy the AI system, it must conduct a FRIA that complies with the minimum requirements set out in the AI Act. The implication of this finding is that public authorities in the member states play a crucial role in the governance structure of the AI Act. They retain a significant degree of competence in respect of decisions not to deploy AI so as to secure fundamental rights, as well as in respect of what assessments they consider necessary prior to deploying the AI system. In this way, the FRIA process can play a vital role in promoting human-centric and trustworthy AI. This means AI that does not lead to significant hollowing out of national democracies, nor to the undermining of fundamental rights and ultimately to the disempowerment of the human beings. However, in order for it to perform this role, the authorities, agencies and bodies that are required to conduct FRIAs need to understand their responsibilities and take them seriously.

2. Textual analysis of the obligations

2.1 The FRIA obligation of deployers

Article 27 requires that public authorities and private entities providing public services,[8] prior to deploying a high-risk AI system, perform an assessment of the impact on fundamental rights that the use of that system may produce.

[7] The term was introduced by the Court of Justice in C-267/91 and C-268/91 *Keck and Mithouard*, judgment of 24 November 1993, EU:C:1993:905.

[8] As well as private entities deploying AI systems intended to be used to evaluate the creditworthiness of natural persons, or AI systems intended to be used to assess risk and pricing in respect of health or life insurance. This article will focus on the role of public bodies.

This sentence requires some unpacking. First, this is an obligation that falls on *deployers* of AI systems – one of the two key categories of operators regulated by the AI Act. As set out above, the deployer is defined as a 'person, public authority, agency or other body using an AI system under its authority'.[9] The other key operator is the *provider*: the person 'that develops an AI system … or that has an AI system … developed and places it on the market or puts the AI system into service under its own name or trademark'.[10] Providers have very extensive obligations under the AI Act, but the FRIA obligation binds deployers.

Second, this obligation only arises in respect of the deployment of AI systems classified as high-risk. The AI Act does not regulate all AI – it adopts a risk-based approach[11] and classifies different applications at different risk levels – some are minimal or limited risk, and entail a very light regulatory burden. Others are considered to pose an unacceptable risk and are prohibited.[12] Applications that are designated as high-risk are allowed but entail extensive regulatory burdens for both providers and deployers.

The AI Act also regulates General Purpose AI systems (GPAIs). GPAIs are defined as AI systems 'trained with a large amount of data using self-supervision at scale, that display […] significant generality and [are] capable of competently performing a wide range of distinct tasks'.[13] Sections 2 and 3 of Chapter V of the AI Act, which govern GPAIs, impose additional obligations on providers of such systems. However, these provisions do not impose any obligations on deployers, so this article will not engage with the requirements for GPAI systems.

The FRIA obligation under Article 27 applies only in respect of certain types of high-risk systems, listed in Annex III of the Act. These are the systems that are used to make predictions or evaluations which will have an impact on human beings – AI systems used in settings such as hiring, admission to education, immigration decisions, law enforcement, biometric identification.[14] This explains why the obligation also extends to private actors engaged in the assessment of creditworthiness or life/health insurance pricing. These are all applications where an incorrect decision can significantly affect the life of an individual.

Third, and importantly, the obligation applies mostly in respect of public bodies, or private bodies providing public services.[15] The original amendment introducing the FRIA obligation, proposed by the European Parliament, covered all deployers of high-

[9] AI Act, Article 3(4)
[10] AI Act, Article 3(3)
[11] Martin Ebers, 'Truly Risk-based Regulation of Artificial Intelligence: How to Implement the EU's AI Act (2025) 16 *European Journal of Risk Regulation* 684.
[12] AI Act Article 5.
[13] AI Act Article 3(63). Large language models are typical examples of GPAIs.
[14] AI Act *Annex III*.
[15] With the addition of private bodies assessing creditworthiness or insurance pricing of individuals, as set out above.

risk AI systems, including all those in the private sector.[16] However, following the trialogue negotiations, this obligation was limited primary to public bodies. This obligation on public bodies to conduct FRIAs reflects the status of states as primary bearers of human rights duties.[17]

The AI Act stipulates the necessary elements that the FRIA must contain.[18] The deployer must describe the processes in which the system will be deployed, what the intended purpose(s) will be, when and how often the system will be used, who is likely to be affected by these processes and what specific risks of harm may arise through the use of the system. The deployer must further specify what measures for human oversight and for risk mitigation are to be taken. Once the assessment is conducted, the deployer shall notify the market surveillance authority of its results.[19]

2.2 Obligations of providers of high-risk AI

In order to clarify the nature and import of the FRIA obligation, I will contrast that obligation with the obligations of providers of high-risk AI. A provider who intends to place on the market or put into use an AI system referred to in Annex III, which, as we have discussed above, includes AI systems that potentially have significant impacts on the fundamental rights of individuals,[20] needs to comply with an extensive range of obligations set out in Sections 2 and 3 of Chapter III. However, if a provider assesses that its AI 'does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons' the system will be exempt from the high-risk obligations.[21] The provider needs to document that assessment.[22]

The implication of this provision is that a provider of a system that prima facie falls under the scope of Annex III needs to do an assessment of the impact that the system might have on fundamental rights. It is a fairly rudimentary assessment, but the obligation is there, and the assessment needs to be documented.

If, on the other hand, the provider considers that the system does pose a significant risk of harm to fundamental rights, then it needs to comply with the obligations set out in Sections 2 and 3 of Chapter III. These are very extensive obligations. Of

[16] Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), Amendment 413. This original proposal had

[17] See Article 1 of the European Convention on Human Rights that requires the state parties 'to secure to everyone in their jurisdiction the rights [in the Convention]. It is accepted that fundamental rights can have some horizontal application. This does not negate the primary responsibility on the state to secure human rights.

[18] These elements are set out in an exhaustive list in AI Act article 27(1)(a) to (f).

[19] AI Act Article 27(3)

[20] See footnote 6 above.

[21] AI Act Article 6(3).

[22] AI Act Article 6(4).

particular significance is the obligation, set out in Article 9, to put in place a risk management system.

