Triumph or Tragedy?
An Analytical Assessment of the EU Artificial Intelligence Act

Review Draft of 6 August 2026

Abstract

The Artificial Intelligence Act (AIA) of the European Union has been portrayed as a world-leading regulatory regime that will protect the public against the technological threats inherent in AI, and encourage adoption of beneficial applications. A great deal of analysis has been published since the law was proposed in 2021. This has continued following its passage in 2024, and the coming into force of the first of its provisions in 2025.

This contribution evaluates the AIA not as law, but as the underpinnings of the several separate regimes for different categories of applications that it establishes as interventions into complex socio-technical systems. The article applies an evaluation framework for regulatory regimes that provides a comprehensive view comprising 16 criteria for an efficacious scheme. This identifies ambiguities and exceptions that are likely to undermine attempts to achieve compliance, to reduce the incidence of negative impacts and implications, and to manage risks.

The framework brings a considerable degree of structure to the assessment of regime performance. Beyond the present analysis, it supports also the conduct of evaluations by other parties, and lays a firm foundation for empirical studies of regulatee behaviour and regulator activities as these gradually become feasible. The results of this and subsequent evaluations should assist in the emergence of some future scheme that will be more likely than the AIA to bring order to the current chaos of AI applications.

1. Introduction

In recent years, rapid adoption has been evident of several forms of Artificial Intelligence (AI) that appear to embody both significant benefits and significant threats. In an endeavour to placate widespread public concern about the threats, statutory intervention was developed by the European Commission (EC) in the form of the Artificial Intelligence Act (AIA)[1]. This was enacted in 2024, with its provisions coming into effect in a series of steps. The legislation is widely seen as being highly influential in all jurisdictions in which AI is being actively developed and applied.

The majority of commentary on the AIA has been positive, or at least hopeful, with relatively few works critically examining the proposal or the political economy of its development, passage and implementation. The present paper is offered as a timely, sceptical, and moderately deep assessment of the AIA, its effectiveness in achieving its claimed purposes, and the political realities that undermine it.

Artificial Intelligence technologies are widely acknowledged to have substantial negative impacts and implications and to carry risks[2],[3],[4]. Reflecting the extent and seriousness of

1 European Union, 'Regulation on harmonised rules on artificial intelligence' (EU) 2024/1689, August 2024, at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

2 Tais Fernanda Blauth, Oskar Josef Gstrein and Andrej Zwitter, 'Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI' [2022] *IEEE Access* 10, 77110-77122 <https://doi.org/10.1109/access.2022.3191790>.

3 Roger Clarke, 'Why the world wants controls over Artificial Intelligence' (2019) 35(4) *Computer Law & Security Review* 423-433 <https://doi.org/10.1016/j.clsr.2019.04.006>.

4 Roger Clarke, 'Principles for the responsible application of Generative AI' (2025) 57 *Computer Law & Security Review* 106131 <https://doi.org/10.1016/j.clsr.2025.106131>.

the threats, widespread concern exists about AI's impacts, and there is demand worldwide for regulatory action[5]. The AIA is claimed to be the first substantive endeavour to regulate applications of AI technologies, and is progressively coming into force between 2024 and 2027. The EC seeks to encourage development, deployment and use of Artificial Intelligence, in order to extract economic benefits from it. Many writers see the AIA as being likely to exhibit the 'Brussels Effect'[6], by influencing the practice of AI well beyond the European Union (EU)[7] -- although some conclude differently[8].

The AIA has been the subject of a vast amount of analysis since its path towards enactment began in April 2021[9]. It is large and complex, and contains about 90,000 words in 100 pp. of dense text. The Recital alone contains 34,500 words in 180 numbered paragraphs over 31 pp. This has since been augmented by guidance totalling a further 135pp. and 60,000 words, relating to only the first provisions that came into effect[10], with a second of 36pp.[11] published a mere 18 days before the relevant provisions came into effect. This has been followed by additional documents, important among them the 65-page 'Digital Omnibus' changes of November 2025[12]. The scale and complexity of the text of the AIA inevitably gives rise to a rich diversity of interpretations.

In their endeavours to address a multi-headed and rapidly-changing phenomenon, the AIA's drafters used a number of key terms in novel ways. The phrase 'AI System' occurs 1,080 times, 'risk' qualified in several ways occurs 776 times, 'high-risk' 472 times and 'systemic risk(s)' 80 times. The usages of the key terms, combined with the richness of their contexts of use in the document, present to regulatees as a blizzard of words, and provide researchers and consultants alike with an intellectual banquet on which to feast[13].

The analysis presented in this article is not legal scholarship, and it has not been performed by a lawyer. The perspective adopted is that of a consultant and researcher in strategic and policy aspects of transformative and disruptive information technologies, and the focus is on law as an instrument of public policy. It reflects insights in the substantial prior literature in the field of technology law, including early analyses[14] ,

---

5Nicole Gillespie, et al. 'Trust, atttudes and use of artificial intelligence: A global study' The University of Melbourne and KPMG, 29 April 2025 <https://doi.org/10.26188/2882291

6Anu Bradford, *Brussels Effect: How the European Union Rules the World* (Oxford University Press, Incorporated, 2020).

7Graham Greenleaf 'The 'Brussels effect' of the EU's 'AI Act' on data privacy outside Europe' Privacy Laws & Business 1 (2021) 3-7, at https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=3898904, Graham Greenleaf 'EU AI Act: The second most important data privacy law' Privacy Laws & Business, June 2024, at https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4913686

8Martin Ebers, 'Truly Risk-based Regulation of Artificial Intelligence How to Implement the EU's AI Act' [2024] *European Journal of Risk Regulation* 1-20 <https://doi.org/10.1017/err.2024.78>, pp.18-20

9European Commission, 'Proposal for a Regulation on a European approach for Artificial Intelligence' 21 April 2021, athttps://ec.europa.eu/newsroom/dae/document.cfm?doc_id=75788

10European Commission, 'Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)' Draft of 4 February 2025, at https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

11European Commission, 'The General-Purpose AI Code of Practice', 10 July 2025, at https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai

12 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)' Draft Regulation 2025/0359, 19 November 2025, at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025PC0836

13Clarke R. (2026) 'An Assessment of Key Terms in the EU Artificial Intelligence Act' Xamax Consultancy Pty Ltd, Review Draft of 26 July 2026, at https://rogerclarke.com/EC/AIATerm-260726.pdf

14Lilian Edwards 'The EU AI Act: a summary of its significance and scope' Ada Lovelace Institute, April 2022 <https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf>

optimistic contributors[15] and particularly critical works in the business-oriented information systems literature[16] and in law[17].

The work reported here is intended to complement the many legal analyses of specific aspects of the Act. The focus is on the provisions of the AIA that represent the underpinnings of a regulatory regime. The key terms are defined as follows:

> ***Regulation*** *is the process whereby a socio-technical system adapts its structure and processes in order to accommodate disturbances or damage that it undergoes, so that it operates and adapts as an integrated whole*
>
> ***A Regulatory Regime*** *is a set of mechanisms that influence or control the way entities behave within a socio-technical system, and that thereby contribute to the achievement of economic, social and/or environmental policy objectives*

Rather than offering dispassionate, scholarly analysis, the work is motivated by the public policy need for control to be exercised over inherently dangerous and obscure technology. A critique is provided of the likely overall effects of the EU's highly complex scheme, applying a framework for the evaluation of regulatory regimes that is presented elsewhere[18].

Section 2 provides an outline of the AIA and its declared purposes. In section 3, a previously-published Regulatory Design and Evaluation Framework is outlined whose key elements are as the Objects of Regulation, Required Attributes, a 7-layer Model of Regulatory Mechanisms, and archetypal Players and Plays. The focus is on a regime's 'efficacy' by which is meant its overall quality, encompassing comprehensiveness, effectiveness. efficiency, flexibility and adaptability. Section 4 identifies and describes each of the categories distinguished by the AIA, of which four are subject to separate regulatory regimes of varying intensity. The focus throughout is on the AIA's capacity to deliver regulatory efficacy, not on the law *per se*. Uncertainties and exceptions are noted. Questions also arise in relation to enforcement arrangements. Section 5 summarises the outcomes of the evaluation. Section 6 concludes the article with Discussion and Implications.

2. The AI Act

The AIA was prepared during 2021-24 by the European Commission (EC, which comprises over 30,000 public service employees), passed in March 2024 by the EU Parliament (which in a sense represents citizens but is dominated by the EC), and adopted in May 2024 by the

15 Andrej Zwitter, Oskar Josef Gstrein and Noman Haleem, 'General-purpose AI regulation and the European Union AI Act' [2024] *SSRN Electronic Journal* 1-26 <https://doi.org/10.2139/ssrn.4916400>, Prof Celso Cancela Outeda, 'The EU's AI Act: A Framework for Collaborative Governance' [2024] *Internet of Things* 101291 <https://doi.org/10.1016/j.iot.2024.101291>.

