RETHINKING THE LIST-BASED APPROACH TO HIGH-RISK SYSTEMS UNDER THE AI ACT

TIAGO SÉRGIO CABRAL*

In this article, I critically analyse the expedited procedure for amending the list of high-risk systems under the AI Act. I conclude that the expedited procedure, along with the list-based approach in general, are suboptimal solutions as they fail to safeguard two key objectives: (i) protection of individuals' fundamental rights; and (ii) legal certainty for businesses. The option of carrying out a revision of the legal instrument through the ordinary legislative procedure, while always a possibility, may be too slow for its purpose and its success is far from certain. As such, I argue: that a test-based approach would have been a better option to future-proof the AI Act; that its building blocks are already include in the AI Act; and that it would have been advantageous both for individuals and businesses.

1 INTRODUCTION

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')[1] is the first comprehensive sectorial regime focusing on artificial intelligence ('AI') in a major world economic bloc. In regulating AI, the AI Act opts for a risk-based approach, adapting its obligations in accordance with the risk that different AI systems/models represent to fundamental rights.[2]

Within the categories of AI systems/models established by the AI Act, high-risk systems were given particular focus by the EU's legislator, with Articles 6 to 49 of the AI Act (Chapter III) being focused on such systems.[3] When defining which systems should fit in this category, the legislator opted for a (double) list-based classification through Annexes I and III of the AI Act.[4]

---

* PhD Candidate at the University of Minho (Portugal) | Researcher at JusGov (Portugal) | Project Expert for the Portuguese team in the 'European Network on Digitalization and E-governance' (ENDE).

[1] For an overview of the process resulting in the approval of the AI Act and the evolution of this legal instrument through the legislative procedure, see Francesca Palmiotto, 'The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation' (2025) First View European Journal of Risk Regulation 1.

[2] See, European Commission, 'Artificial Intelligence – Q&As' <https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1683> accessed 18 January 2025.

[3] Bird&Bird, 'European Union Artificial Intelligence Act: A Guide' 22–34 <https://www.twobirds.com/-/media/new-website-content/pdfs/capabilities/artificial-intelligence/european-union-artificial-intelligence-act-guide.pdf> accessed 1 January 2025.

[4] 'EU AI Act: First Regulation on Artificial Intelligence' (Topics | European Parliament, 6 August 2023) <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence> accessed 16 January 2025; 'AI Act | Shaping Europe's Digital Future' (12 December 2024) <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> accessed 16 January 2025; 'Entry into Force of the European AI Regulation: The First Questions and Answers from the CNIL' <https://www.cnil.fr/en/entry-force-european-ai-regulation-first-questions-and-answers-cnil> accessed 16 January 2025; 'Understanding the EU AI Act' <https://www.hunton.com/insights/legal/eu-ai-act> accessed 16 January 2025.

This type of approach, while in theory better from a perspective of legal certainty for businesses, may not be flexible enough to ensure that the legislation is future-proof. In this article, I argue that the AI Act does not offer adequate solutions to review the list of high-risk systems currently established, which may represent an added risk to fundamental rights of individuals (particularly in an innovative field, such as AI) and that even the supposed benefits for legal certainty for businesses may become less clear if we consider the implementation of the AI Act's lists of high-risk systems.

2 HIGH-RISK AI SYSTEMS THROUGH THEIR INCLUSION IN EU PRODUCT SAFETY LEGISLATION

While not outright forbidden, like the AI uses included in Article 5 of the AI Act, the legislator still considered that high-risk systems require significant guardrails to mitigate the negative impacts for fundamental rights of individuals that the incorrect, negligent or improper use of these systems could have.[5] High-risk systems can be divided into two sub-categories, based on the source of their classification: (i) high-risk AI Systems through their inclusion in European Union ('EU') product safety legislation which we will analyse in this section; and (ii) high-risk AI Systems based on their direct identification in the AI Act which we will further delve into in the next section.[6]

Under Article 6(1) of the AI Act, an AI system will be considered as high-risk[7] when it is both (i) either intended to be used as a safety component[8] of a product or the AI system in itself is a product, covered by one of the legislative acts listed in the list of product safety legislation in Annex I of the AI Act; and (ii) the product for which the AI system is a safety component, or the AI system itself as a product, has to undergo a third-party conformity assessment procedure[9] with a view to its placing on the market or putting into service under one of the legislative acts referred to in Annex I. For the assessment of the level of risk of the product, it is not relevant whether the placing on the market or putting into service of the AI system takes place at the same time or independently from the product to which it is linked, if it is linked to any product.[10]

---

[5] In addition to prohibited AI uses (Article 5 of the AI Act) and high-risk AI systems (Article 6 of the AI Act), the AI Act also regulates AI systems subject to specific transparency requirements (Article 50 of the AI Act), general-purpose AI models. and general-purpose AI models with systemic risk (Article 51 and following of the AI Act).

[6] Regarding the regulation of high-risk AI systems and the obligations that are applicable. See, Nuno Sousa e Silva, 'The Artificial Intelligence Act: Critical Overview' (*SSRN*, 24 September 2024) <https://papers.ssrn.com/abstract=4937150> accessed 20 October 2024; Asress Adimi Gikay et al, 'High-Risk Artificial Intelligence Systems under the European Union's Artificial Intelligence Act: Systemic Flaws and Practical Challenges' (SSRN, 18 December 2023) <https://papers.ssrn.com/abstract=4621605> accessed 20 October 2024.

[7] For an overview of the rules applicable to the qualification and regulation of these systems, see Sousa e Silva (n 6); Guillaume Couneson, 'Commentary to Article 6' in Ceyhun Necati Pehlivan, Nikolaus Forgó and Peggy Valcke (eds), *The EU Artificial Intelligence (AI) act: a commentary* (Wolters Kluwer 2025).

[8] Under Article 3(14) of the AI Act a safety component is 'a component of a product or of an AI system which fulfils a safety function for that product or AI system, or the failure or malfunctioning of which endangers the health and safety of persons or property'.