The Risk Management System (RMS) must include 'the identification and analysis of the foreseeable risks to … fundamental rights' that the system might pose, both when used for its intended purpose and in conditions of reasonable foreseeable misuse.[23] This assessment of the potential risks to fundamental rights needs to be documented,[24] and provided with the instructions for use.[25] In addition, when the provider submits the technical documentation required for the conformity assessment, this assessment needs to be included.[26]

These are instances of what could be called 'implicit Fundamental Rights Impact Assessments' and, on a textual analysis of the relevant provisions of the AI Act they appear to be a very clear analogue of the explicit Fundamental Rights Impact Assessment set out in Article 27. If we consider the recitals of the respective provisions, we can see that there are striking similarities:

Recital 96	**Recital 95**
The aim of the fundamental rights impact assessment is for the deployer to identify the specific risks to the rights of individuals or groups of individuals likely to be affected, identify measures to be taken in the case of a materialisation of those risks.	This process should ensure that the provider identifies risks or adverse impacts and implements mitigation measures for the known and reasonably foreseeable risks of AI systems to … fundamental rights

Both procedures aim at the identification of risks to fundamental rights, and the implementation of measures that will mitigate against those risks. In the case of the RMS, the responsibility falls on the provider, and with the FRIA, the responsibility will be on the deployer. But in both cases, what is required is an assessment of the impact of the system on fundamental rights. Importantly, the obligation includes, in both cases, an obligation to document how the assessment was carried out, what risks were identified, if any, and what measures, if any, were taken to mitigate those risks.

Both providers and deployers have an obligation to monitor the continuous operation of high-risk operating systems and where necessary take action. For the deployer, Article 26(5) requires them to continuously monitor the operation of the high-risk AI system, and if they consider that there is a risk to health, safety, or fundamental rights, the deployer must notify the provider. For the provider the RMS must be 'a continuous iterative process planned and run throughout the entire lifecycle' of the

[23] AI Act Article 9(2)(a) and (b).
[24] AI Act Article 9(1).
[25] AI Act, Article 13(3)(b)(iii)
[26] AI Act, Article 11(1) and Annex IV, point 5

system[27], and Article 72(1) requires the provider to 'establish and document a post-market monitoring system'. There are therefore obligations on both deployers and providers not only to prospectively assess the potential impact of the AI system on fundamental rights, but to retrospectively assess the actual impact of the system when it is in use.

This comparison between the RMS requirements for providers and the Article 27 obligations for deployers might suggest that both impose equivalent duties: that the FRIA obligation and the obligations of providers of high-risk AI systems to assess and mitigate potential risks to fundamental rights are similar. However, in the following sections, I argue that these obligations are of a fundamentally different nature.

3. Contextual and teleological analysis of the obligations

In order to understand how the obligations in the AI Act are to be interpreted and applied, and why they differ, it is necessary to consider the objectives of the AI Act. The EU is what is called a 'purposive' polity.[28] It has objectives, which are set out in the Treaties,[29] and it has competence to act only where such action is necessary to achieve those objectives. This is called the principle of conferral: the member states confer competences on the EU in order to achieve certain objectives that the member states have in common, and the EU acts in order to achieve those objectives.[30] This also explains that other very important principle of EU law – the principle of sincere cooperation, under which the member states agree to 'assist each other in carrying out the tasks which flow from Treaties',[31] which are those necessary to achieve the objectives of the EU, and to refrain from any measure which 'could jeopardise the attainment of Union objectives'. [32]

Therefore, the obligations which the EU imposes on member states and others are necessarily connected to the achievement of EU objectives. As the Court put it in Opinion 2/13 the interpretation of all EU norms must be 'ensured within the framework of the structure and objectives of the EU'.[33] The interpretation of EU norms must be guided by the *telos* of the EU.[34]

---

[27] AI Act Article 9(2)
[28] G. Davies, 'Legitimacy and Purposive Competence' (2015) 21 *European Law Journal* 2-22.
[29] Article 3 Article 19 Treaty on European Union (Consolidated Version) [2016] OJ C202/1 (TEU).
[30] AI Act, Article 5(1) and (2) TEU
[31] AI Act, Article 4(3) TEU
[32] *Ibid.*
[33] Opinon 2/13 of 18 December 2014, EU:C:2014:2454, para 170.
[34] Koen Lenaerts and José Gutiérrez-Fons 'To say what the law of the EU is : methods of interpretation and the European Court of Justice' (2013) EUI Distinguished Lectures of the Academy - https://hdl.handle.net/1814/28339 . Pierre Pescatore, 'Les objectifs de la Communauté européenne comme principes d'interprétation dans la jurisprudence de la Cour de justice ', in Miscellanea W.J. Ganshof van der Meersch, vol. 2, (Bruylant 1972).

With that 'functional constitution' picture in mind,[35] we can consider the objectives of the AI Act.

3.1 The objectives of the AI Act

Article 1 of the Act sets out the purposes of the AI Act as follows:

- To improve the functioning of the internal market;
- To promote the uptake of human-centric and trustworthy AI;
- To ensure a high level of protection of […] fundamental rights.

3.1.1 The internal market objective

The primary legal basis of the AI Act[36] is Article 114 TFEU.[37] This is the primary market integration provision, and allows the EU legislator to introduce measures harmonising the laws of the member states in a particular field, in order to facilitate the functioning of the internal market. Where member state laws regulating AI at national level might undermine the functioning of the internal market, Article 114 allows the EU to harmonise those laws at the European level, so that there will be one uniform standard that economic operators need to comply with in respect of AI products and services.

The internal market objective has been a central aim of the EU since its inception. It is an area where the EU and the member states have shared competence.[38] This does not mean that both the EU and the member states have competence to regulate this area concurrently. The Member States only have competence 'to the extent that the Union has not exercised its competence.'[39] Once the EU has exercised its competence by introducing harmonising legislation, EU law 'occupies the field' and the member states no longer have competence in that area,[40] unless the EU legislation expressly allows that. As the EU has introduced the AI Act, in questions concerning AI safety, EU law now occupies the field, and member states' competence in this area is limited.

3.1.2 The industrial policy objective

The second objective listed in Article 1 is to promote the uptake of AI. As Recital 1 of the AI Act notes, the use of AI can provide key competitive advantages to both economic actors and to society at large. There has been a policy decision at both member state and EU level that the development and deployment of AI is to be encouraged.

---

[35] Turkuler Isiksel *Europe's Functional Constitution* (Oxford University Press 2016).
[36] AI Act, citation 1
[37] *Treaty on the Functioning of the European Union* (Consolidated Version) [2016] OJ C202/47.
[38] AI Act, Article 4(2)(a) TFEU
[39] AI Act, Article 2(2) TFEU
[40] C-5/94 *The Queen v Ministry of Agriculture, Fisheries and Food, ex parte: Hedley Lomas Ltd* [1996] EU:C:1996:205, para 18.