16 Fanny Vainionpaa, et al. 'A Review of Challenges and Critiques of the European Artificial Intelligence Act (AIA)' Proc. Int'l Conf. Infor. Syst., 2023, 14, at https://oulurepo.oulu.fi/bitstream/handle/10024/47651/nbnfioulu-202402061598.pdf, Woersdoerfer M. (2024) 'Mitigating the adverse effects of AI with the European Union's artificial intelligence act: Hype or hope?' Global Business and Organizational Excellence 43,3 (January 2024) 106-126, at https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4630087

17 Veale M. & Borgesius F.Z. (2021) 'Demystifying the Draft EU Artificial Intelligence Act' Computer Law Review International 22,4 (2021) 97-112, at https://arxiv.org/pdf/2107.03721, Irena Barkane, 'Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance' [2022] *Information Polity* 2022, 147-162, <https://doi.org/10.3233/ip-211524>, Wachter S. (2024) 'Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond' Yale Journal of Law & Technology 26,3 (2024) 671-718, at https://yjolt.org/sites/default/files/wachter_26yalejltech671.pdf

18 Roger Clarke, 'Regulatory regimes for disruptive IT: A framework for their design and evaluation' (2026) 60 *Computer Law & Security Review* 106231 <https://doi.org/10.1016/j.clsr.2025.106231>.

Council of the EU (which represents the governments of the member states). The AIA is formally an EU Regulation, 2024/1689, and hence is a law that applies to and within all member states, as part of each member state's law. (EU Directives, on the other hand, set goals for member states to implement). The AIA became EU law on 1 August 2024, with various elements taking effect from 2 February 2025, 2 August 2025, 2 August 2026 and 2 August 2027 (Article 113).

The descriptions in Section 4 draw on the AIA and the EU's high-level summary[19] and a variety of secondary sources in refereed literatures, which are cited where they are relied upon.

The AIA's objective is declared as follows (AIA, Recital (1), emphases added, and reformatted for clarity):

The purpose of this Regulation is

- ***to improve the functioning of the internal market*** *by laying down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence systems (AI systems) in the Union, in accordance with Union values,*
- ***to promote the uptake of human centric and trustworthy artificial intelligence (AI)***
- ***while ensuring a high level of protection*** *of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (the 'Charter'), including democracy, the rule of law and environmental protection,*
- ***to protect against the harmful effects of AI systems*** *in the Union, and*
- ***to support innovation****.*

The driver for the AIA is clearly the stimulation of economic development by supporting AI innovation and promoting its uptake. Control over negative impacts, implications and risks is expressed firstly as a constraint on the economic objective ("while ensuring") and then as an apparently secondary objective ("to protect"). Hence, although the large majority of the provisions relate to protections, the ultimate purpose of those protections is to overcome barriers to adoption of AI technologies. The strangeness of this approach has been noted[20]:

> *"The proposal mixes reduction of trade barriers with broad fundamental rights concerns in a structure unfamiliar to many information lawyers ... [which] brings a range of novelties and tensions"*

Many regulatory regimes focus on the achievement of public trust (i.e. by whatever means), whereas the AIA contains few mentions of 'trust', but 19 of 'trustworthiness', implying an endeavour to earn public trust rather than relying largely on 'public education', in the sense of public relations and marketing.

The following section provides an overview of the framework applied in this article.

---

3. The Evaluation Framework

The perspective that the author brings to this matter is that of an information systems professional and researcher much of whose consultancy career has had as its focus strategic and policy aspects of transformative and disruptive information technologies. This has involved assessment of regulatory regimes applicable to many technologies and

19 European Commission, 'High-level summary of the AI Act' 27 February 2024, at https://artificialintelligenceact.eu/high-level-summary/https://artificialintelligenceact.eu/high-level-summary/

20 Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach' (2021) 22(4) *Computer Law Review International* 97-112 <https://doi.org/10.9785/cri-2021-220402>, p.98.

their applications, including data matching, drones, wearable cameras, 'big data' analytics, and electronic markets of many kinds, most recently those delivered by tech platforms as diverse as Airbnb 'homestay' letting and Uber ride-sharing. From this work, conducted over a 30-year period, a framework has been progressively developed, which is consolidated in a companion paper[21]. Table 1 provides an overview of the elements of the Regulatory Design and Evaluation Framework, supported by brief descriptions below.

Table 1: Overview of the Regulatory Design and Evaluation Framework

References in this Table are to the companion paper[22]

1	**Nature and Objectives**	**Regulation** is the process whereby a socio-technical system adapts its structure and processes in order to accommodate disturbances or damage that it undergoes, so that it operates and adapts as an integrated whole **A Regulatory Regime** is a set of mechanisms that influence or control the way entities behave within a socio-technical system, and that thereby contribute to the achievement of economic, social and/or environmental policy objectives
2	**The Objects of Regulation**	Categories of Objects of Regulation, in Table 1 include a technology, an application, a sector, a product, a practice, a profession, an outcome
3	**Required Attributes**	16 Attributes, grouped under Process, Product and Outcomes in Table 2, which support Regulatory Regime Design or Evaluation
4	**Regulatory Mechanisms**	A 7-Layered Model, in Figure 2, grouped under Government, Self-Governance and Systemic Governance
5	**Players and Plays**	16 archetypal actors and their patterns of behaviour, in Figure 3, grouped into Regulator, Regulatee and Beneficiary clusters
6	**The Nature of Principles**	The Principles and Rules on which Regimes are built
7	**Articulation, Regulation**	Recommended Co-Regulatory Institutions and Processes, in Table 5
8	**Evaluation**	Evaluation Template and scoring alternatives, Appendices 1 and 2

A regulatory regime can be applied to various categories of objects. In the case of the AIA, the primary focus is artefacts that embody what the AIA refers to as AI technology ("a AI system"), but the regulatory measures apply differentially depending on the particular purposes they are applied to and the risk-level to which the Act assigns them, and the obligations arising from the regulatory regime are assigned to particular enterprise-categories (primarily "providers", but to some extent also "deployers"). The meaning of key terms used in the AIA are examined in a prior article[23]. The central term 'AI System' has been the subject of more detailed consideration by other authors[24].

The purpose of the Framework is to support the evaluation of the efficacy of regulatory regimes generally. The term 'efficacy' is used as an overall term to encompass all of the desirable elements, including effectiveness, efficiency, flexibility and adaptability. Statutory, code and/or case law is likely to at least influence the process of exercising control over behaviour, and in many cases there will be a substantial body of relevant formal law. The focus of the evaluation framework is not the law, however, but the efficacy of the regulatory regime as a whole, including rather than specifically the law.

---

21 Roger Clarke, 'Regulatory regimes for disruptive IT: A framework for their design and evaluation' (2026) 60 *Computer Law & Security Review* 106231 <https://doi.org/10.1016/j.clsr.2025.106231>.

22 ibid.

23 Clarke R. (2026) 'An Assessment of Key Terms in the EU Artificial Intelligence Act' Xamax Consultancy Pty Ltd, Review Draft of 26 July 2026, at https://rogerclarke.com/EC/AIATerm-260726.pdf

24 Meinel P., Baum K., Hermanns H., Pöppelmann E., Langer M. & Lauber-Rönsberg A. (2026) 'What are AI systems? Rethinking the core definition in the EU AI Act' Computer Law & Security Review 62 (September 2026) 106373, at https://pdf.sciencedirectassets.com/271884/1-s2.0-S2212473X26X20028/1-s2.0-S2212473X26001148/main.pdf

The mechanisms are ordered into a hierarchical model of seven layers, with formal law (featuring 'government' and 'compliance') making up the top two, self-regulation (using the catchwords 'governance', 'safeguards' and 'mitigation') the middle three, and systemic governance (comprising infrastructural and natural regulatory features) the foundational two. Three generic entities are distinguished: Regulators, Regulatees and Beneficiaries, with a more detailed model of the players involved[25].

The article that defines the Framework identifies 16 criteria[26], and is supported by an Evaluation Template. The key contribution of the framework is to provide structure to the assessment of regime performance against defined criteria. The evaluation process involves assessing the particular regulatory regime's delivery against each of the criteria. Assessors can refine the analysis, or conduct their own evaluations against the criteria, or evaluate against an enhanced or alternative version of the criterion-set. In addition, a scoring process is provided, as a means of encouraging assessors to focus in turn on each of the criteria, and on the extent to which the particular regime does and does not satisfy them. Any endeavour to deliver an objective score would be, by its nature, futile. However, to assist evaluators in achieving an integrated view of the regime as a whole, a pragmatic, weighted-score approach is offered. This suggests assigning two scores: one a simple ternary indicator 'Yes, Some, No', and the other a subjective score on the scale 0-5 for 6 Process factors and 0-7 for 10 Product and Outcome factors, giving an overall score out of 100.

The following section identifies the five categories of AI System identified by the AIA, outlines the nature of and provisions relating to each category, and considers important factors relevant to the question of whether and to what extent the regulatory regime is likely to be efficacious in the sense used in this article.