[9] Eva Thelisson and Himanshu Verma, 'Conformity Assessment under the EU AI Act General Approach' (2024) 4 AI and Ethics 113.

[10] See, Arnoud Engelfriet, *The Annotated AI Act: Article-by-Article Analysis of European AI Legislation* (Ius Mentis 2024) 94–97; Guillaume Couneson, 'Commentary to Article 7' in Ceyhun Necati Pehlivan,

3 HIGH-RISK AI SYSTEMS BASED ON THEIR DIRECT IDENTIFICATION IN THE AI ACT

As explained above, Annex III of the AI Act sets down a number of systems, divided into 8 categories that are directly established as high-risk. These are:

Table 1

Type of System	Source
Biometrics, in so far as their use is permitted under relevant EU or national law	
Remote biometric identification systems. *This shall not include AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be.*	Annex III(1)(a)
AI systems intended to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics.	Annex III(1)(b)
AI systems intended to be used for emotion recognition.	Annex III(1)(c)
Critical infrastructure	
AI systems intended to be used as safety components in the management and operation of critical digital infrastructure and road traffic or in the supply of water, gas, heating or electricity.	Annex III(2)(a)
Education and vocational training	
AI systems intended to be used to determine access or admission or to assign natural persons to educational and vocational training institutions at all levels.	Annex III(3)(a)
AI systems intended to be used to evaluate learning outcomes, including when those outcomes are used to steer the learning process of natural persons in educational and vocational training institutions at all levels.	Annex III(3)(b)
AI systems intended to be used for the purpose of assessing the appropriate level of education that an individual will receive or will be able to access, in the context of or within educational and vocational training institutions at all levels.	Annex III(3)(c)
AI systems intended to be used for monitoring and detecting prohibited behaviour of students during tests in the context of or within educational and vocational training institutions at all levels.	Annex III(3)(d)
Employment, workers' management and access to self-employment	
AI systems intended to be used for the recruitment or selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications and to evaluate candidates.	Annex III(4)(a)

Nikolaus Forgó and Peggy Valcke (eds), The EU Artificial Intelligence (AI) act: a commentary (Wolters Kluwer 2025) 7.

Type of System	Source
AI systems intended to be used to make decisions affecting terms of work-related relationships, the promotion or termination of work-related contractual relationships, to allocate tasks based on individual behaviour or personal traits or characteristics or to monitor and evaluate the performance and behaviour of persons in such relationships	Annex III(4)(b)
Access to and enjoyment of essential private services and essential public services and benefits	
AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for essential public assistance benefits and services, including healthcare services, as well as to grant, reduce, revoke or reclaim such benefits and services.	Annex III(5)(a)
AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems used for the purpose of detecting financial fraud.[11]	Annex III(5)(b)
AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance	Annex III(5)(c)
AI systems intended to evaluate and classify emergency calls by natural persons or to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by police, firefighters and medical aid, as well as of emergency healthcare patient triage systems.	Annex III(5)(d)
Law enforcement, in so far as their use is permitted under relevant EU or national law	
AI systems intended to be used by or on behalf of law enforcement authorities, or by EU institutions, bodies, offices or agencies in support of law enforcement authorities or on their behalf to assess the risk of a natural person becoming the victim of criminal offences.	Annex III(6)(a)
AI systems intended to be used by or on behalf of law enforcement authorities or by EU institutions, bodies, offices or agencies in support of law enforcement authorities as polygraphs or similar tools.	Annex III(6)(b)
AI systems intended to be used by or on behalf of law enforcement authorities, or by EU institutions, bodies, offices or	Annex III(6)(c)

[11] Adding to the extensive existing regulation of this practice – see Joana Rita Sousa Covelo de Abreu, Diogo Morgado Rebelo and César Analide, 'O Mercado Único Digital e a "(Leigo)Ritmia" Da Pontuação de Crédito Na Era Da Inteligência Artificial' (2020) 2 Revista de Direito e Tecnologia 1; Francisco Andrade and Diogo Morgado Rebelo, 'Schufa's Case C-634/21 on ADM: The "Lenders" Quest' for GDPR-Friendly Scoring Has Not Been Settled Yet!' (*SSRN*, 2 July 2024) <https://papers.ssrn.com/abstract=4882806> accessed 19 January 2025; Alessandra Silveira, 'Automated Individual Decision-Making and Profiling [on Case C-634/21 - SCHUFA (Scoring)]' (2023) 8(2) UNIO – EU Law Journal 74.

Type of System	Source
agencies, in support of law enforcement authorities to evaluate the reliability of evidence in the course of the investigation or prosecution of criminal offences.	
AI systems intended to be used by law enforcement authorities or on their behalf or by EU institutions, bodies, offices or agencies in support of law enforcement authorities for assessing the risk of a natural person offending or re-offending not solely on the basis of the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680, or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups.	Annex III(6)(d)
AI systems intended to be used by or on behalf of law enforcement authorities or by EU institutions, bodies, offices or agencies in support of law enforcement authorities for the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of the detection, investigation or prosecution of criminal offences.	Annex III(6)(e)
Migration, asylum and border control management, in so far as their use is permitted under relevant EU or national law	
AI systems intended to be used by or on behalf of competent public authorities or by EU institutions, bodies, offices or agencies as polygraphs or similar tools.	Annex III(7)(a)
AI systems intended to be used by or on behalf of competent public authorities or by EU institutions, bodies, offices or agencies to assess a risk, including a security risk, a risk of irregular migration or a health risk, posed by a natural person who intends to enter or who has entered into the territory of a Member State.	Annex III(7)(b)
AI systems intended to be used by or on behalf of competent public authorities or by EU institutions, bodies, offices or agencies to assist competent public authorities for the examination of applications for asylum, visa or residence permits and for associated complaints with regard to the eligibility of the natural persons applying for a status, including related assessments of the reliability of evidence.	Annex III(7)(c)
AI systems intended to be used by or on behalf of competent public authorities, or by EU institutions, bodies, offices or agencies, in the context of migration, asylum or border control management, for the purpose of detecting, recognising or identifying natural persons, with the exception of the verification of travel documents.	Annex III(7)(d)
Administration of justice and democratic processes	
AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting	Annex III(8)(a)