Industrial policy, and the promotion of the uptake of specific technologies, is not one of the express EU objectives specified in Article 3 TEU. Article 173 TFEU states that the Union and the member states should 'foster better exploitation of the industrial potential of innovation and technological development'. However, the EU only has coordinating and supporting competence in the field of industrial policy.[41] This means that in this area, it is the member states that are in the driving seat. The EU may take measures to support the member states, but this expressly excludes the possibility of harmonising measures. Therefore, member states are still free to pursue their own policies and establish their own priorities in this field.

The objective is not merely to promote the uptake of AI, but the promotion of the uptake of *human-centric and trustworthy AI*. The AI Act seeks to steer the development and use of AI in ways that reflect European values and fundamental rights. This is connected to the third objective.

3.1.3 The fundamental rights objective

The third objective is to ensure a high level of protection of health, safety and fundamental rights. This is expressed more as a condition, or limitation than as an objective. The AI Act was not introduced 'in order to protect fundamental rights'. The protection of fundamental rights, as such, is not listed as one of the aims of the EU in Article 3 TEU. Rather, Article 2 TEU stipulates that the union is founded on the values of respect for human rights. Article 6 TEU recognises the Charter as primary law of the EU, and the Charter itself states that the Union institutions and agencies are bound by the rights in the Charter in everything they do.[42] But both Article 6 and the Charter itself are quite clear that the Charter does not extend the competences of the EU in any way.[43] And in the exhaustive list of EU competencies set out in Title I of the TFEU, there is no mention of the protection of fundamental rights.

The conclusion that can be reached following this analysis, is, as Smuha notes, that:

> the creation of an internal market for the free circulation of AI and the promotion of its uptake is the [AI Act]'s primary aim, with the protection of fundamental rights and other values being something to keep in mind[44]

This priority of the interests of the internal market is also made evident in the regulatory architecture of the AI Act. The Act is modelled[45] on the so-called 'New

[41] AI Act, Article 6(b)
[42] AI Act, Article 51(1) CFR
[43] Article 6(1) Treaty on European Union, [2016] OJ C202/01 (TEU) and Article 51(1) Charter of Fundamental Rights of the European Union [2012] OJ C326/391 (CFR). For an analysis of the implications of these provisions see Daniel Augenstein 'Engaging the Fundamentals: On the Autonomous Substance of EU Fundamental Rights Law' (2013) 14 *German Law Journal* 1917
[44] Natalie Smuha *Algorithmic Rule by Law: How Algorithmic Regulation in the Public Sector Erodes the Rule of Law*. (Cambridge University Press 2024), p. 267.
[45] AI Act, Recital 9 and Recital 83.

Legislative Framework' – a framework that was specifically developed by the EU with the 'aim … to improve the internal market for goods'.[46]

3.2 The obligations of the providers

If we consider the obligation of providers under the AI Act framework with this context in mind, we can see that they are most closely linked to the internal market objectives. The internal market requires that products and services move freely within and between member states[47] – it requires the removal of anything that might hinder, directly or indirectly, actually or potentially, free movement.[48] Discrepancies between the member states with regard to the rules which providers have to comply with in order to market or put into service their products are clear barriers to free movement.[49] So there needs to be a uniform set of rules which providers can follow when determining whether their systems are in conformity with the AI Act.

3.2.1 The New Legislative Framework

The Act is modelled on the so-called 'New Legislative Framework', which, as already noted, was developed with the 'aim… to improve the internal market for goods'. A key element of the NLF is that it places the primary responsibility of ensuring compliance with the 'manufacturer'. In the context of the AI Act, the provider stands in for the 'manufacturer'. This equivalence between provider and manufacturer has been subject to criticism, as it does not take into account that 'the way downstream deployers use it and adapt it, may be as significant as how it is originally built'.[50] Nonetheless, under this framework, it is the provider that has the primary responsibility to ensure that the AI systems that are put into use are in conformity with the requirements of the Act.[51] In most cases that provider will be a private company.[52]

---

[46] European Commission 'The New Legislative Framework' , available at <https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en> accessed 18 November 2025.

[47] Article 26 Treaty on the Functioning of the European Union (TFEU) [2016] OJ C202/47.

[48] 8/74 *Procureur du Roi v Benoît and Gustave Dassonville* [1974] EU:C:1974:82; C-55/94 *Reinhard Gebhard v Consiglio dell'Ordine degli Avvocati e Procuratori di Milano* [1995] EU:C:1995:411.

[49] 120/78 *Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein (Cassis de Dijon)* [1979] EU:C:1979:42.

[50] Lillian Edwards 'Regulating AI in Europe: four problems and four solutions' (2022) *Expert Opinion for Ada Lovelace Institute* <https://www.adalovelaceinstitute.org/wp-content/uploads/2022/03/Expert-opinion-Lilian-Edwards-Regulating-AI-in-Europe.pdf| accessed 18 November 2025.

[51] In some situations, the conformity assessment procedure can require the involvement of a notified body (AI Act, Article 43(1)(b)). The notified body is usually a private body that is paid to check that the high-risk AI system conforms with the requirements of the Act (AI Act, Article 34).

[52] The AI Act defines 'provider' as a 'natural or legal person, public authority or agency'. However, private investment accounts for the majority of investment of AI' (European Parliament Report 'AI Investment: EU and Global Indicators' (2024) at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/760392/EPRS_ATA(2024)760392

This gives these companies significant responsibility; as well as a great deal of power. It is these companies who are responsible for designing and implementing the Risk Management System. The RMS must consist of 'appropriate' risk management measures, it must address risks that can be 'reasonably' mitigated, and it must ensure that the residual risk, after the mitigation measures, is 'acceptable'. These terms are vague and seem to leave a lot of discretion to the provider companies. As Smuha notes, the AI Act 'provides a high 'margin of appreciation' for the very actors that the Act is supposed to regulate'.[53]

3.2.2 Harmonised Standards

Under the AI Act, as is typical for all legislation under the NLF, the apparent discretion of the providers is constrained by the development of harmonised standards.[54] Under Article 40 of the AI Act, the Commission is required to issue standardisation requests. These are to cover all matters concerning obligations of providers of high risk systems and of general purpose AI systems.[55] These standards will be developed by standard-setting bodies.[56] These bodies are private entities within which 'large commercial stakeholders, possessing the required expertise and resources, play a disproportionately large role in providing input for harmonised standards'.[57]

The providers, in developing best practice in the design of Risk Management Systems and generally ensuring that their systems conform with the Act's requirements, can be expected to give sufficient weight to the objective of facilitating the internal market in AI systems. After all, as companies engaged in the provision of AI systems, their existence depends on being able to market and put into service AI systems, The standard-setting bodies have an explicit mandate to 'promote investment and innovation in AI as well as competitiveness and growth of the Union market'[58] and

EN.pdf; Complex AI systems are invariably developed by legal, not natural persons (United Kingdome Government 'AI sector study 2023' 23 October 2024), http://www.gov.uk/government/publications/artificial-intelligence-sector-study-2023/artificial-intelligence-sector-study-2023.