---

4. The Multiple Regulatory Schemes under the AIA

The AIA distinguishes four categories of "AI systems", depending on their level of "Risk". It claims to create distinct regulatory regimes for three of them, as outlined in Table 2.

Table 2: AI System Risk Levels and Regulatory Schemes

Subject to Regulatory Regimes

- "**Unacceptable Risk**" AI systems, which are "**prohibited**", addressed in section 4.1 immediately below
- "**High-Risk"** AI systems", which are "**regulated**", addressed in section 4.2
- "**Limited-Risk**" AI systems, "**subject to lighter transparency obligations**", addressed in section 4.3

Not Subject to any Regulatory Regime (as at early 2025)

- **Minimal-Risk** AI systems

A fifth category, and the fourth that is subject to a regulatory regime, is a "**General purpose AI (GPAI) system**". This is addressed in section 4.4. Enforcement aspects are considered in section 4.5. The structure adopted in this Section may appear complex and cumbersome, but it is dictated by that of the AIA.

25Roger Clarke, 'Regulatory regimes for disruptive IT: A framework for their design and evaluation' (2026) 60 *Computer Law & Security Review* 106231 <https://doi.org/10.1016/j.clsr.2025.106231>, Figure 3.

26ibid., Table 2.

4.1 The Regulation of Unacceptable-Risk / Prohibited AI Systems

'Unacceptable-Risk / Prohibited AI Systems' are defined in a closed-ended manner (Art.5). The eight items describe **applications of "AI systems"** rather than the characteristics of the artefact, or the process or technique(s) used to achieve an output or outcome.

The Article contains 1,750 words of a moderate degree of complexity, posing challenges for both commentators and implementors. The eight items are subject to **over 20 exclusions**, based variously on the intended outcomes; the extent to which harm is caused; the attributes of the users and usees (i.e. those who are indirectly impacted); the data involved; the source of the data; or the organisation performing the function, or in which, or for which, the function is performed.

The **scope of exclusions** is unclear and may well remain so, but appears to be very broad. For example, to be Prohibited under each of Arts. 5.1(a) deception and 5.1(b) vulnerability exploitation, a very high bar is set, because an AI system must (i)"distort behaviour", and (ii) "cause" (iii) "significant harm".

Similarly, Art. 5.1(c) social scoring (the classification of people based on their social behaviour or personality characteristics) only applies where the data is used out of context or people are treated in a "detrimental or unfavourable" manner, and even then not if the biometric dataset was "lawfully acquired" (which would doubtless be claimed to be the case with most declared uses).

Use for Art. 5.1(d) 'predictive policing', is permitted if it (i) "augments" (ii) "human assessment". Art. 5.1(e) "compiling facial recognition databases" is not prohibited if it is "targeted" (i.e. the result of personal surveillance[27]), or "untargeted" (i.e. mass surveillance) provided that it is from any source other than "the internet" (which is not a source but a means of communication with sources) or "CCTV footage". Art. 5.1(f) "inferring emotions" is permitted in most contexts, and even in "workplaces and educational institutions" if "for medical or safety reasons".

In Art. 5.1(g), the "biometric categorisation systems" prohibition only applies to a closed-ended list of what the high-level summary[28] calls 'inferred sensitive attributes', and an exemption is granted for the use of "lawfully acquired biometric datasets". In Art. 5.1(h), "'real-time' remote biometric identification (RBI) in publicly accessible spaces for the purposes of law enforcement" is not prohibited, but rather authorised, for a wide range of law enforcement activities, subject to some requirements in the 1,150 words of Arts. 5.1(h) and 5.2-5.7. In relation to "the processing of biometric data for purposes other than law enforcement", the GDPR Art.9 prohibitions remain in place.

In short, the prohibitions provisions embody a large array of loopholes, and determining thresholds for each criterion will be fraught, contested, take time, and even then remain uncertain. Legal advisors and consultants are obliged to draw opportunities to the attention of their clients, and to assist their clients in the event that they seek to escape the prohibition by utilising any of the exceptions. An early analysis of the AIA's prohibition provisions drew attention to both their importance and the enormous challenges involved in defining boundaries and achieving desired regulatory effects[29]. Art.5 came into effect on 2 February 2025. A very substantial guidance document was published 2 days later, still in

27 Roger Clarke, 'Information technology and dataveillance' (1988) 31(5) *Communications of the ACM* 498-512 <https://doi.org/10.1145/42411.42413>.

28 European Commission, 'High-level summary of the AI Act' 27 February 2024, at https://artificialintelligenceact.eu/high-level-summary/https://artificialintelligenceact.eu/high-level-summary/

29 Neuwirth R.J. (2023) 'Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA)' Computer Law & Security Review 48 (April 2023) 105798, at https://www.sciencedirect.com/science/article/abs/pii/S0267364923000092

draft[30]. The final version, 129 pages and 66,000 words, is dated 27 July 2025, 6 months after the provisions came into force. This appears to generally confirm the impression of the exceptions having very broad scope[31].

It is reasonable to expect that a great many activities will escape the Art.5 provisions by virtue of the more than 20, often very broad, exceptions, and that relatively few activities will be prevented. The question therefore arises as to which, if any, of the 'might have been Prohibited / Unacceptable Risk' applications of AI Systems are subject to any of the other regulatory regimes. Another author has provided an assessment of the AIA's inadequacies in relation to the analysis and management of risk, and proposed a corrective solution[32].

4.2 The Regulation of High-Risk / Regulated AI Systems

Even if an AI system escapes prohibition, it may be a 'High-Risk / Regulated AI System'. This is also defined in terms of **applications of "AI systems"** rather than the characteristics of the artefact. or the process or technique(s) used to achieve an output or outcome. or the AI system's impacts. The included AI system applications fall under two headings:

The first heading is "[an AI system] intended to be used as **a safety component of a product**, or the AI system is itself a product, **covered by the Union harmonisation legislation listed in Annex I**" and that "is required to undergo a third-party conformity assessment" under that legislation (Art.6-1). These are commonly referred to as **Embedded AI Systems**.

Annex I lists 11 Regulations and 9 Directives that apply to many categories of artefacts (including machinery, toys, medical devices, appliances and various kinds of vehicles), which are by their nature capable of causing harm and hence subject to obligations relating to safety. It may be that the existing law already applies to AI-based safety components and especially AI-based safety products, and hence it appears that these provisions may add no further protections. This could only represent a satisfactory public policy response if analyses have been undertaken, and the threats inherent in these new technologies have been found to be already addressed by extant laws across 11 EU industry segments plus 9 industry segments across 27 member-state jurisdictions. It is not clear that such studies have been done, nor that such conclusions have been justifiably reached.

The second heading covers eight **sub-categories** of "areas [of application of] AI systems referred to **in Annex III**" (Art.6-2, Annex III). These have been referred to as **Standalone AI Systems**, and encompass a wide array of areas of application, encompassing Biometrics, Critical infrastructure, Education, Employment, essential services, Law enforcement, Migration and public administration. However, the following paragraphs of this article identify many exceptions, the combination of which create the scope for apparently-regulated "High-Risk AI systems" to escape from the category entirely, or at least from any pre-deployment obligations.

Four generic exceptions are declared, in relation to "a narrow procedural task", "improv[ing] the result of a previously completed human activity", adjuncts to "a

---

30 European Commission, 'Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)' Draft of 4 February 2025, at https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

31 Paul Weiss, 'European Commission Publishes Guidance on Prohibited AI Practices Under the EU AI Act' 25 February 2025, at https://www.paulweiss.com/practices/litigation/artificial-intelligence/publications/european-commission-publishes-guidance-on-prohibited-ai-practices-under-the-eu-ai-act?id=56629

32 Gasiola G.G. (2025) 'Rebuilding the pyramid: The AI Act's risk-based approach using a binary decision diagram' Computer Law & Security Review 58 (September 2025) 106189, at https://pdf.sciencedirectassets.com/271884/1-s2.0-S2212473X25X00031/1-s2.0-S2212473X25000616/main.pdf

completed human assessment" and "[being] a preparatory task to an assessment" that is relevant to an Annex III use-case (Art.6.3).

In addition to the four generic exceptions, the eight sub-categories defined in Annex III are subject to **a dozen exceptions within their detailed descriptions.** In some cases, closed-ended lists are used, which are likely to have the effect of excluding unmentioned sub-categories of applications, whether or not that was the intention, and whether or not the list is inconsistent with text elsewhere. Some forms of exception, such as "except when detecting financial fraud", create the possibility of 'laundering' systems by designing that feature in, and inter-twining its use with some other feature. Accidental exceptions may arise where a provision is very difficult to comprehend, such as that for 'predictive policing'.

There are **four further, substantial and largely uncontrolled exceptions** in the second bullet, supplemented by heavy qualification in the fourth bullet, whereby **"providers" are authorised to self-assess** whether any particular AI system is "high-risk", subject to the uncontrolled proviso "must document such an assessment before placing it on the market or putting it into service". See Art.43.2.