Type of System	Source
facts and the law and in applying the law to a concrete set of facts or to be used in a similar way in alternative dispute resolution.[12]	
AI systems intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda. *This does not include AI systems to the output of which natural persons are not directly exposed, such as tools used to organise, optimise or structure political campaigns from an administrative or logistical point of view*	Annex III(8)(b)

4.1 THE PROCEDURE FOR INTRODUCING AMENDMENTS TO ANNEX III OF THE AI ACT

4.1[a] Description of the procedure to add or modify the list of high-risk AI systems

The AI Act allows for the introduction of amendments to Annex III by means of a delegated act[13] adopted by the European Commission (Article 7 of the AI Act)[14] and requires the European Commission to annually assess whether a revision of this annex is necessary (Article 112(1) of the AI Act).[15]

As per the rules of the AI Act, the European Commission can add or modify the list of high-risk systems under Annex III of the AI Act when two cumulative criteria are fulfilled:

a) the AI systems are intended to be used in any of the areas listed in Annex III; and

[12] Regarding the use of AI systems by judicial authorities and particularly courts, see, Joana Covelo De Abreu, 'The "Artificial Intelligence Act" Proposal on European e-Justice Domains Through the Lens of User-Focused, User-Friendly and Effective Judicial Protection Principles' in Henrique Sousa Antunes et al (eds), *Multidisciplinary Perspectives on Artificial Intelligence and the Law* (Springer International Publishing 2024); Tiago Sérgio Cabral, 'Inteligência Artificial e Atividade Judicial: Análise Das Principais Questões a Nível de Proteção de Dados Pessoais e o Futuro Regulamento Da União Europeia Sobre IA' in Ricardo Pedro and Paulo Caliendo (eds), *Inteligência artificial no contexto público: Portugal e Brasil* (Almedina 2023).

[13] About the rules and limitations governing delegated acts see Alina Kaczorowska-Ireland, *European Union Law* (4th edn, Routledge 2016) 160; Tiago Sérgio Cabral, 'A Short Guide to the Legislative Procedure in the European Union' (2020) 6 UNIO – EU Law Journal 161; Tiago Sérgio Cabral and Marília Frias, 'National Laws and Implementing Regulation 2019/947/EU' (VdA - Vieira de Almeida, Cabinet d'avocats) <https://www.vda.pt/fr/publications/insights/by-marilia-frias-tiago-sergio-cabral/21300/> accessed 20 October 2024.

[14] See also the text of Recital 52 stating that 'As regards stand-alone AI systems, namely high-risk AI systems other than those that are safety components of products, or that are themselves products, it is appropriate to classify them as high-risk if, in light of their intended purpose, they pose a high-risk of harm to the health and safety or the fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence and they are used in a number of specifically pre-defined areas specified in this Regulation. *The identification of those systems is based on the same methodology and criteria envisaged also for any future amendments of the list of high-risk AI systems that the European Commission should be empowered to adopt, via delegated acts, to take into account the rapid pace of technological development, as well as the potential changes in the use of AI systems*' (emphasis added).

[15] Until the end of the period of the delegation of power laid down in Article 97 of the AI Act. Additionally, by 2 August 2028 and every four years thereafter, the European Commission is required to evaluate and report to the European Parliament and to the Council, among others, the need for amendments extending existing area headings or adding new area headings in Annex III of the AI Act.

b) the AI systems pose a risk of harm to health and safety, or an adverse impact on fundamental rights, and that risk is equivalent to, or greater than, the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III.

Furthermore, the evaluation of the risk of harm to health and safety, or an adverse impact on fundamental rights and its seriousness should follow the detailed criteria established in Article 7(2) of the AI Act. These criteria seem, based on the wording and logic behind this provision, to be exhaustive.

4.1[b] Description of the procedure to suppress systems from the list of high-risk AI systems

Likewise, through a delegated Act, the European Commission may suppress AI systems from the list of high-risk AI systems in Annex III of the AI Act (Article 7(3) of the AI Act). To do so, the following cumulative criteria must be fulfilled:

a) the high-risk AI system concerned no longer poses any significant risks to fundamental rights, health or safety (in light of the same criteria used to evaluate the addition or modification of systems in the list); and
b) the deletion does not decrease the overall level of protection of health, safety and fundamental rights under EU law.

4.1. [c] Interplay between the procedure to amend Annex III under Article 7 of the AI Act and the procedure to amend the derogations to the high-risk classification under Articles 6(6-8 of the AI Act).

Article 6(6)-(8) of the AI Act also provides tools which allow the European Commission to, through delegated acts, exercise a degree of control over AI systems considered high-risk. While Article 7 achieves this through the addition, modification or suppression of AI systems considered high-risk under Annex III (as long as they are part of the areas listed in Annex III), Article 6(6)-(8) allow the European Commission to add, modify or suppress conditions for triggering the derogation to the general rule that AI systems included in Annex III of the AI Act will be considered high-risk[16] Aware of the interplay between both regimes, the European legislator goes as far as to establish that any amendments to the derogation regime should remain consistent with amendments to Annex III adopted under Article 7 [17]

Paragraphs 6 to 8 of Article 6 allow the European Commission to broaden or narrow the application of the high-risk regime to AI systems already included in Annex III by adding, amending or suppressing derogations. This may be useful if the European Commission concludes: (i) that certain specific applications of the AI systems in Annex III are facing

[16] According to Article 6(3) of the AI Act, an AI system referred to in Annex III shall not be considered to be high-risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making. This derogation should apply when: (i) the AI system is intended to perform a narrow procedural task; (ii) the AI system is intended to improve the result of a previously completed human activity; (iii) the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or
(iv) the AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III of the AI Act.
[17] See Article 6(8) of the AI Act.

regulatory overburden even though they do not pose a significant risk of harm to the health, safety or fundamental rights of natural persons and, thus, that it is necessary to add new derogations or amend existing derogations to exempt them; or (ii) that certain specific applications of the AI systems in Annex III currently benefiting from the derogations do, in fact, pose a significant risk of harm to the health, safety or fundamental rights of natural persons and, thus, that it is necessary to ensure they will be subject to the general rule by suppressing or amending existing derogations exempting the abovementioned AI systems.