[53] Smuha 'Legal Safeguards', p. 272.

[54] AI Act, Article 40 and 43.

[55] General Purpose AI Models are defined (in AI Act, Article 2(66)) as AI systems 'trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks'. Providers of such models have a number of additional obligations under Chapter V of the AI Act.

[56] The European Commission has issued the first draft standardisation request within the framework of the AI Act, addressed to CEN and CENELEC (European Commission *Draft standardisation request to the European Standardisation Organisations in support of safe and trustworthy artificial intelligence*, 5 December 2022).

[57] Sybe de Vries, Olia Kanevskaia and Rik de Jager 'Internal Market 3.0: The Old "New Approach" for Harmonising AI Regulation' (2023) 8 *European Papers* 583-610, at p. 605. See also Marion Ho-Dac 'Considering Fundamental Rights in the European Standardisation of AI: Nonsense or Strategic Alliance ' in K Jakobs (ed) *Joint Proceedings EURAS and SIIT 2023*

[58] *Draft Standardisation request* Recital 13.

can similarly be expected to give sufficient weight to the interests of the internal market objective.

There is evidence that, more recently, the standard-setting bodies have been under considerable pressure to ensure that the requirements on providers are not unduly burdensome, and do not undermine the competitiveness of European tech companies. The EU Commission has called for 'an innovation-friendly rulebook'[59] and is driving a 'simplification agenda' aimed at reducing the regulatory burden on companies developing AI.[60]

Whilst both providers and the standard-setting bodies are required to ensure that AI systems placed in the market in the EU are safe and trustworthy, and respect fundamental rights, neither the AI companies nor the standard-setting bodies are likely to have the necessary expertise to address the fundamental rights implications of the AI systems.[61] Furthermore, it can be assumed that the companies that provide AI systems, both in their capacity as providers under the Act, and when participating in the making of standards within the standard-setting bodies, will be guided by their commercial objectives to provide AI systems.[62] Conversely, it cannot be assumed that these companies will have the necessary and sufficient incentives to ensure that the systems do not breach fundamental rights.[63] Fundamental rights concerns are likely to be seen as potential obstacles to the attainment of the company's commercial objectives, and the company might not be incentivised to care sufficiently about potential harmful impacts of their AI systems on fundamental rights, if they could benefit from externalising these costs.[64]

3.2.3 The role of the Market Surveillance Authority

The fact that both the AI providers, the notified bodies and the standard-setting bodies are all likely to give priority to the internal market objective and may not have the expertise or the incentive to ensure the protection of fundamental rights, might be remedied if the governance structure of the AI Act ensures sufficient oversight of

---

[59] Commissioner Henna Virkkunen (Tech Sovereignty, Security and Democracy), Press Release 16 September 2025, at https://digital-strategy.ec.europa.eu/en/news/commission-collects-feedback-simplify-rules-data-cybersecurity-and-artificial-intelligence-upcoming

[60] Call for Evidence 'Digital Package on Simplification' 16 September 2025, Ares(2025)7724296 - 16/09/2025

[61] de Vries 'Internal Market 3.0', (*supra,* n. 68) p, 602.

[62] All employees, directors and managers of the company will be required, by law, to act in the interests of that company (see generally, Eduardo Gill-Pedro 'Whose Freedom is it Anyway? The Fundamental Rights of Companies in EU Law' (2022) 18 *European Constitutional Law Review* 183-206).

[63] Agathe Balayn and Seda Gürses 'Beyond Debiasing: Regulating AI and its inequalities' Report for European Digital Rights, 2 September 2021. <https://edri.org/wp-content/uploads/2021/09/EDRi_Beyond-Debiasing-Report_Online.pdf> accessed at 18 November 2025.

[64] Bogdan Kulynych et al 'POTs: Protective Opitimisation Technologies' (2020) *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* <https://dl.acm.org/doi/10.1145/3351095.3372853> Accessed 18 November 2025.

the AI providers. The AI Act provides a power to the designated market surveillance authority of a Member State carry out an evaluation of an AI system that it considers presents a risk to the health, safety or fundamental rights of persons.[65] If the authority considers that there may be a risk to fundamental rights, it shall cooperate with the relevant authority protecting fundamental rights.[66] If the evaluation determines that the system does not comply with the requirements of the AI Act, the authority can require the operator to take immediate action to correct the matter, including requiring the operator to withdraw the AI system from the market.

This procedure is an important backstop to ensure that AI systems that have undergone the certification procedure do not cause serious harm to individuals. However, here too, the priority of the market objective is made apparent. AI systems that have been developed in accordance with harmonised standards or with common specifications enjoy a presumption of conformity,[67] and therefore the authority will bear the burden of rebutting this presumption. Even where this is not the case, a requirement by a national authority that a market operator withdraw a product or service from the market, or otherwise take additional corrective action, constitutes a clear interference in the free movement rights of that operator. In the language of free movement of goods, imposing additional requirements in respect of any of the criteria in Section 2 of Chapter III can be seen as imposing 'product requirements'. Such requirements are a *prima facie* breach of the free movement rights of the providers.[68] The providers' rights are directly effective,[69] which means that providers will be able to bring proceedings in the national court challenging such a measure, and ultimately it will be up to the Court of Justice to determine the extent of the powers of the national market surveillance authority under article 79 of the AI Act.[70]

As already noted, the AI Act has the primary objective of facilitating the functioning of the internal market. Adopting a teleological interpretation of the Act, is likely[71] that the Court will consider that Article 79 is a derogation from the general rule that operators should be free to market products bearing a CE mark. Whenever a member

[65] AI Act, Article 79.
[66] Under AI Act, Article 77.
[67] See AI Act, Article 40 and 41 respectively.
[68] The classic 'product requirements' case is 120/70 *Cassis de Dijon* (*supra*, n.49). See also C-470/93 *Verein gegen Unwesen in Handel und Gewerbe Köln e.V. v Mars* GmbH [1995] ECLI:EU:C:1995:224 and 16/83 *Karl Prantl* [1984] ECLI:EU:C:1984:101. For a discussion of these cases see C. Barnard *The Substantive Law of the EU* (7th edn. Oxford University Press 2022), p. 94.
[69] See *mutatis mutandis* C-288/08 *Kemikalieinspektionen v Nordiska Dental AB* [2009] EU:C:2009:718.
[70] See Regulation (EU) 2019/1020 *on market surveillance and compliance of products* OJ (2019) L-169/1, Article 18, as well as Article 19 *Treaty on European Union* (Consolidated Version) [2016] OJ C202/1 (TEU)
[71] The provision is not yet in force at the time of writing, so this section requires a degree of speculation on how the Court of Justice would ultimately interpret it. However, the Court's previous practice provides a good guide (Lenaerts and Gutiérrez-Fons 'To say what the law of the EU is', page 33 and cases cited therein.