On the other hand, "an AI system referred to in Annex III shall **always** be considered to be **high-risk where the AI system performs profiling of natural persons**" (Art.6.3). For this purpose, "profiling" means "profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679", commonly known as the General Data Protection Regulation (GDPR) (Art.3(52)). The GDPR definition is (emphases added):

> ***Profiling*** *is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*

This corresponds to the preparation and use of **a 'digital persona' associated with a particular entity or identity**[33] (emphasis added):

> *[**A digital persona**] is a model of [a particular] individual's public personality based on data and maintained by transactions, and intended for use as a proxy for [that] individual*

This is quite different from another longstanding use of the term 'profiling' to refer to the generation and use of an abstract model of the key characteristics of a category of identities, such as a 'drug-mule', or a student who would benefit from a particular form of intervention[34] (emphasis added)

> *[**Profiling** is] a technique whereby a set of characteristics of a particular class of person is inferred from past experience, and data-holdings are then searched for individuals with a close fit to that set of characteristics*

The unequivocal nature of the stipulation that 'all Annex III AI systems that perform profiling are High-Risk' is challenging to interpret. Of the eight categories in Annex III, only '2. Critical infrastructure AI systems' appear unlikely to perform profiling to 'evaluate aspects of a natural person'; whereas it appears that the other seven generally do so. The question arises as to whether the stipulation that they are automatically High-Risk

---

33 Roger Clarke, 'The digital persona and its application to data surveillance' (1994) 10(2) *Information Society* 77,-92 <https://doi.org/10.1080/01972243.1994.9960160>, Roger Clarke, 'Persona missing, feared drowned: the digital persona concept, two decades later' (2014) 27(2) *Information Technology & People* 182-207 <https://doi.org/10.1108/itp-04-2013-0073>.

34 Roger Clarke, 'Profiling: A Hidden Challenge to the Regulation of Data Surveillance' Journal of Law and Information Science 4,2 (December 1993) <http://rogerclarke.com/DV/PaperProfiling.html>

overrides all, some, or even any, of the many exceptions built into the Annex III descriptions.

For those "AI systems" for which an escape-route does not exist, providers are subject to requirements defined in Arts.8-39, which amount to 12,000 words. AIA Chapter III (High-Risk AI Systems) Section 2 (Requirements for high-risk Al systems) is written in a manner that creates interpretation challenges from regulatory and compliance perspectives. It comprises eight Articles, commencing with an introduction (Art.8), followed by substantive requirements in relation to a Risk management system (Art.9), Data and data governance (Art.10), Technical documentation (Art.11), Record-keeping (Art.12), Transparency and provision of information to deployers (Art.13), Human oversight (Art.14), and Accuracy, robustness and cyber-security (Art.15).

Art.8.1 declares that "High-risk AI systems shall comply with the requirements laid down in this Section", but the clause uses the passive voice, there appears to be no universal statement that all compliance responsibilities rest with providers, and there are only incidental mentions of "provider" in Arts. 9-10 and 13-15, and none at all in Arts.11 and 12. To developers, providers, service-providers and deployers of such AI systems, it is something of a mystery as to whether any particular party has to actually do anything.

Art.13 re Transparency and provision of information to deployers is indicative of how what seem at first to be requirements melt away to nothingness. Providers of high-risk AI systems are nominally required to deliver 'transparency'. However, such impact as the clauses might have had are undermined by the omission of any requirement for an explanation of the rationale underlying any inference the AI system draws, decision it makes, or action it performs (emphases added):

> *3. The instructions for use shall contain at least the following information:*
>
> *(b) the characteristics, capabilities and limitations of performance of the high-risk AI system, including: ...*
>
> *(iv) where applicable, the technical capabilities and characteristics of the high-risk AI system to provide information that is relevant to explain its output; ...*
>
> *(vii) where applicable, information to enable deployers to interpret the output of the high-risk AI system and use it appropriately*

A comprehensive critique of the AIA's failure in relation to transparency is provided by another author[35]:

> *the current framework [Art.50-1] insufficiently safeguards the rights of individuals, particularly vulnerable groups, due to narrow content requirements, lack of effective remedies, ... exemptions for law enforcement and ostensibly 'obvious' AI use ... [mere requirement of] notification that an AI system is being used ... [neglect of] the critical role of deployers, who are often better positioned to ensure meaningful transparency at the point of interaction [and failure to confer] actionable rights to affected persons*

The associated Art.86 (Right to explanation of individual decision-making) similarly avoids delivering any such right. The active words are "the right to obtain from the deployer clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken" (Art.86-1, emphases added). Neither the 'role' nor the 'main elements' represents an explanation of the

35Block M.J. (2026) 'Transparency in human-AI interaction – An analysis of Article 50(1) AI Act' Computer Law & Security Review 61 (July 2026) 106327, at https://pdf.sciencedirectassets.com/271884/1-s2.0-S2212473X26X20016/1-s2.0-S2212473X26000684/main.pdf, pp,.1,9

rationale. Despite the emptiness of the requirement, the Article also incorporates a string of exceptions, some unclear and extensible.

The complete absence of a right of access to the underlying rationale is reaffirmed by the absence from the 1160 words of Art.26 (Obligations of deployers of high-risk AI systems) of any requirement to explain inferences, decisions and actions to individuals adversely affected by them[36].

The Recitals contain fine words ("The deployer should also inform the natural persons about their right to an explanation provided under this Regulation" in Recital 93, and "Affected persons should have the right to obtain an explanation where a deployer's decision is based mainly upon the output from certain high-risk AI systems" in 171, emphases added). As in many other places, the fine words in the Recitals are a facade, because they are not expressed and articulated in the statute itself.

Accountability by regulatees for their behaviour is a fundamental element of any regulatory scheme. Accountability exists only if a set of requirements is satisfied[37]. A reviewer of an inference drawn, a decision made or an action taken by an entity needs to be able to assess the reasonableness of the entity's behaviour. Where the behaviour is unreasonable, some form of corrective or compensatory measure is necessary. The reviewer needs to be able to audit the process used by the entity, whether through observation, replication, inspection of records, or demand for and consideration of testimony. At the heart of any review is the requirement that the reviewer have access to a humanly-understandable explanation of the rationale underlying the inference, decision or action.

If the inference, decision or action derives from a process that is obscure, or that cannot be assessed against criteria, or that depends on ephemeral data or data-states that cannot be rediscovered or regenerated, no rationale can be provided. In that case, the reviewer is left with the choice of applying the 'strict liability' principle and determining in the claimant's favour if harm is found to have occurred, or relieving the entity of accountability.

Various categories of AI systems, including those using generative AI and recent forms of data analytics, apply 'artificial neural network' or other techniques that are purely empirical, and whose behaviour cannot be usefully modelled by business process descriptions, algorithms, decision-trees, rules, or other expressions of rational processes. Moreover, many such AI systems continually adapt their internal data-states. Those ephemeral data-states are generally not capable of being reconstructed. For these multiple reasons, those categories of AI system cannot generate explanations, and hence are incompatible with the notion of accountability.

Despite some efforts invested into the idea of Xplainable AI (XAI), it has produced little of value and remains aspirational. I contend that it is untenable for a society to abandon accountability principles merely because doing so serves the interests of providers of dangerous technology, nomatter how beguiling the claims about its potential benefits.

Section 3 (Obligations of providers and deployers of high-risk Al systems and other parties) is, on the other hand, a little clearer. Art.16's title refers to "Obligations of providers". Providers have obligations under all of Arts.16-25. Deployers may have obligations arising from Art.20, and do in the case of Art.25 (where, rather confusingly, a deployer is "considered to be a 'provider'"), Art.26 (which is headed "Obligations of

---

36 Ida Varošanec, 'On the path to the future: mapping the notion of transparency in the EU regulatory framework for AI' [2022] 36(2) *International Review of Law, Computers & Technology* 95-117 <https://doi.org/10.1080/13600869.2022.2060471>.

37 Roger Clarke, 'Why the world wants controls over Artificial Intelligence' (2019) 35(4) *Computer Law & Security Review* 423-433 <https://doi.org/10.1016/j.clsr.2019.04.006>, pp.428-429, Claudio Novelli, Mariarosaria Taddeo and Luciano Floridi, 'Accountability in artificial intelligence: what it is and how it works' [2023] 39 *AI & SOCIETY* 1871-1882 <https://doi.org/10.1007/s00146-023-01635-y>.

deployers of high-risk Al systems", but whose regulatory effect is unclear) and Art.27. There are also various procedural obligations under Articles 28-39.

The "High-Risk / Regulated AI Systems" provisions under Annex III (Standalone AI Systems) were to come into effect on 2 August 2026, but that was later deferred until 2 December 2027. Similarly, those under Annex I (Embedded AI Systems) were scheduled for 2 August 2027, but later deferred to 2 August 2028. Longer deadlines are set for "AI systems that have been already placed on the market / put into service before the AI Act entered into force". The fog surrounding these provisions may be a little less thick by the time they come into force. Alternatively, the obligations may be retracted, or further weakened, or additional exceptions created.