There are, however, significant differences between Article 7 and paragraphs 6 to 8 of Article 6. . First, it is not possible to add new systems to Annex III based on paragraphs 6 to 8 of Article 6 even within the areas already in this Annex. Secondly, it is not possible to fully suppress AI systems from Annex III based on this regime.[18] Moreover, while Article 7 is limited by the eight areas in Annex III, the regime under paragraphs 6 to 8 of Article 6 is even more limited, as it can only affect the specific systems already included in Annex III. Article 7 is, hence, significantly broader, being a tool designed for more throughout changes to Annex III.

4.1[c] Why the procedure for introducing amendments in Annex III of the AI Act may not be fit for purpose

In essence, as explained above, Article 7 of the AI Act establishes an expedited procedure for introducing amendments to Annex III. The aim of this expedited procedure is to avoid the challenges of legislative interventions under the regular rules of the ordinary legislative procedure.[19]

The expedited procedure, which at its core has not changed much since the Commission's initial proposal,[20] does, however, have one very strong shortcoming: if a new system cannot be included in one of the eight areas currently in Annex III, the European Commission cannot intervene.[21] Therefore, a system that supports the use of AI in a new domain could remain unregulated[22] for an extended period of time, even if the seriousness of the risks and negative consequences it could bring to individuals is clear.

---

[18] Although, in theory, the European Commission could add new derogations or broaden the current derogations to a degree that it would result in a, de facto, suppression. Nonetheless, doing this would likely breach the consistency requirements under Article 6(8) and, if that were the aim, it would be wiser and more adequate to suppress the AI system from Annex III through Article 7(3).

[19] The EU AI Act where approved both under the Article 16 TFUE and Article 114 TFEU legal basis both subject to the ordinary legislative procedure. For more development on the legislative procedures in the EU, see Cabral, 'A Short Guide to the Legislative Procedure in the European Union' (n 13); Christilla Roederer-Rynning, 'Passage to Bicameralism: Lisbon's Ordinary Legislative Procedure at Ten' (2019) 17 Comparative European Politics 957; Justin Greenwood and Christilla Roederer-Rynning, 'Taming Trilogues: The EU's Law-Making Process in a Comparative Perspective' in Olivier Costa (ed), *The European Parliament in Times of EU Crisis* (Springer International Publishing 2019); Christilla Roederer-Rynning and Justin Greenwood, 'The Culture of Trilogues' (2015) 22(8) Journal of European Public Policy 1148.

[20] See Article 7 of the 2021 Commission proposal.

[21] Articles 6(6-8) also do not offer a solution as new systems cannot be added to Annex III under the rules for amending the derogations.

[22] At least in what concerns the AI Act, as it might still be subject to other EU legislation. See, inter alia, Giovanni Sartor, 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' (EPRS, 2020) <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf> accessed 30 October 2024; Magda Cocco et al, 'European Parliament Think Tank Study on the Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' (*VdA*, 30 June 2020)

In fact, in my opinion, the criticism of the lack of flexibility in the expedited procedure for revising Annex III could be extended to the list-based classification itself.

Under the current system established in the AI Act, if the legislator deems in the future that it must expand the scope of this legal instrument to further types of AI systems, it may rely on two options. The first option is the revision of the AI Act through a new legislative procedure and introduction of the system in Annex III. As well as being time-consuming and complex, this has the disadvantage of potentially reopening the entire law to new discussion.[23] A sub-option of this approach would be to conduct a targeted revision of Annex III when adopting another legal instrument. For example, if the EU was regulating a specific type of AI system through a separate legal instrument, it could also amend Annex III of the AI Act through this instrument to include the type of system being regulated in Annex III. There are some advantages to this approach, mainly that the likelihood of extensive amendments to the AI Act is lower.[24] However, it still depends on separate legislation and is a fairly complex process. Additionally, the legal instrument used to amend the AI Act should have a scope that is adequate for this purpose (i.e. unrelated legislation such as, for example, legislation about the financial sector would be inadequate).

The second hypothesis would be to either introduce changes in product safety legislation by: (i) expanding current product safety legislation already considered in Annex I

<https://www.lexology.com/library/detail.aspx?g=6f8813cf-0c7a-4a50-aa8e-20ccb48367bf> accessed 30 October 2024; Tiago Sérgio Cabral and Alessandra Silveira, 'Da Utilização de Inteligência Artificial Em Conformidade Com o RGPD: Breve Guia Para Responsáveis Pelo Tratamento' in Henrique Alves Pinto, Jefferson Carús Guedes, and Joaquim Portes De Cerqueira César, *Inteligência Artificial aplicada ao processo de tomada de decisões* (Editora D'Plácido 2020); Tiago Sérgio Cabral, 'Regulamento Sobre a Inteligência Artificial Na União Europeia : Potenciais Impactos Nas Entidades Públicas' (2021) 12 Revista de Direito Administrativo 89; Inês Neves, 'The EU Directive on Violence against Women and Domestic Violence – Fixing the Loopholes in the Artificial Intelligence Act' (*UNIO – EU Law Journal: The Official Blog*, 29 March 2024) <https://officialblogofunio.com/2024/03/29/the-eu-directive-on-violence-against-women-and-domestic-violence-fixing-the-loopholes-in-the-artificial-intelligence-act/> accessed 30 October 2024; CIPL, 'Artificial Intelligence and Data Protection How the GDPR Regulates AI' (*CIPL*, 12 March 2020) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf> accessed 4 January 2024; Diogo Morgado Rebelo and César Analide, 'Inteligência Artificial Na Era Data-Driven: A Lógica Fuzzy Das Aproximações Soft Computing e a Proibição de Sujeição a Decisões Tomadas Exclusivamente Com Base Na Exploração e Prospeção de Dados Pessoais' (2019) 6 Forum de Proteção de Dados 60.