state seeks to derogate from its free movement obligations, the court will interpret the derogation strictly and the burden will be on the member state to show that its actions were truly necessary and proportionate.[72] This burden applies even where the member state seeks to rely on fundamental rights considerations to justify the restriction on free movement.[73]

It should be noted that the operator will not only be able to rely on directly effective fundamental freedoms, but even fundamental rights. Article 16 of the Charter guarantees 'the freedom to conduct a business in accordance with Union law and national laws'. A company that has developed an AI system that has undergone a certification procedure has a *prima facie* legally enforceable right to place that system on the market.[74] Therefore national authorities, national courts and ultimately the Court of Justice are required to take account of the fundamental rights of the company when determining the lawfulness of a measure restricting the marketing of an AI system.

The market integration telos of the AI Act is further strengthened by the industrial policy objective, which, as set out above, is one of the objectives of the AI Act. While the EU does not have competence to harmonise national law *in order* to achieve industrial policy objectives, once it has demonstrated that EU legislation is necessary to facilitate the functioning of the internal market, it is open to the legislator to frame that legislation in a manner that also promotes other important objectives,[75] such as industrial policy. The industrial policy objective would also entail a stricter scrutiny of measures by the national authorities that might hinder 'innovation, deployment and the uptake of AI systems'.[76]

3.2.4 The market priority in the framing of providers' duties

The analysis of the legal provisions set out above show that the regulatory structure of the AI Act has a strong market bias. While the Act aims to 'ensure a high level of protection of fundamental rights' and to promote the uptake of 'human-centric and trustworthy' AI, the mechanisms that it puts in place seem more focused on ensuring the free movement and easy uptake of AI technology. It should be noted that the AI Act is an instrument for maximum harmonisation, which means that the EU standard

---

[72] C. Barnard 'Derogations, Justifications and the Four Freedoms: Is State Interest Really Protected?' In C. Barnard & O. Odud (Eds). *The Outer Limits of European Union Law* (Oxford University Press 2009) 273–306.

[73] C-438/05 *International Transport Workers' Federation and Finnish Seamen's Union v Viking Line ABP* [2007] EU:C:2007:772. See also Christian Joerges and Florian Rödl 'On De-formalisation in European Politics and Formalism in European Jurisprudence in Response to the "Social Deficit" of the European Integration Project' (2008) 4 *Hanse Law Review* 3, p. 14.

[74] Eduardo Gill-Pedro, 'Freedom to conduct business in EU law : freedom from interference or freedom from domination?' (2017) 9 *European Journal of Legal Studies* 103-134.

[75] See *mutatis mutandis* C-358/14 *Poland v Parliament and Council* [2016] EU:C:2016:323, para. 34.

[76] AI Act, Recital 3.

constitutes both a floor and a ceiling.[77] The ability of member states, or of democratic processes within member states, to demand a higher level of protection of fundamental rights from AI providers is very limited.[78]

3.3 The deployer's obligations to conduct a FRIA

While the textual analysis above indicated that the obligations of the providers and of the deployers appeared quite similar; in this section I will highlight how a contextual and teleological analysis reveals very important differences between these two sets of obligations.

3.3.1 The FRIA as a minimum obligation

In the previous section, I noted how, in respect of the obligation of providers, the AI Act is a maximum harmonisation instrument, which creates both a floor and a ceiling for the member states. Member states are precluded by the AI Act from requiring providers to comply with stricter requirements than those in the AI Act. When it comes to FRIA, I argue that this logic does not apply. While there is a clear obligation on member states to allow AI systems that conform with the AI Act to enter the domestic market, there is no obligation on deployers to deploy a high-risk AI system. However, if they do decide to deploy, they must conduct a FRIA prior to deploying it. The FRIA must enable the deployer to identify the potential risks to fundamental rights that the deployment might entail, as well as measures to be taken in case those risks materialise[79] - it must fulfil the minimum requirements of the AI Act. But, given that there is no obligation on the deployer to deploy, that deployer can conduct a more extensive assessment of the fundamental rights than required under the Act.

The conclusion that Article 27 provides for minimum harmonisation only, and that member state authorities have no obligation to deploy might appear to run counter to the text of Recital 1, which states that the Act prevents 'Member States from imposing restrictions on the … use of AI systems'. [80]

However, when viewed through the lens of the internal market objective, a deployer's decision not to adopt an AI system does not amount to a 'product requirement'. In the terminology of free movement law, it is better understood as a 'selling

[77] This is made clear in Recital 1, which states that the AI Act prevents 'member states from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation'.

[78] As Smuha notes, there is an important exception in Article 2(11) which allows member states the possibility of 'maintaining or introducing laws, regulations or administrative provisions which are more favourable to workers in terms of protecting their rights in respect of the use of AI systems by employers.'.

[79] AI Act, Recital 96

[80] On the hand, even a textual interpretation can suggest that the FRIA obligation is a minimum requirement. Recital 96 states that deployers 'could involve relevant stakeholders, including the representatives of groups of persons likely to be affected by the AI system'. This appears to leave open the possibility for deployers to conduct more extensive consultation prior to deploying.

arrangement': a measure that regulates how a product is used, not whether it can circulate freely.

3.3.2 Selling Arrangements

As every EU law student knows, the concept of selling arrangements was introduced by the Court of Justice in *Keck*.[81] In this case, the Court of Justice considered the question of what kind of national measures amounted to a restriction in free movement of goods, as prohibited by Article 34 TFEU. In previous caselaw, the Court had drawn the scope of this provision very widely, so that all measures which are 'capable of hindering, directly or indirectly, actually or potentially, intra-Community trade'[82] are measures that have equivalent effect to quantitative restrictions and as such are *prima facie* prohibited under Article 34 TFEU. As David Edwards, one of the judges that drafted the *Keck* decision, points out, under this definition it is difficult to conceive of a measure that a member state could introduce that would not be capable of hindering trade.[83] As Weatherill puts it, the broad interpretation of Article 36 TFEU 'dramatically confines the residual space allowed for national regulatory autonomy'.[84] In order to ensure that member states preserved a degree of control over the regulation of the market within their jurisdiction, the Court introduced, in *Keck*, the concept of 'selling arrangements'. As the Court put it:

> National provisions restricting or prohibiting certain selling arrangements [a restriction on free movement] so long as those provisions apply to all relevant traders operating within the national territory and so long as they affect in the same manner, in law and in fact, the marketing of domestic products and of those from other Member States.