Successive deferrals and adjustments have occurred. Industry lobbying resulted, in November 2025, in an EC Proposal for a further 65-page Regulation 2025/0359[38], referred to as the 'Digital omnibus on AI', which addressed "several implementation challenges identified through consultations". In relation to high-risk AI systems, providers are now permitted to process special categories of personal data for bias detection and correction, subject to some conditions, and the implementation timeline of data governance obligations for high-risk AI systems has been further eased. A further Media Release in May 2026 referred to postponements to late 2027 and 2028, and to further exemptions[39].

The eight broad sub-categories of Standalone AI Systems nominally described as 'High-Risk' and as being 'Regulated' are qualified by about 30 categories of exception, many very broad or easily invoked, and many of the obligations that could arise in any case offer only very weak protections against powerful and obscure technology applied by powerful organisations. It appears very likely that a great many of the AI Systems that escaped the 'Unacceptable-Risk' category and hence were not 'Prohibited', will also escape this category. Given the impactfulness of many such applications, it is unsurprising that their use is of serious concern to various stakeholders. It is difficult to consider a regime to be efficacious when it fails to address public concerns about the regulation of organisational behaviour.

4.3 The Regulation of Limited-Risk AI Systems

Art.50 is headed "Transparency obligations for providers and deployers of certain AI systems". The AIA uses the terms 'non-high risk' and 'not high-risk'. The high-level summary uses the term 'Limited-Risk AI Systems', and the term '**Limited-Risk/Transparency-Only AI Systems'** is adopted here. There are five sub-categories, expressed in four sub-paras. of Art.50[40].

The first sub-category is "**AI systems intended to interact directly with natural persons**" (Art.50-1). Examples used in the EC's high-level summary are "chatbots" and "deepfakes" (which is a pejorative term for synthetic media creations that are designed to appear real, do so, and are or may be intended to deceive observers into thinking they are real). However, the sole obligation arising is on "providers" of "AI systems intended to interact directly with natural persons", and the obligation is merely that "the natural persons

---

38 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)' Draft Regulation 2025/0359, 19 November 2025, at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025PC0836, European Parliament, 'Legislative Train Schedule: Digital omnibus on AI' 14 December 2025, at https://www.europarl.europa.eu/legislative-train/theme-a-new-plan-for-europe-s-sustainable-prosperity-and-competitiveness/file-digital-omnibus-on-ai

39 European Commission, 'EU agrees to simplify AI rules to boost innovation and ban 'nudification' apps to protect citizens' 7 May 2026, at https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1024

40 Lee Bygrave and Rebecca Schmidt (2025) 'Regulating Non-High-Risk AI Systems under the EU's Artificial Intelligence Act, with Special Focus on the Role of Soft Law' University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2024-10, 29 January 2025, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4997886, pp.2-11

concerned are informed that they are interacting with an AI system, unless this is obvious ..." (emphases added). In apparent conflict with the Act, the high-level summary states that the obligation is also intended to apply to "deployers": "developers and deployers must ensure that end-users are aware that they are interacting with AI (chatbots and deepfakes)"[41] (emphasis added).

Even outside law enforcement, however, the 'obligations' fade away to nothingness. The assessment of the meaning of "AI system" in the companion paper[42] concluded that the term is not limited to any particular generation of development tool and requires no particular attributes of coding techniques or outcomes. Hence any computer-based system is "obviously" an 'AI system. Notices such as 'You are using an AI system' are therefore redundant, and the provision can be safely ignored. The sole obligation relating to this category of 'limited risk' activity is valueless or purely nominal, and, to the sceptical observer, a sham.

Further, it has been argued that[43]:

> *Transparency alone is insufficient to address these issues ... given the well-established harms that such systems may cause. For example, in the past, chatbots have advised users to take their own lives, given dieting tips to people battling eating disorders, and produced reputation-damaging outputs (e.g., false sexual assault charges against innocent people).*

The second sub-category is "**AI systems**, including general-purpose AI systems, **generating synthetic audio, image, video or text content**" (Art.50-2). However, the sole obligation is on "providers", to "ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated" (emphases added). In addition, four **exceptions** exist. One is "an assistive function for standard editing", which appears to create an opportunity for avoidance that is very easily exploited. Another is "AI systems" "authorised by law to detect, prevent, investigate or prosecute criminal offences". Detection and prevention activities are not limited to law enforcement agencies, so this loophole is available to organisations generally.

The third sub-category is "**an emotion recognition system or a biometric categorisation system**" (Art.50-3). The sole obligation in this case is on "deployers", to "*inform* the natural persons exposed thereto of the operation of the system". This is presumably a requirement to inform them that the system is in operation, rather than to inform them how it works. A (potentially large) **exception** exists for "AI systems used for biometric categorisation and emotion recognition, which are permitted by law to detect, prevent or investigate criminal offences". This appears to grant permission not only to law enforcement agencies, but to all organisations, at least in relation to the detection and prevention of crime. If so, the feature is not a protection, but rather an authorisation, and hence a substantial contribution to the burgeoning surveillance society[44].

The fourth sub-category is "**an AI system that generates or manipulates image, audio or video content constituting a deep fake**" (Art.50-4, para. 1). The obligation is again on "deployers", but only to "disclose that the content has been artificially generated or manipulated" (emphases added).

---

41 European Commission, 'High-level summary of the AI Act' 27 February 2024, at https://artificialintelligenceact.eu/high-level-summary/https://artificialintelligenceact.eu/high-level-summary/

42 Clarke R. (2026) 'An Assessment of Key Terms in the EU Artificial Intelligence Act' Xamax Consultancy Pty Ltd, Review Draft of 26 July 2026, at https://rogerclarke.com/EC/AIATerm-260726.pdf

43 Sandra Wachter, 'Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond' [2024] *SSRN Electronic Journal* <https://doi.org/10.2139/ssrn.4924553>, p.683-684.

44 Roger Clarke, 'Responsible application of artificial intelligence to surveillance: What prospects?' [2022] *Information Polity* 1-17 <https://doi.org/10.3233/ip-211532>.

In any case, an exception applies where the use is "authorised by law to detect, prevent, investigate or prosecute criminal offence", and a strong qualification applies where "the content forms part of an evidently artistic, creative, satirical, fictional or analogous work or programme".

The fifth sub-category is "**an AI system that generates or manipulates text** which is published with the purpose of informing the public on matters of public interest" (Art.50-4, para. 2). The "deployers ... shall disclose that the text has been artificially generated or manipulated" (emphases added).

The same law enforcement exception exists as for the fourth category. In addition, an exception exists where the system's output has "undergone a process of human review or editorial control and where a natural or legal person holds editorial responsibility". The use of the passive voice ("has undergone") means that, if the entity that generates or manipulates the text claims editorial responsibility, the text has been washed free of the obligation. All deployers escape even the minimalistic need to disclose that the text was AI-generated. In any case, given the extent to which the orientation and standards of editorship, in journalism and general publication, have changed during the early decades of the 21st century, this provision appears devoid of benefit other than in the narrow realm of formal academic publishing.

The AIA envisages that the EC will "encourage and facilitate the drawing up of codes of conduct", in two cases "to facilitate the effective implementation of the obligations regarding the detection and labelling of artificially generated or manipulated content" (Arts.50-7, 56), and in another case "including related governance mechanisms, intended to foster the voluntary application to AI systems, other than high-risk AI systems, of some or all of the requirements set out in Chapter III, Section 2" (Art.95).

Because of the substantial absence of unavoidable obligations, the AIA represents no threat to organisations' use of AI systems, and hence creates no motivation to pay any more than lip-service to any such codes of conduct, and no incentive to voluntarily implement safeguards. The self-regulatory nature of the 'limited risk' regime appears to be even more vacuous than the rest of the provisions.

4.4 The Regulation of GPAI Models

During the 3-year period during which the AIA was negotiated through the EU's process-bound, administrative processes, and its legislative structures, Generative AI burst on the scene, being "adopted more rapidly than both [PCs and the Internet]"[45]. The EC responded to this innovation by adding provisions relating to "General purpose AI (GPAI) systems" and "GPAI models". The term 'GPAI' appears to have emerged in about 2022-23[46], as an alternative to 'foundation models'. The latter term, also of recent origin, was defined in Stanford University publication of 2021[47] as "any [AI] model that is trained on broad data (generally using self-supervision at scale) that can be adapted (e.g., fine-tuned) to a wide

---

45 UN Office of Information and Communications Technology, 'Generative AI Primer' 29 Aug 2023, at https://unite.un.org/sites/unite.un.org/files/generative_ai_primer.pdf, World Intellectual Property Organization, 'Patent Landscape Report: Generative Artificial Intelligence' 2024, at https://www.wipo.int/web-publications/patent-landscape-report-generative-artificial-intelligence-genai/en/index.html, Roger Clarke, 'Principles for the responsible application of Generative AI' (2025) 57 *Computer Law & Security Review* 106131 <https://doi.org/10.1016/j.clsr.2025.106131>, Alexander Bick, Adam Blandin and David J Deming, *The Rapid Adoption of Generative AI* (Federal Reserve Bank of St. Louis, 2024) <https://doi.org/10.20955/wp.2024.027>.