[23] That is not to say that it is not possible to conduct very targeted amendments of EU legislation. See, for example, the recent amendment to the EU Cybersecurity Act which is intended introduce European certification schemes for managed security services. However, even in this case from the proposal to its approval more than one year and half passed. In addition, while it is certain that the European Commission could define the scope very narrowly to limit the amendments that can be introduced by the remaining institutions. After all, as clarified by Advocate General Tesauro in *Eurotunnel SA and Others v SeaFrance,* 'the amendments adopted [cannot[fall outside the scope of the measure in question, as defined by the proposal'. However, this in itself could raise issues, for example, by resulting in the other institutions voting the proposal down for not agreeing with its scope or, worst case scenario, introducing significant amendments and testing the limits of current case-law, bringing further uncertainty. Cabral, 'A Short Guide to the Legislative Procedure in the European Union' (n 13); Opinion of Advocate General Tesauro in Case
C-408/95 *Eurotunnel SA and Others v SeaFrance* EU:C:1997:250; Case C-408/95 *Eurotunnel SA and Others v SeaFrance* EU:C:1997:532; Case C-409/13 *Council v Commission* EU:C:2015:217.

[24] It would likely exceed the scope of the legal instrument as defined by the European Commission when presenting the proposal.

of the AI Act[25] to include the new type of system; or (ii) creating new product safety legislation and revising Annex I of the AI Act. In either case, this approach has strong limitations as it implies that the AI system is already subject or will become subject to product safety legislation, which could be difficult to implement and potentially costly/unnecessary for some systems.[26] In both cases, if a revision of the AI Act itself were necessary, it could degenerate into a full new discussion around the AI Act which would hinder legal certainty.[27]

4.1[d] A better system for defining high-risk systems under the AI Act

Considering the limitations of the procedure for introducing amendments in Annex III of the AI Act and of the list-based approach in general, the most appropriate approach to ensuring the protection of fundamental rights of individuals would be to establish a test to be carried out by providers, in which they would have to assess the level of risk of their system and, depending on the result, classify it as high-risk or not. Strictly speaking, the European legislator even established the fundamental rights impact assessment, which could probably have been adapted to this objective. That is, AI systems would be considered high-risk and subject to additional rules pursuant to the result of the fundamental rights impact assessment.[28] If the legislator wanted to guarantee that the AI systems currently

[25] To guarantee an efficient regulatory intervention Annex I.A. would be recommended.
[26] Option (ii) also shares the risk of reopening Annex III as explained above.
[27] The AI Act is required to carefully balance the protection of fundamental rights with the necessity to not hinder and, if possible, even foster, innovation. As argued by Manuel David Masseno, 'there is no real alternative to implementing public policies which centre on the data economy' (our translation) of which the current AI boom is one of the results. See, Manuel David Masseno, 'Entre dados e algoritmos: como a união europeia procura proteger os cidadãos-consumidores em tempos de inteligência artificial assente em big data' [2023] Revista do Direito 47. For more context around the AI Act some of its other issues, see also Tiago Sérgio Cabral, 'A proposta de Regulamento sobre a Inteligência Artificial na União Europeia: breve análise' in Joana Covelo de Abreu, Larissa Coelho, and Tiago Sérgio Cabral (eds), *O Contencioso da União Europeia e a cobrança transfronteiriça de créditos: compreendendo as soluções digitais à luz do paradigma da Justiça eletrónica europeia* (e-Justice, vol II (University of Minho 2021); Cabral, 'Regulamento Sobre a Inteligência Artificial Na União Europeia : Potenciais Impactos Nas Entidades Públicas' (n 22); Cabral, 'Regulamento Sobre a Inteligência Artificial Na União Europeia : Potenciais Impactos Nas Entidades Públicas' (n 22); Magda Cocco et al, 'Assessment List for Trustworthy AI & Inception Impact Assessment on the Requirements for AI' (*VdA*) <https://www.lexology.com/library/detail.aspx?g=be1686c3-8302-4263-b8f6-49ab7397e215> accessed 30 October 2024; Federica Paolucci, 'Shortcomings of the AI Act: Evaluating the New Standards to Ensure the Effective Protection of Fundamental Rights' (*Verfassungsblog*, 14 March 2024) <https://verfassungsblog.de/shortcomings-of-the-ai-act/> accessed 17 March 2024; Sousa e Silva (n 6); Marco Almada and Nicolas Petit, 'The EU AI Act: A Medley of Product Safety and Fundamental Rights?' (*SSRN*, 30 December 2022) <https://papers.ssrn.com/abstract=4308072> accessed 16 January 2025; Marco Almada and Anca Radu, 'The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy' (2024) 25(4) German Law Journal 646; Emre Kazim et al, 'Proposed EU AI Act – Presidency Compromise Text - Select Overview and Comment on the Changes to the Proposed Regulation' (*SSRN*, 6 April 2022) <https://papers.ssrn.com/abstract=4060220> accessed 16 January 2025.
[28] Under the General Data Protection Regulation's data protection impact assessment, whose logic seems to, at least partially inspire the fundamental rights impact assessment, controllers who are required to carry out a data protection impact assessment should use this exercise to implement measures designed to lower the risk of the data processing activity. If they are unable to do so at a satisfactory level, they will be required to consult the supervisory authority. See, WP29, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' <https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711> accessed 30 May 2024; Jens Ambrock and Moritz Karg, 'Commentary to Article 35' in Gerrit Hornung, Euangelos Papakōnstantinu, and Indra Spiecker Döhmann (eds), *General data protection regulation:*

included in Annex III would generally be considered high-risk, it would be enough to include a presumption, rebuttable only when the criteria of Article 6(3) of the AI Act are met.[29]