The case introduced a distinction between on the one hand measures that concerned product requirements – such as rules concerning the product's ingredients or composition, or rules concerning its packaging – and on the other and measures that concerned how the product could be marketed or sold – such as rules concerning shop opening hours, or arrangements for how products could be promoted or displayed, or where they could be sold or used. The former are MEEQRs, but the latter will only be caught by Article 34 TFEU if they disadvantage products from other member states in relation to domestic products. As Weatherill notes,

---

[81] C-267/91 and C-268/91 *Criminal proceedings against Bernard Keck and Daniel Mithouard* [1993] EU:C:1993:905.
[82] 8/74 *Procureur du Roi v. Dassonville* [1974] EU:C:1974:82.
[83] David Edwards 'What Was Keck Really About?' In: Fabian Amtenbrink et al (eds) *The Internal Market and the Future of European Integration* (Cambridge University Press 2019), p. 166.
[84] Stephen Weatherill 'Surrendering the right to regulate' in Fabian Amtenbrink et al (eds) *The Internal Market and the Future of European Integration* (Cambridge University Press 2019), p. 119.

> Keck rejects EU free movement law as a basis for general review of regulatory choices made at state level even in the absence of evidence of hindrance to the interpenetration of national markets.

The question will be whether the decision by a public authority to either not deploy an AI system, or to conduct a more extensive FRIA prior to doing so, applies 'to all relevant traders operating within the national territory' equally, and they affect in the same manner, in law and in fact, the marketing of domestic products and of those from other member states. If there are no factors that show that the decision by the public authority is discriminatory, then it will not be considered a hindrance to the interpenetration of national markets by providers of AI systems established in other member states.

Of course, the decision will affect the market actors in that it will reduce market opportunities. But what the free movement rules are concerned with is 'equality of market access – what is often called the level playing field'.[85] The free movement rules do not have the objective of removing regulatory constraints per se, merely in order to facilitate 'the unhindered pursuit of commercial opportunities'.[86]

Subsequent cases narrowed the scope of the *Keck* exception by excluding from its ambit selling arrangements that restricted market access[87] to the extent that they 'involve universal bans or otherwise clearly restrict trade, for instance because they substantially affect consumer behaviour'.[88] Here too the decision to deploy falls outside the scope of the free movement rules, as it is a decision by an individual 'user' concerning whether or not to deploy AI in a specific context – it is not a measure that is likely to affect consumer behaviour, *it is* consumer behaviour. This conclusion may not hold if there is evidence that public authorities in a member state are coordinating deployment decisions in a way that partitions the market or has protectionist effects. This, however, will be a matter to be determined in the specific instance. Equating a public authority's decision to deploy or not deploy AI with a 'selling arrangement' has a key implication: such decisions would fall largely outside the scope of EU law. If the deployer falling under the scope of Article 27 choses to deploy a high-risk AI system, it must conduct a FRIA prior to doing so, and that FRIA must comply with the minimum

---

[85] Edwards 'What was *Keck*' (*supra*, n. 84). In a range of cases, the Court held that national measures 'likely to limit the total volume of sales in that Member State and, consequently, also to reduce the volume of sales of goods from other Member States' were not restrictions on free movement where they did 'not affect the marketing of products originating from other Member States more than it affects the marketing of products from the Member State in question' (C-71/02 *Herbert Karner Industrie-Auktionen GmbH v Troostwijk GmbH* [2004] EU:C:2004:181). See also C-441/04 *A-Punkt Schmuckhandels GmbH v Claudia Schmidt.*[2006] and C-190/20 *DocMorris NV v Apothekerkammer Nordrhein* [2021] EU:C:2021:609.

[86] Opinion of AG Tesauro in C-292/92 *Ruth Hünermund and others v Landesapothekerkammer Baden-Württemberg* [1993] EU:C:1993:863.

[87] C-110/05 *Commission v Italy (trailers)* [2009], EU:C:2009:66, C-142/05 *Åklagaren v Percy Mickelsson and Joakim Roos* [2009] EU:C:2009:336.

[88] Justin Lindeboom 'What *Keck and Mithouard* Actually Said – And Its Legacy' (2023) 8 *European Papers* 353-362, at p. 359.

requirements stipulated in the AI Act. On the other hand, if the deployer decides not to deploy an AI system, even if it might comply with the minimum FRIA requirements, or decides to conduct an assessment that goes beyond what a FRIA would require, or in situations where the AI Act would not require a FRIA, [89] such action will fall outside the scope of EU law.[90]

3.3.3 FRIAs as selling arrangements

To provide concrete examples: A local authority considers whether to deploy an AI-based spam filter to manage incoming email communications. Such a system would typically fall within the category of minimal-risk AI systems under the AI Act.[91] In such cases, there is no obligation under the AI Act for the deployer to conduct a Fundamental Rights Impact Assessment (FRIA). However, the authority notes that some individuals who contact it via email may be in vulnerable situations, including persons experiencing psychiatric illness, substance dependence, or have suicidal tendencies. The authority is concerned that the AI system could inadvertently filter out emails from such individuals, leading to potential infringements of their fundamental rights. Would the authority be precluded from voluntarily conducting a FRIA to assess and mitigate these risks, even though no FRIA is formally required under Article 27 of the AI Act?

Similarly, if a planning authority is considering deploying a high-risk AI system to assist in the preliminary evaluation of planning applications this will likely trigger a mandatory FRIA under Article 27. In fulfilling this obligation, the authority may wish to extend the scope of its FRIA to identify potential risks not only to natural persons (as required under Article 27(1)(d)), but also to legal persons (e.g., businesses submitting planning applications). Would such an extension of the FRIA beyond the strict scope of Article 27 be prohibited?

I suggest that in both cases the AI Act would not prevent the authority from conducting a FRIA. Member states have obligations to secure fundamental rights within their jurisdiction which precede, and are independent from, their obligations under EU law.[92] Where they take action to ensure a higher level of protection of fundamental rights, in situations where EU law permits this, such action will 'fall within the exercise of the powers retained by the member states'.[93]

---

[89] Alessandro Mantelero 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template' (2024) 54 *Computer Law & Security Review,* p. 17

[90] Joined cases C-609/17 and C-610/17 *TSN ry v Hyvinvointialan liitto ry and AKT ry v Satamaoperaattorit ry* [2019] EU:C:2019:981.