46 Brown I. (2023) 'Allocating accountability in AI supply chains: a UK-centred regulatory perspective' Ada Lovelace Institute, June 2023, at https://www.adalovelaceinstitute.org/wp-content/uploads/2023/06/Allocating-accountability-in-AI-supply-chains-June-2023.pdf

47 Bommasani R. and 100 others (2021) 'On the Opportunities and Risks of Foundation Models' Human-Centered Artificial Intelligence, Stanford University, 16 August 2021, at https://crfm.stanford.edu/report.html, p.3

range of downstream tasks". As discussed in the companion article[48], the EC's definition of 'GPAI System' does not match well with the rapidly-mutating understanding of those active in the field.

Obligations similar to those for Limited-Risk/Transparency-Obligated AI Systems are imposed on **providers of** "**general-purpose AI systems**, generating synthetic audio, image, video or text content" (Art.50-2). The obligation is to "ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated" (emphasis added). Four **exceptions** exist, including "an assistive function for standard editing" (which appears to create an opportunity for avoidance), and "[AI systems] authorised by law to detect, prevent, investigate or prosecute criminal offences".

It does not appear that any obligations are placed on "deployers" of "GPAI systems", nor on "end-users" of them.

Obligations are also placed on "**GPAI model providers**" generally, and to a lesser extent on their "authorised representative[s]" in the EU (Arts.53-54, Annexes XI-XIII). Those obligations are to:

- Draw up **technical documentation**, including training and testing process and evaluation results.
- Draw up information and **documentation to supply to downstream providers** that intend to integrate the GPAI model into their own AI system in order that the latter understands capabilities and limitations and is enabled to comply.
- Establish a policy to respect the Copyright Directive.
- Publish a sufficiently detailed **summary about the content used for training the GPAI model**.

These are not unduly onerous, and are in any case a cost of doing business. Some providers will presumably express the required documentation very carefully, so as to be seen to have achieved compliance while minimising the publication of information that may compromise what the provider perceives to be competitive advantage.

Entities that are "**providers of GPAI models with systemic risks**" are subject to additional obligations (Art.55). As discussed in the companion article[49], the EC's malleable definition of this category in terms of "high impact capabilities evaluated on the basis of appropriate technical tools and methodologies" (Art.51-1(a)), is highly problematical.

The additional obligations of such providers are to (Art.55):

- Perform **model evaluations**, including conducting and documenting adversarial testing to identify and mitigate systemic risk.
- Assess and **mitigate possible systemic risks**, including their sources.
- Track, document and **report serious incidents** and possible corrective measures to the AI Office and relevant national competent authorities without undue delay.
- Ensure an adequate level of **cybersecurity protection**.

These are also, at least to some extent, appropriate business practices, and requirements of good organisational governance and of insurers. They are also for the most part internal matters subject to only limited external disclosure. Further, it is envisaged that compliance will be facilitated by Codes of Practice and in due course a European standard (Arts.55-2, 56), voted on by governments. On the other hand[50]:

---

48 Clarke R. (2026) 'An Assessment of Key Terms in the EU Artificial Intelligence Act' Xamax Consultancy Pty Ltd, Review Draft of 26 July 2026, at https://rogerclarke.com/EC/AIATerm-260726.pdf

49 Clarke R. (2026) 'An Assessment of Key Terms in the EU Artificial Intelligence Act' Xamax Consultancy Pty Ltd, Review Draft of 26 July 2026, at https://rogerclarke.com/EC/AIATerm-260726.pdf

50 Sandra Wachter, 'Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond' [2024] *SSRN Electronic Journal* <https://doi.org/10.2139/ssrn.4924553>, p.690-691, 692.

> *... standards bodies ... CEN and CENELEC do not have direct democratic legitimacy ... this lack of democratic legitimacy is even more worrying due to the far-reaching legal, ethical, political, and economic consequences of the widespread deployment of AI. Standards bodies will be tasked with creating frameworks that interpret the AIA*
>
> *Providers are not only heavily involved in writing the harmonized standards to which they must adhere but also tasked with assessing whether they comply with those standards. This approach creates a major legal loophole*

AIA provisions in relation to transparency and copyright came into effect on 2 August 2025. On 18 July 2025, the Commission published a 36-page guidance document[51]. This was a mere 15 days before the provisions were due to come into force. This was followed in September 2025 by an FAQ page that attempted to clarify some of the murk[52]. Enforcement powers were withheld until 2 August 2026. At that time, the Commission had not yet exercised its power under Art.51-1(b) to clarify the vagueness of the definition. Finally, GPAI models that were already placed on the market or put into service before 1 August 2024 are required to be compliant by 2 August 2027. See also Art.113.

The AIA envisages that the EC will "encourage and facilitate the drawing up of codes of conduct, including related governance mechanisms, intended to foster the voluntary application to AI systems, other than high-risk AI systems, of some or all of the requirements", and para.2 envisages that these relate to "deployers" as well as "providers" (Art.95). The very large corporations that operate 'tech platforms' have been strenuously resisting governments' endeavours to impose formal regulation to protect the public[53]. For deployers as for providers, the efficacy of these voluntary measures as a regulatory mechanism is in great doubt.

4.5 Enforcement Measures under the AIA

To the extent that any of the four regimes outlined in the preceding sub-sections impose obligations on some providers and/or deployers in respect of some AI Systems and GPAI Systems, the questions arise as to whether any of those obligations are capable of being enforced, and whether any actual enforcement has commenced.

It is readily argued that, given the pioneering nature of the legislation, the absence of any experience among regulatory agencies' staff, and the absence of clarity in relation to key terms in the Act, it would be unreasonable for any regulator to leap quickly into enforcement actions. However, some aspects of the AIA have been in force since 1 August 2024, some relating to Unacceptable-Risk/Prohibited AI Systems since 2 February 2025, and some relating to High-Risk/Regulated AI Systems, some Limited-Risk/Transparency-Obligated AI Systems and some new GPAI Systems since 2 August 2026. The EC provides

---

51 European Commission, 'The General-Purpose AI Code of Practice', 10 July 2025, at https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai

52 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)' Draft Regulation 2025/0359, 19 November 2025, at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025PC0836

53 Cynthia Kroet 'Meta rebuffs EU's AI Code of Practice' Euro News, 18 July 2025, at https://www.euronews.com/next/2025/07/18/meta-rebuffs-eus-ai-code-of-practice

an outline of the AIA's implementation dates[54], and a fuller version is provided on a third-party's site[55].

One early study of compliance[56] found that obligations imposed on 2 August 2025 had more modest impact on a sample of organisations' terms of service and acceptable use policies by late August 2025 than would have reasonably expected (50% of EU companies, 43% of EU subsidiaries of foreign companies, and 14% of companies outside the EU).

Enforcement responsibilities are scattered across scores of agencies at EC and national levels. The capacity of the EC to perform its own enforcement responsibilities, and to provide guidance to the many other regulators, hinges on the staff of units A2 (AI Regulation and Compliance) and A3 (AI Safety)[57]. As at mid-July 2026, those units were reported[58] as numbering 71 people, about half the staff-count of the Office as a whole, with hiring continuing.

In Laux (2023), six principles for the design of oversight mechanisms for AI are proposed:

(1) Justification sufficient to deliver legitimacy,

(2) Periodical review of compliance,

(3) Collective decisions to address corruptibility of individuals,

(4) Distributed institutional competence / separation of powers,

(5) Justiciability and Accountability, and

(6) Transparency.

The governance structures and processes created by the AIA deliver on some of those principles, but fall seriously short on others, very importantly (5) Justiciability and Accountability, and (6) Transparency. As was noted in s.3.2 above, the AIA abandons accountability entirely, by denying transparency to affected parties, and to reviewers. There is no right of access to the rationale underlying inferences, decisions and actions that harm their interests. Transparent explanations are a fundamental requirement for accountability, and without them a court cannot determine the matter and hence the requirement for justiciability also fails.

The AIA's Enforcement, Remedies and Penalties (Arts.74-101) are complex, with provisions extending across about 9,000 words. Even positive reviews anticipate diversity and uncertainty among interpretations and implementations[59]. Generally, such enforcement powers as exist are to be the responsibility of each member-nation's 'market surveillance authority'. These powers are exercised primarily under an existing EU Regulation[60]. The responsibilities in relation to some matters are exercised by "National public authorities or bodies which supervise or enforce the respect of obligations under Union law protecting fundamental rights" (Art.77). Arts. 85-86 also place some limited capability in the hands of beneficiaries of regulation[61].