This would be, as I see it, a better approach from the perspective of protecting fundamental rights of individuals as it would avoid potentially allowing dangerous systems to remain outside of the scope of the AI Act for long periods of time. Additionally, and perhaps surprisingly, it is my conviction that this approach would also have advantages from a legal certainty for businesses perspective. For organizations with long development cycles, it is better to be able to conduct a test today and know if the system that they'll release to the public in a few years' time is likely to be considered as high-risk instead of releasing the system under the assumption that it is not going to be considered as high-risk, create some regulatory panic (as happened with general-purpose AI models)[30] and then have the legislator eventually impose additional requirements.[31] In short, the flexibility of the tests brings predictability and predictability tendentially is better for business.[32] All things considered, a closed list is much more likely to require amendments when faced with technological developments than a test designed to be flexible.[33] It is also important to note that businesses are likely to be in a better position to understand the likely risks of an AI systems at a relatively early stage of the development cycles in comparison to with the EU legislator which has to predict future risks based on extremely limited information.

---

article-by-article commentary (1st edn Nomos 2023) 35; Jens Ambrock and Moritz Karg, 'Commentary to Article 36' in Gerrit Hornung, Euangelos Papakōnstantinu, and Indra Spiecker Döhmann (eds), *General data protection regulation: article-by-article commentary* (1st edn, Nomos 2023) 35; Eleni Kosta, 'Commentary to Article 35' in Christopher Kuner, Lee A Bygrave, and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): a Commentary* (Oxford University Press 2020) 35; Cecilia Alvarez Rigaudias and Alessandro Spina, 'Commentary to Article 36' in Christopher Kuner, Lee A Bygrave, and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): a Commentary* (Oxford University Press 2020) 36; Lukas Feiler, Nikolaus Forgó and Michaela Nebel, *The EU General Data Protection Regulation (GDPR): A Commentary* (2nd edn, Globe Law and Business Ltd 2021) 177–187; Tiago Sérgio Cabral and Alessandra Silveira, 'Commentary to Article 8' in Tiago Sérgio Cabral et al, *The Charter of Fundamental Rights of the European Union: A Commentary* (UMINHO Law School / JusGov 2024) 8.

[29] I.e., when it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making as explained above.

[30] See, Isabel Kusche, 'Possible Harms of Artificial Intelligence and the EU AI Act: Fundamental Rights and Risk' [2024] Journal of Risk Research 1.

[31] Even if provisions are put in place to avoid retroactive application (see Article 111(2) of the AI Act), significant changes will probably be common for many systems, making the exemption to the application only temporary in many cases.

[32] Among the extensive scholarship conducted in this area see, inter alia, Jiwon Lee, David Schoenherr, and Jan Starmans, 'The Economics of Legal Uncertainty' (*SSRN*, 22 November 2022) <https://papers.ssrn.com/abstract=4276837> accessed 18 January 2025; Michał Krzykowski, Michał Mariański, and Jakub Zięty, 'Principle of Reasonable and Legitimate Expectations in International Law as a Premise for Investments in the Energy Sector' (2021) 21 International Environmental Agreements: Politics, Law and Economics 75; Aurelien Portuese, Orla Gough, and Joseph Tanega, 'The Principle of Legal Certainty as a Principle of Economic Efficiency' (2017) 44 European Journal of Law and Economics 131; Benny Hutahayan et al, 'Investment Decision, Legal Certainty and Its Determinant Factors: Evidence from the Indonesia Stock Exchange' (2024) 11 Cogent Business & Management 2332950.

[33] The data protection impact assessment is proving as a flexible tool to address concerns related to AI. See CNIL, 'AI Development Guidelines: Sheet 5 - Carrying out an Data Protection Impact Assessment If Necessary' (*CNIL*, 7 June 2024) <https://www.cnil.fr/en/carrying-out-protection-impact-assessment-if-necessary> accessed 10 June 2024.

While it might take time until the legislator finishes the legislative amendment, organizations cannot really predict what will be the result or content of the legislative intervention. In the case of general-purpose AI systems, the legislator created an entirely new category with specific rules and obligations. Not knowing what to expect is never a development or implementation friendly scenario.

Furthermore, in certain frontier cases, the test-based approach could also provide an incentive for providers – and deployers, within the limitations of their capabilities – to implement additional safeguards directed at lowering the risk to fundamental rights of their systems, with the aim of lowering it enough to guarantee that the system would not be considered as high-risk.

4 POSSIBLE OBJECTIONS AND IMPLEMENTATION

A possible objection to this position is that it would further empower providers of AI systems, granting them decision power regarding which systems should be considered as high-risk. This objection is, however, vulnerable to three counterarguments: (i) the introduction of a presumption of high-risk covering AI systems currently included in Annex III would be sufficient to guarantee that the level of protection would not be lower than what is currently achieved (as referred in subsection 4.1.5.); (ii) adequate cooperation with providers and enforcement would significantly reduce any such risk; and (iii) the current framework may contribute to provider inertia. Providers who apply closed rules and conclude that their AI system is not high-risk will be less likely to implement additional mitigation measures. By reinforcing provider accountability our position enables providers, who have more comprehensive knowledge of their AI systems, to take a more active participation in risk mitigation.

A further possible objection is that the proposed approach would limit the flexibility of the European Commission in adapting the AI Act to new challenges and technologies through the delegated acts referred to in Article 7, paragraphs 1 and 3 of the AI Act. This objection faces three key issues: (i) this flexibility does not exist in a satisfactory manner due to restriction to the eight areas currently in Annex III; (ii) if necessary, introducing an expedited procedure to amend the abovementioned presumptions would provide the European Commission with some degree of control over the assessment; (iii) soft-law could contribute to guide providers in the assessment possibly even avoiding the necessity of amending the presumptions. In any case, the assessment should be, as much as possible, designed to be future-proof to protect legal certainty.