[91] The European Commission provide spam filters as an archetypal example of a minimal-risk application (Commission Press Release, *European Artificial Intelligence Act comes into force,* 1 August 2024 <https://ec.europa.eu/commission/presscorner/detail/ov/ip_24_4123>, accessed 18 November 2025).

[92] For example, obligations under Article 1 of the European Convention on Human Rights, as well as obligations under the member states' own constitutions.

[93] C-609/17 and C-610/17 *TSN and AKT* , para 52.

It is conceded that this conclusion might have negative implications for the functioning of the single market. It will be easier for providers if member states' public authorities are limited in their ability to conduct FRIAs prior to deploying high risk AI systems. But the same can be said for selling arrangements: traders in the single market would find it easier to exercise free movement of goods if member states were not allowed to restrict selling arrangements such as opening times or prohibitions of sale at a loss. Setting the scope of application of the internal market is a political question.[94] As Wetherill notes, in *Keck*

> The Court was anxious lest the scope of internal market law be drawn too broadly, thereby depriving national authorities of the competence to select forms of local market regulation which do not interfere with the process of market-building in the EU.[95]

I suggest that this anxiety is also warranted in the AI market. Determining that decisions by public authorities on whether or not to deploy an AI system fall under the scope of EU free movement law will entail a disproportionate interference in the regulatory autonomy of member states.

3.4 Implications of falling outside the scope of EU law

There are important implications to the conclusion that these actions fall outside the scope of EU law. The first is that a provider whose interests are affected by a decision of a deployer not to deploy their AI system will not be able to rely on EU law to challenge that decision. AI providers have no right to require that a public authority in a member state deploy their systems. Of course, an AI provider has an interest that a public authority deploys their system. But having an interest is not the same as having a legal right.[96] Swedish meat producers have an interest that people eat meat, but if a Swedish university decides to offer more vegetarian dishes in its restaurants, it does not need to consult the Swedish meat producer association. Recital 96 of the AI Act suggests that

> deployers of high-risk AI system, in particular when AI systems are used in the public sector, could involve relevant stakeholders, including the representatives of groups of persons likely to be affected by the AI system, independent experts, and civil society organisations

---

[94] As Bartl notes, it defines the scope of 'a specific pattern of political action', that of internal market rationality. (Marija Bartl, 'Internal market rationality, private law and the direction of the Union: resuscitating the market as the object of the political' (2015) 21 *European Law Journal* 572-598.

[95] Stephen Weatherill, *The Internal Market as a Legal Concept* (Oxford: Oxford Uni. Press, 2017), p. 70.

[96] Eduardo Gill-Pedro, 'Proportionality and the Human Rights of Companies Under the ECHR – Whose Interests are at Stake?' (2020) 89 *Nordic Journal of International Law* 327-342

This list of suggested stakeholders does not include representatives of providers of AI systems, because they are not the focus of the fundamental rights obligations of the putative deployer.

Connected to this conclusion is the finding that the provider's Article 16 rights will not be engaged by the decision not to deploy. As set out above, Article 16 guarantees 'the freedom to conduct business in accordance with Union law and national law and practice'. A lawful decision by a public authority that it will not deploy an AI system because it considers that this would breach its fundamental rights obligation is a part of the law of that member state. The freedom to conduct business does not give companies a right to do that which the national law does not allow.[97] Even if one could interpret Article 16 as guaranteeing a right to that which the law does not allow, the matter is outside the scope of EU law, therefore Article 16 is not applicable.[98]

Finally, where the member state is exercising its own retained powers, it need not consider the industrial policy objective expressed in the AI Act. As set out above, industrial policy is an area where the EU only has supporting competence, and where it has no competence to harmonise the laws of the member states. Whilst the EU legislator has the power to draft legislation in a way that furthers the EU industrial policy objective, the EU has no power to harmonise member states' measures that fall outside the scope of that legislation in order to achieve an industrial policy objective. Therefore, when a national public authority makes a decision on whether or not to deploy an AI system, it need not take into consideration the fact that deployment might further the EU industrial policy objective.

3.5 Standardising a FRIA methodology

Much of the literature on FRIA so far has emphasised the need to develop a predictable and replicable methodology to conduct impact assessments. Bertaina et al put forward a very concrete proposal for a quantitative methodology to conduct FRIAs.[99] Their proposed methodology includes a 'quantitative matrix', which will be used as 'an analytical tool intended to evaluate the potential impact of the AI system on the whole sphere of fundamental rights'. The ambition of the authors is to propose a 'common standard tool' that all deployers could rely on for assessing the impact of fundamental rights. It should be noted that the authors were analysing the version of the Act proposed by the European Parliament, that included a broader application of the FRIA obligation to private deployers. The authors emphasise that, when designing

[97] Eduardo Gill-Pedro, 'Freedom to conduct business in EU law : freedom from interference or freedom from domination?' (2017) 9 *European journal of legal studies* 103-134.
[98] See *mutatis mutandis*, Joined Cases C-446/12 to C-449/12 *W. P. Willems and Others v Burgemeester van Nuth and Others* [2015] EU:C:2015:238, para. 49.
[99] Samuele Bertaina et al 'Fundamental Rights and Artificial Intelligence Impact Assessment: a new quantitative methodology in the upcoming era of AI Act' (2024) *International Joint Conference on Neural Networks*,<https://ieeexplore.ieee.org/document/10650347> accessed 18 November 2025.

their framework 'specifically thought about private sector applications'. This may explain their emphasis on standardised procedures.

Janssen et al suggest a 'practical' FRIA framework with four phases that operate to systematically guide organizations through evaluating the fundamental rights implications of their AI systems.[100] On a similar vein, Skoric et al attempt 'to develop processes for AI impact assessment and detailed governance frameworks that enable meaningful and effective impact assessment methodologies for specific contexts'.[101] Others have gone further than proposing methodologies, and have 'identified rules and principles into a set of synthetic requirements to create an automated risk assessment methodology' which would allow 'the full automation of the conduct of fundamental rights impact assessments'.[102]

These are laudable ambitions, but there is a danger in seeking to develop common standards to conduct FRIAs. As Mantalero notes 'the variability of the impact of AI on fundamental rights cannot be captured in assessment standards'. While it may be desirable to 'outline key phases of the assessment' and 'define best practice' and suggest 'common approaches' to conducting FRIAs, these should not be inscribed in formal standards.[103]

It should be noted that the power of the Commission to make standardisation requests concern only the obligations of providers. Article 27(5) AI Act requires that the AI Office develop a template for a questionnaire. However, such a template is meant as tool 'to facilitate deployers in complying with their obligations' rather than a standard that they are required to follow to demonstrate compliance. There is danger if the process by which a public authority decides whether or not to deploy an AI system becomes juridified, depoliticised and subject to internal market rationality.