---

54 Timeline for the Implementation of the EU AI Act, at https://ai-act-service-desk.ec.europa.eu/en/ai-act/timeline/timeline-implementation-eu-ai-act

55 EU Artificial Intelligence Act Implementation Timeline, at https://artificialintelligenceact.eu/implementation-timeline/

56 Szostak K., van Dijck G. & Kollnig K. (2026) 'Mind the competitiveness gap: Measuring the AI Act's extraterritorial reach' Computer Law & Security Review 62 (September 2026) 106357, at https://www.sciencedirect.com/science/article/pii/S2212473X26000982, p.8

57 EC (2026) 'European AI Office' European Commission, 31 July 2026, at https://digital-strategy.ec.europa.eu/en/policies/ai-office#ecl-inpage-the-structure-of-the-ai-officeundefined

58 Haeck P. (2026) 'The European Commission expects 40 jobs to open up in both units over the course of 2027' Politico, 31 July 2026, at https://www.politico.eu/article/commission-launches-major-hiring-push-for-ai-office/

59 Andrej Zwitter, Oskar Josef Gstrein and Noman Haleem, 'General-purpose AI regulation and the European Union AI Act' [2024] *SSRN Electronic Journal* 1-26 <https://doi.org/10.2139/ssrn.4916400>, pp.13-16.

60 EU (2019) 'Regulation (EU) 2019/1020 on market surveillance and compliance of products' European Parliament and Council, 20 June 2019, at https://eur-lex.europa.eu/eli/reg/2019/1020/oj/eng

The Article 86 right, however, is constructively misrepresented in the heading of the Article as "Right to explanation ...". The article does not create a right to understand the rationale. The law merely creates "the right to obtain from the deployer clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken" (emphases added). This limits the right to knowledge of where in the process AI was used, and the highlights (only) of what was done that harmed the victim's interests. There are many aspects of the claims in the Recitals that are not borne out by a careful reading of the Articles; but the misrepresentation of the effect of this particular Article is simply blatant.

In the specific case of GPAI models, providers are subject to some measures that are the responsibility of an EU-level AI Office (Art.65). The following statement about their "governance" appears in the high-level summary:

How will the AI Act be implemented?

- *The AI Office will be established, sitting within the Commission, to monitor the effective implementation and compliance of GPAI model providers.*
- *Downstream providers can lodge a complaint regarding the upstream providers [sic] infringement to the AI Office.*
- *The AI Office may conduct evaluations of the GPAI model to:*
    - *assess compliance where the information gathered under its powers to request information is insufficient.*
    - *Investigate systemic risks, particularly following a qualified report from the scientific panel of independent experts.*

This overlooks the roles to be played by many other actors, in particular the European Artificial Intelligence Board, at least one but probably multiple national regulatory agencies in every country, perhaps including both existing and new agencies, plus data protection agencies at both national and EU levels. Coordination and inter-operation may prove challenging. See in particular Recitals 156-179 and Articles 65-96.

Furthermore (emphasis added)[62]:

> *Very limited obligations apply to providers and deployers of GPAI systems ... Governance of GPAI providers overwhelmingly and problematically relies on transparency mechanisms. While it is essential that providers of GPAI models and systems make certain information and documentation available, this is only the first step in adequate governance.*

The outlines provided above have identified large numbers of weaknesses in the AIA's provisions, in the institutional arrangements, and in the enforceability of the various measures. The origins of some of these weaknesses lie in the EU's complex governance structures and processes, and the framing of AI regulation within the existing market supervision arrangements (emphasis added)[63]:

> *... the Draft AI Act ... has severe weaknesses. It is stitched together from 1980s product safety regulation, fundamental rights protection, surveillance and consumer protection law ... these pieces and their*

---

61 Sandra Wachter, 'Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond' [2024] *SSRN Electronic Journal* <https://doi.org/10.2139/ssrn.4924553>, p.693.

62 Sandra Wachter, 'Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond' [2024] *SSRN Electronic Journal* <https://doi.org/10.2139/ssrn.4924553>, p.699.

63 Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach' (2021) 22(4) *Computer Law Review International* 97-112 <https://doi.org/10.9785/cri-2021-220402>, p.112.

> *interaction may leave the instrument making little sense and impact. The prohibitions range through the fantastical, the legitimising, and the ambiguous ... Counterintuitively, the Draft AI Act may contribute to deregulation more than it raises the regulatory bar.*

The final version of AIA is of even less value than the earlier drafts would have been[64]:

> *... the strong lobbying efforts of big tech companies and member states were unfortunately able to water down much of the AIA. An overreliance on self-regulation, self-certification, weak oversight and investigatory mechanisms, and far-reaching exceptions for both the public and private sectors are the product of this lobbying*

Following industry lobbying, the limited protections afforded by AIA were further weakened in November 2025. The EC announced in the context of its 'Digital Omnibus on AI' that (1) high-risk AI systems providers will be permitted to process special categories of personal data for bias detection and correction, (2) the implementation timeline of data governance obligations for high-risk AI systems will be eased, (3) the obligation on providers and deployers of AI systems to ensure AI literacy of their staff will be withdrawn, and (4) providers and deployers will be offered "more flexibility in the post-market monitoring"[65].

---

5. Conclusions from the Evaluation of the AIA Regulatory Regimes

The Framework outlined in Section 3 was applied to the regulatory regimes described in Section 4. Details of the study are provided in a supporting document[66] That evaluation reaches the following conclusions:

(1) The provisions relating to the first of the AIA regimes, addressed in Section 4.1, concerned with **'Unacceptable Risk/Prohibited AI Systems'**, would be reasonably expected to be the strongest of the AI regimes. However, the cluster of criteria associated with Process achieved the barest of Passes, and those associated with Product and Outcomes were each scored well below Pass-level. **It is difficult to see how this could be regarded as an efficacious regulatory regime**;

(2) The second of the AIA regimes, addressed in Section 4.2, is concerned with **'High-Risk/Regulated AI Systems'**.

No evaluation was undertaken of the 11 EU regimes, nor of the many (potentially 9x27) member-state regimes, that regulating safety products, listed in Annex I to the AIA. However, it is far from clear that those regimes will, without careful amendments, satisfactorily address the risks arising from **embedment of obscure AI Systems** into a wide array of products that, by definition, embody dangers to life, limb and property.

Evaluation was undertaken in relation to the eight sub-categories of **Standalone AI Systems** listed in Annex III, which are subject to the AIA. They fared even worse than the first regime. Process scored similarly, at a bare Pass, and Product and Outcomes yet lower, because of the wide array of designed-in loopholes, and the strong incentive to use them that arises from complex and in part incoherent expressions and

---

64 Sandra Wachter, 'Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond' [2024] *SSRN Electronic Journal* <https://doi.org/10.2139/ssrn.4924553>, p.672.

65 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)' Draft Regulation 2025/0359, 19 November 2025, at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025PC0836

66 Roger Clarke, 'Application of the Regulatory Design and Evaluation Framework to the EU Artificial Intelligence Act (AIA)' Xamax Consultancy Pty Ltd, 21 January 2026, http://rogerclarke.com/EC/RRE-AIA-Annex.html.

the consequent high compliance costs and uncertainties. Of especial concern is the absence of any obligations on deployers of high-risk AI systems to provide explanations for inferences, decisions and actions unfavourable to people's interests, and of any obligations on providers to enable deployers to do so. Accordingly, **the overall grade assigned was a Very Bad Fail**;

(3) The third of the AIA regimes, addressed in Section 4.3, is concerned with **'Limited-Risk/Transparency-Only' AI Systems**. Minimal obligations exist, and are available to many providers and deployers of five sub-categories of AI systems. All three clusters of criteria were scored at dismally low levels, giving an overall grade of a Very Low Fail -- **so inadequate that it can barely be regarded as a regulatory regime**;

(4) The remaining 'catch-all' category is referred to as **Minimal-Risk AI Systems**. The richness of exceptions built into all of the 'Unacceptable/Prohibited', 'High-Risk/Regulated' and 'Limited-Risk/Transparency-Obligated' regimes described in Sections 4-1 to 4.3 is so great that it appears that a very large majority of 'AI Systems' and applications of them will drop into this bucket. These include many that are impactful and are the subject of considerable public concern. **Most appear to be subject to no obligations at all, and the remainder have trivial transparency obligations**, and without any safeguards, mitigation measures, enforcement, or avenues for recourse in the event of harm being done;

(5) The fourth AIA regime, addressed in Section 4.4, is concerned with **GPAI models**. Understandably, the EC has adopted a very preliminary, 'watch and be prepared to act further' approach. It was found that **it does not reach a sufficient level of meaningfulness to justify review as a regulatory regime**.

This combination of multiple heavily-loopholed regulatory regimes appears unlikely to be able to satisfy the public policy need.

---

6. Discussion and Implications

The purpose of the work reported in this article was declared as examination of the AIA as the underpinnings of a regulatory regime, assessment of it by means of a separately-published framework for the evaluation of regulatory regimes, and delivery of a comprehensive view of the AIA's efficacy. The particulars of the assessment are subject to a great many qualifications. I contend, however, that the method (developed over decades, applied many times, and published separately) provides a workable basis for assessment, and is sufficiently explicit to support critique, and to facilitate adaptation and application by others.