A third objection to my position is that it would require an amendment to the AI Act and create exactly what it tries to avoid: legal uncertainty. There is some merit to this objection since, ideally, my position would have been adopted as part of the negotiations that resulted in the AI Act and be part of the law as entered into force on 1 August 2024.[34] Since that was not the case, there are two suboptimal scenarios: (i) amend the very recent AI Act; or (ii) maintain the list-based approach, at least for the time being, regardless of its shortcomings.

[34] With progressive application of its requirements starting with Chapter I and Chapter II from 2 February 2025.

Introducing amendments to the AI Act at this point in time would be highly damaging to the expectations of all entities involved in the AI value chain and possibly hinder AI development in the EU. As such, even though the current framework could be vastly improved I cannot defend its immediate amendment. However, it is important to note that Article 112 of the AI Act includes various moments for the evaluation and review of the current text. By 2 August 2028 and every four years thereafter, the European Commission must evaluate and report to the European Parliament and to the Council on, inter alia, the need for amendments extending the existing eight areas or adding new areas in Annex III [35]. These reviews can result in proposals to review the AI Act.[36] As such, I consider that, if in any of the abovementioned revisions the European Commission concludes that the current Annex III is no longer fit for purpose,[37] namely because the eight areas need to be extended or new areas added, it should opt to implement the approach proposed in this article instead of simply reviewing the eight areas under Annex III.

If our proposed approach were adopted , high-risk systems would be defined based on whether: (i) they are considered high-risk by the proposed assessment; or (ii) are considered high-risk based on Article 6(1) of the AI Act (see Section 3). The current list of high-risk systems under Annex III of the AI Act might not disappear but instead, if deemed necessary, serve as a presumption (i.e. systems included in this list would be presumed to be high-risk). Article 6(3) should then regulate the derogations to the application of the presumption, and Article 6(6)-(8) should regulate the rules applicable to the introduction of amendments to the conditions that must fulfilled to trigger the derogations to the presumption.

It is important to note that, while these reviews seem to be the ideal time to implement such a change, the same logic applies to any change to Annex III that requires reopening the AI Act. That is to say, and although this would be undesirable, if outside of the abovementioned review period the legislator considers it absolutely necessary to revise the AI Act to introduce new high-risk areas (e.g. due to the emergence of new types of AI systems), replacing the simple introduction of the new high-risk areas by the introduction of our proposed approach would be best.

[35] See Article 112(2)(a) of the AI Act.
[36] See Article 112(10) of the AI Act.
[37] These may happen in 2028 or in any of the revisions occurring frequently thereafter.

LIST OF REFERENCES

Adimi Gikay A et al, 'High-Risk Artificial Intelligence Systems under the European Union's Artificial Intelligence Act: Systemic Flaws and Practical Challenges' (SSRN, 18 December 2023) <https://papers.ssrn.com/abstract=4621605> accessed 20 October 2024
DOI: https://doi.org/10.2139/ssrn.4621605

Almada M and Petit N, 'The EU AI Act: A Medley of Product Safety and Fundamental Rights?' (*SSRN*, 30 December 2022) <https://papers.ssrn.com/abstract=4308072> accessed 16 January 2025
DOI: https://doi.org/10.2139/ssrn.4308072

Almada M and Radu A, 'The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy' (2024) 25(4) German Law Journal 646
DOI: https://doi.org/10.1017/glj.2023.108

Alvarez Rigaudias C and Spina A, 'Commentary to Article 36' in Kuner C, Bygrave LA, and Docksey C (eds), *The EU General Data Protection Regulation (GDPR): a Commentary* (Oxford University Press 2020)
DOI: https://doi.org/10.1093/oso/9780198826491.003.0073

Ambrock J and Karg M, 'Commentary to Article 35' in Hornung G, Papakōnstantinu E, and Spiecker Döhmann I (eds), *General data protection regulation: article-by-article commentary* (1st edn Nomos 2023)
DOI: https://doi.org/10.5771/9783845276984-687

— —, 'Commentary to Article 36' in Hornung G, Papakōnstantinu E, and Spiecker Döhmann I (eds), *General data protection regulation: article-by-article commentary* (1st edn, Nomos 2023)
DOI: https://doi.org/10.5771/9783845276984-706

Andrade F and Morgado Rebelo D, 'Schufa's Case C-634/21 on ADM: The "Lenders" Quest' for GDPR-Friendly Scoring Has Not Been Settled Yet!' (*SSRN*, 2 July 2024) <https://papers.ssrn.com/abstract=4882806> accessed 19 January 2025
DOI: https://doi.org/10.2139/ssrn.4882806

Cabral TS and Silveira A, 'Da Utilização de Inteligência Artificial Em Conformidade Com o RGPD: Breve Guia Para Responsáveis Pelo Tratamento' in Alves Pinto H, Carús Guedes J, and Portes De Cerqueira César J, *Inteligência Artificial aplicada ao processo de tomada de decisões* (Editora D'Plácido 2020)

— —, 'Commentary to Article 8' in Cabral TS et al, *The Charter of Fundamental Rights of the European Union: A Commentary* (UMINHO Law School / JusGov 2024)

Cabral TS, 'A Short Guide to the Legislative Procedure in the European Union' (2020) 6 UNIO – EU Law Journal 161
DOI: https://doi.org/10.21814/unio.6.1.2711

— —, 'A proposta de Regulamento sobre a Inteligência Artificial na União Europeia: breve análise' in Covelo de Abreu J, Coelho L, and Cabral TS (eds), *O Contencioso da União Europeia e a cobrança transfronteiriça de créditos: compreendendo as soluções digitais à luz do paradigma da Justiça eletrónica europeia* (e-Justice, vol II (University of Minho 2021)