4. Conclusion

This paper puts forward two related arguments. First, the obligation which the AI Act imposes on deployers to conduct a FRIA is to be understood as a minimum requirement. Deployers are free to assess the potential impact on fundamental rights of AI systems even where this is not required under Article 27 or to conduct more extensive assessments than required by the AI Act. Second, the decision by a public

---

[100] Helen Janssen, Michelle Lee and Jatinder Singh 'Practical Fundamental Rights Impact Assessments' (2022) 30 *International Journal of Law and Information Technology* 200-232;
[101] Vanja Skoric, Giovanni Sileno and Senai Ghebreab, "Roles of Standardised Criteria in Assessing Societal Impact of AI," 2024 *IEEE Conference on Artificial Intelligence* <https://ieeexplore.ieee.org/document/10605413> accessed 18 November 2025.
[102] Lucilla Gatt et al. 'FRIA Implementation Model According to the AI Act' (2024) *IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering*, <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10796624> accessed 18 November 2025.
[103] Alessandro Mantelero The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template (2024) 54 *Computer Law & Security Review*

authority of whether or not to deploy an AI system to perform a particular task is a matter which should be considered the equivalent to a 'selling arrangement', and as such something which falls outside the scope of EU law, provided that the decision does not differentiate between imported and domestic AI systems, nor amount to a complete ban or prohibition of use of an AI system.

There are a number of implications that flow from these arguments. I highlighted two central ones. First, if the decision to deploy is not a matter that falls under the scope of EU law, then providers of AI systems do not have a right under EU law that an authority deploys an AI system. A decision by a public authority not to deploy an AI system is not open to challenge by a provider on the grounds that either its free movement rights or its fundamental rights have been breached. Second, if the obligation to conduct a FRIA is a minimum obligation, and member states may exercise retained powers to conduct more extensive FRIAs, then it will not be appropriate to attempt to create a standardised methodology for the conduct of a FRIA, except to the extent that this can serve a guide for compliance with the minimum requirements.

There is a strong political drive within the EU to 'channel the power of artificial intelligence'[104] coupled with a fear that the EU is losing in the race for 'digital sovereignty' against the United States and China.[105] This has led to calls for a reduction of the regulatory burdens on developers and deployers of AI systems, as well as to demand that AI systems be developed and deployed extensively within the EU member states, through the digitalisation of public services.[106] In its *recent AI Continent Action Plan*[107], the Commission has highlighted the role of the public sector as 'a leading strategic driver of the Apply AI Strategy'.

This political drive is not restricted to the EU institutions. The member states themselves are committed to an expansion in the use of AI in a range of sectors, including in the public sector. As the recently released report by the Swedish AI Commission puts, Sweden needs to make 'a deliberate effort to make the most of the opportunities offered by AI'.[108] This includes promoting the use of AI in the public sector, as there is, according to this Swedish AI Commission 'a strong need for the public sector as a whole to embrace and realise the development potential that AI

[104] Commission President von der Leyen *State of the Union Speech,* 15 September 2021 <https://ec.europa.eu/commission/presscorner/api/files/document/print/ov/speech_21_4701/ > accessed 18 November 2025.
[105] European Commission '2030 Digital Compass: the European way for the Digital Decade' (COM(2021) 118 final), at 3.3.
[106] *Ibid*, 3.4.
[107] Commission Communication 'Ai Continent Action Plan' of 9 April 2025 (COM(2025) 165 final)
[108] AI Kommissions Färdplan för AI' SOU 2025/15, 4 February 2025 <https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2025/02/sou-202512/> accessed 18 November 2025.

offers'[109] This attitude towards the development and deployment of AI technology is reflected in many other national policies on AI.[110]

Whilst these political goals may be understandable, they should not preclude proper consideration of the fundamental rights risks which deployment of AI systems in the public sector entails.[111] As noted above, the aim of the AI act is not merely to promote the uptake of any AI, but only of 'human-centric and trustworthy' AI.[112] The AI Act constrains the ability of member states to control the development and marketing of AI systems. The obligations of providers are harmonised by the AI Act, and member states, and public authorities within the member states, have little scope to modulate those obligations. The main tool open to public authorities to ensure that AI systems operating in its jurisdiction are truly human-centric and trustworthy, and does not breach fundamental rights, is the ability of those public authorities to determine whether or not to deploy an AI system in a particular context, assisted by the FRIA process.

A decision by a public authority, such as a university, a local authority or a court, to deploy AI is not a neutral, technocratic purchasing decision. AI can be seen not only as a form of technology, but as a specific ideology.[113] AI technologies embody a certain understanding of the world – it is a practice which reinforces certain assumptions about relations of power, about the validity of certain modes of understanding the world, and of the importance of certain interests over others.[114] Where a public body integrates an AI system into its decision making process, this will shape the way in which those decisions are made – it might amplify certain voices and perspectives, it might exclude certain forms of participation or inclusion.[115] The decision to adopt AI technology in the processes by which public authorities make decisions is a decision that can transform the nature of democracy in that political community.

The EU has harmonised the laws of the member states in respect of the development, marketing and use of AI systems. It has done this in order to facilitate the functioning of the digital single market, and to promote the use of trustworthy AI while ensuring a high level of protection of health, safety and fundamental rights. Doing so necessarily constrains the ability of member states to regulate the use of AI. However, the member states' public authorities retain the power to determine for themselves whether or not to deploy AI in specific contexts. To deprive them of that power, and

---

[109] *Ibid*.
[110] See *OECD National AI policies & strategies Live Repository*, <https://oecd.ai/en/dashboards/overview> accessed 18 November 2025.
[111] For a database of AI risks in a range of sectors and applications, see MIT's 'AI Risk Repository' <https://airisk.mit.edu/> accessed 18 November 2025.
[112] See 3.1 above.
[113] Jaron Lanier and E. Glen Weyl 'AI is an Ideology, not a Technology' *Wired,* 15 March 2020, <https://www.wired.com/story/opinion-ai-is-an-ideology-not-a-technology/> accessed 18 November 2025.
[114] Simon Lindgren *Critical Theory of AI* (Polity 2024).
[115] Kate Crawford *Atlas of AI* (Yale University Press 2021).

to make those decisions to deploy subject to internal market rationality would lead to the profound disempowerment of the political communities in the member states.