The literature evidences a wide range of views on the many facets of the EC's work. Seen through the lens of the selected evaluation framework, the rosiness pales, the uncertainties and ambiguities pile up, the obligations are exposed as being very limited, the avoidability of obligations through the exploitation of the vast numbers of exceptions becomes very apparent, and the credibility of claims of ease of understanding, application and compliance, and of enforceability, appears to be very low.

A cynical view would be that the EC's objectives of economic progress and the stimulation of innovation entirely dominate its concern for the interests of individuals. The 'Ethics Guidelines for Trustworthy AI' delivered by the EC's own Expert Group in 2019[67] were seen as being inconsistent with economic progress. Rather than conducting a program to operationalise those Guidelines, a very different approach to design was adopted, with protections treated not as objectives but as constraints that required careful manipulation in order to become enablers.

---

67 European Parliament, 'Regulation (EU) 2019/1020 on market surveillance and compliance of products' 20 June 2019, at https://eur-lex.europa.eu/eli/reg/2019/1020/oj/eng

The EC 's economics-motivated approach was vindicated in that national governments demanded an even weaker scheme, and the European Parliament capitulated, abandoning its attempts to strengthen the provisions. Both the EC and the Parliament acceded to the demands of self-interested corporations active in the development and deployment of AI that innovation should be fettered minimally, or not at all, by protection of the interests of those negatively impacted by AI innovation.

A key issue identified in this analysis is the need for individuals and organisations subject to it to be able to discover what provisions of the AIA apply to their work and to their products and services, to understand those provisions, and to relate them to the development and deployment of their products and services. It was argued in a prior article that the key terms used in the AIA, viz. 'AI System', 'GPAI', 'risk' and 'systemic risk', verge on incomprehensibility by the AI practitioner audience that ought to be a primary target for communications about the AIA's provisions. The circumstances and nature of such obligations as the AIA imposes, and their allocation to actors in the value-chain, are also highly unclear. There is accordingly a low likelihood of behavioural adjustments by developers and deployers that will deliver public protections.

A systematic literature review of business-oriented literature identified many concerns about negative impacts of the AIA on innovation, summarised as being premature regulation, excessive scope, ambiguous expression, unclear requirements, incompatibility with existing regulatory regimes, and onerous compliance obligations[68]. On the contrary, the findings of the analysis in the present article suggest that compliance obligations will be readily avoided by the large majority of providers and deployers of AI systems.

The negative impacts are far more likely to arise from time and effort expended in order to understand and exploit the loopholes, and from the failure of the EU and its member-nations to exercise control over harmful impacts, leading to public distrust, thereby creating the risk of public backlash, and of non-adoption and even abandonment of technologies which, with appropriate care, have benefits to offer.

The analysis presented above suggests that, contrary to the hopeful tone of many authors, the dysfunctionality of the AIA as a regulatory instrument is deeply embedded in terminology and definitions, and in structures, processes and convoluted expressions. Attempts to adapt individual elements of the regimes in order to deliver effective protections would be piecemeal and pointless. The more appropriate approach is to treat the AIA as a promotional tool for dangerous technologies, with bureaucratic camouflage obscuring its ineffectiveness until, in due course, empirical evidence has been gathered to enable re-examination of analyses such as that in the present article.

A recent worldwide survey of AI sentiment concluded that "There is a strong public mandate for AI regulation, with 70% believing regulation is necessary. However, only 43% believe current laws are adequate. The analysis in this paper suggests that even such a high level of optimism was unwarranted. People expect international laws (76%), national government regulation (69%), and co-regulation with industry (71%)"[69]. So the question needs to be addressed about what can be done about the situation.

An approach is available, whereby a far better balance between macro-economic and human interests could be achieved, and reasonable protections against harmful impacts and implications could be devised that constrain business and government only to the extent justifiable. By adopting this approach, the risks of non-adoption, backlash, luddite behaviour by disaffected publics, and negative return on AI investment could all be greatly reduced.

---

68 Fanny Vainionpaa, et al. 'A Review of Challenges and Critiques of the European Artificial Intelligence Act (AIA)' Proc. Int'l Conf. Infor. Syst., 2023, 14, at https://oulurepo.oulu.fi/bitstream/handle/10024/47651/nbnfioulu-202402061598.pdf

69 Nicole Gillespie, et al. 'Trust, atttudes and use of artificial intelligence: A global study' The University of Melbourne and KPMG, 29 April 2025 <https://doi.org/10.26188/2882291, p.5.

"Co-Regulation ... refers to a regulatory model in which [all] stakeholders have significant input to a set of requirements, and even draft them, but do so within a statutory context that exercises control over the process, and makes the requirements enforceable[70]. A useful term to distinguish such instruments from mere industry codes is 'Statutory Codes'. Elements [of] Formal Regulation are essential, to establish generic legal protections. ... Co-regulation can also be the most effective approach in dealing with the ravages of specific technologies, particularly during a technology's early years of dynamism and opacity"[71]. A fuller description of co-regulation, in that case with its focus on Internet privacy, is available[72], as is a specific proposal for a co-regulatory approach to AI[73].

The AIA embodies some of the trappings of a co-regulatory scheme, but falls far short of fulfilling the requirements[74]. In particular, the objectives have a strong focus on industry economics, with broader economic and social interests relegated to constraints; and the power-balance among participants in code processes is very heavily weighted in favour of providers, and of private and public sector user organisations.

It has been argued that an element of the co-regulatory approach is embedded in the AIA, in the form of codes of practice, and that it would be beneficial for that code mechanism to be further developed. An important distinction has also been drawn between codes of practice under Arts. 56, plus 53-4 and 55, and (voluntary) codes of conduct under Art.95[75]:

> *... codes of practice may be regarded as instruments of meta-regulation that are truly embedded in the Act, whereas codes of conduct are simply instruments for potential meta-regulation. As such, codes of practice will likely play a much more crucial role under the Act than will codes of conduct.*

This author's contention in this article is, on the other hand, that the evidence demonstrates that the AIA cannot, and will not, deliver the necessary protections for human interests. The failure to address public expectations undermines achievement of the EC's declared objectives: The AIA cannot assure investors, business and government of public acceptance of AI systems. Commentary on the AIA needs to mature beyond the early excitement about the possibility of effective structures, processes, obligations, enforcement, and hence public confidence and successful AI investments. The AIA needs to be seen in the cold, hard light of day, and its inherent inadequacies and impending failure recognised and factored into discussions about a constructive way ahead.

A far more appropriate solution may be found by shifting the focus away from both AI in general and GPIA in particular. The AIA is presaged on the assumption that the appropriate object of the regulatory regime is a technology. Many have expressed serious doubts about the appropriateness of putting particular technologies at the heart of regulatory regimes[76]. Other categories of objects include an industry-sector or -segment, a practice, an impact, an outcome and a profession. The AIA's definition of AI System, at

---

70 G. Hepburn 'Alternatives To Traditional Regulation' OECD Regulatory Policy Division, undated, apparently of 2006, at http://www.oecd.org/gov/regulatory-policy/42245468.pdf

71 Roger Clarke, 'A Comprehensive Framework for Regulatory Regimes as a Basis for Effective Privacy Protection' Proc. 14th Computers, Privacy and Data Protection Conference, Brussels, 27-29 January 2021 <http://rogerclarke.com/DV/RMPP.html>

72 Roger Clarke, 'Internet privacy concerns confirm the case for intervention' (1999) 42(2) *Communications of the ACM* 60-67 <https://doi.org/10.1145/293411.293475>.

73 Roger Clarke, 'Regulatory alternatives for AI' (2019) 35(4) *Computer Law & Security Review* 398-409 <https://doi.org/10.1016/j.clsr.2019.04.008>.

74 Roger Clarke, 'Regulatory regimes for disruptive IT: A framework for their design and evaluation' (2026) 60 *Computer Law & Security Review* 106231 <https://doi.org/10.1016/j.clsr.2025.106231>, Table 5.

75 Lee Bygrave and Rebecca Schmidt (2025) 'Regulating Non-High-Risk AI Systems under the EU's Artificial Intelligence Act, with Special Focus on the Role of Soft Law' University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2024-10, 29 January 2025, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4997886, p.1, pp.12-25.

Art. 3(1), when stripped of unhelpful verbiage, has its focus on "a machine-based system that ... infers ... how to generate ... decisions that can influence physical or virtual environments". Others[77] have argued that the focus should be both narrowed and broadened to "[any] system that generate[s] decisions that can influence physical or virtual environments", or in those authors' terms, all automated decision-making systems.

---

76 Lyria Bennett Moses, 'Regulating in the Face of Socio-Technical Change', in Roger Brownsword, Karen Yeung and Eloise Scotford, *Oxford Handbook of Law, Regulation and Technology* (Oxford University Press, 2017).

77 José-Miguel Bello y Villarino et al., 'Are We Regulating the Right Digital Systems? Testing Emerging Artificial Intelligence Frameworks against Real-World Public Sector Systems' (2025) 48(4) *University of New South Wales Law Journal* 1165-1195 <https://doi.org/10.53637/vrjl5367>.