— —, 'Inteligência Artificial e Atividade Judicial: Análise Das Principais Questões a Nível de Proteção de Dados Pessoais e o Futuro Regulamento Da União Europeia Sobre IA' in Pedro R and Caliendo P (eds), *Inteligência artificial no contexto público: Portugal e Brasil* (Almedina 2023)

— —, 'Regulamento Sobre a Inteligência Artificial Na União Europeia : Potenciais Impactos Nas Entidades Públicas' (2021) 12 Revista de Direito Administrativo 89

Couneson G, 'Commentary to Article 6' in Necati Pehlivan C, Forgó N and Valcke P (eds), *The EU Artificial Intelligence (AI) act: a commentary* (Wolters Kluwer 2025)

Couneson G, 'Commentary to Article 7' in Necati Pehlivan C, Forgó N and Valcke P (eds), The EU Artificial Intelligence (AI) act: a commentary (Wolters Kluwer 2025)

Covelo De Abreu J, 'The "Artificial Intelligence Act" Proposal on European e-Justice Domains Through the Lens of User-Focused, User-Friendly and Effective Judicial Protection Principles' in Sousa Antunes H et al (eds), *Multidisciplinary Perspectives on Artificial Intelligence and the Law* (Springer International Publishing 2024)
DOI: https://doi.org/10.1007/978-3-031-41264-6_21

Emre Kazim et al, 'Proposed EU AI Act – Presidency Compromise Text - Select Overview and Comment on the Changes to the Proposed Regulation' (*SSRN*, 6 April 2022) <https://papers.ssrn.com/abstract=4060220> accessed 16 January 2025
DOI: https://doi.org/10.2139/ssrn.4060220

Engelfriet A, *The Annotated AI Act: Article-by-Article Analysis of European AI Legislation* (Ius Mentis 2024)

Feiler L, Forgó N, and Nebel M, *The EU General Data Protection Regulation (GDPR): A Commentary* (2nd edn, Globe Law and Business Ltd 2021)

Greenwood J and Roederer-Rynning C, 'Taming Trilogues: The EU's Law-Making Process in a Comparative Perspective' in Olivier Costa (ed), *The European Parliament in Times of EU Crisis* (Springer International Publishing 2019)
DOI: https://doi.org/10.1007/978-3-319-97391-3_6

Hutahayan B et al, 'Investment Decision, Legal Certainty and Its Determinant Factors: Evidence from the Indonesia Stock Exchange' (2024) 11 Cogent Business & Management 2332950
DOI: https://doi.org/10.1080/23311975.2024.2332950

Kaczorowska-Ireland A, *European Union Law* (4th edn, Routledge 2016)
DOI: https://doi.org/10.4324/9781315561035

Kosta E, 'Commentary to Article 35' in Kuner C, Bygrave LA, and Docksey C (eds), *The EU General Data Protection Regulation (GDPR): a Commentary* (Oxford University Press 2020)
DOI: https://doi.org/10.1093/oso/9780198826491.003.0072

Krzykowski M, Mariański M, and Zięty J, 'Principle of Reasonable and Legitimate Expectations in International Law as a Premise for Investments in the Energy Sector' (2021) 21 International Environmental Agreements: Politics, Law and Economics 75
DOI: https://doi.org/10.1007/s10784-020-09471-x

Kusche I, 'Possible Harms of Artificial Intelligence and the EU AI Act: Fundamental Rights and Risk' [2024] Journal of Risk Research 1
DOI: https://doi.org/10.1080/13669877.2024.2350720

Lee J, Schoenherr D, and Starmans J, 'The Economics of Legal Uncertainty' (*SSRN*, 22 November 2022) <https://papers.ssrn.com/abstract=4276837> accessed 18 January 2025
DOI: https://doi.org/10.2139/ssrn.4276837

Masseno MD, 'Entre dados e algoritmos: como a união europeia procura proteger os cidadãos-consumidores em tempos de inteligência artificial assente em big data' [2023] Revista do Direito 47

Morgado Rebelo B and Analide C, 'Inteligência Artificial Na Era Data-Driven: A Lógica Fuzzy Das Aproximações Soft Computing e a Proibição de Sujeição a Decisões Tomadas Exclusivamente Com Base Na Exploração e Prospeção de Dados Pessoais' (2019) 6 Forum de Proteção de Dados 60

Portuese A, Gough O, and Tanega J, 'The Principle of Legal Certainty as a Principle of Economic Efficiency' (2017) 44 European Journal of Law and Economics 131
DOI: https://doi.org/10.1007/s10657-014-9435-2

Roederer-Rynning C, 'Passage to Bicameralism: Lisbon's Ordinary Legislative Procedure at Ten' (2019) 17 Comparative European Politics 957
DOI: https://doi.org/10.1057/s41295-018-0141-2

—— and Greenwood J, 'The Culture of Trilogues' (2015) 22(8) Journal of European Public Policy 1148
DOI: https://doi.org/10.1080/13501763.2014.992934

Silveira A, 'Automated Individual Decision-Making and Profiling [on Case C-634/21 - SCHUFA (Scoring)]' (2023) 8(2) UNIO – EU Law Journal 74
DOI: https://doi.org/10.21814/unio.8.2.4842

Sousa Covelo de Abreu JR, Morgado Rebelo D, and Analide C, 'O Mercado Único Digital e a "(Leigo)Ritmia" Da Pontuação de Crédito Na Era Da Inteligência Artificial' (2020) 2 Revista de Direito e Tecnologia 1

Sousa e Silva N, 'The Artificial Intelligence Act: Critical Overview' (*SSRN*, 24 September 2024) <https://papers.ssrn.com/abstract=4937150> accessed 20 October 2024
DOI: https://doi.org/10.2139/ssrn.4937150

Thelisson E and Verma H, 'Conformity Assessment under the EU AI Act General Approach' (2024) 4 AI and Ethics 113
DOI: https://doi.org/10.1007/s43681-023-00402-5