European Journal of Risk Regulation (2025), 1–16
doi:10.1017/err.2025.10024

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Technology Neutrality as a Way to Future-Proof Regulation: The Case of the Artificial Intelligence Act

Atte Ojanen[1,2]

[1]Demos Helsinki, Finland and [2]Department of Philosophy, Contemporary History and Political Science, University of Turku, Finland
Email: atte.ojanen@demoshelsinki.fi

Abstract

Technology neutrality is a guiding principle of the European Union's technology regulation, stating that legislation should not favour or discriminate against any particular technology, but rather focus on the effects or functions of technologies broadly. This article examines the principle as a way to future-proof regulation by allowing legislation to adapt to the changes in technology over time. Effects of technology neutrality have not been sufficiently analysed in the novel context of regulation of artificial intelligence, which arguably poses more significant societal risks than telecommunications, where the principle first evolved. To address this gap in research, this article analyses whether the technology neutral nature of the EU's Artificial Intelligence Act (AI Act) renders it more future-proof. It identifies three main factors that affect future-proofness of the AI Act in light of technology neutrality: definition of AI, the risk-based approach and its enforcement mechanisms. The findings indicate that the AI Act's deviations from technology neutrality, including specific provisions for general-purpose AI models significantly improved its scope and future-proofness. Thus, technology neutrality and future-proof regulation should not be treated synonymously, and strict adherence to neutrality may even obscure the political choices and democratic agency essential for AI regulation.

Keywords: AI Act; artificial intelligence; future-proof; risk regulation; technology neutrality

I. Introduction

The pace of technological change and its disruptive effects force policymakers to consider how technology can be governed in a more anticipatory and future-proof way. The well-known 'Collingridge dilemma'[1] demonstrates that technological innovations tend to outpace the ability of incremental laws to keep up. Impacts of technology cannot be easily predicted until its widespread deployment in society, at which point regulation is

[1] D Collingridge, *The Social Control of Technology* (New York, St Martin's Press 1982).

difficult.[2] This is squarely seen with regulation of artificial intelligence (AI) and its emerging risks, whether algorithmic bias, misuse or safety issues.[3]

One of the most prevalent principles underlying the regulation of technology is the principle of technology neutrality. Technology neutral regulation, while subject to multiple interpretations, generally focuses on effects of technologies in broader terms, rather than regulating the technology itself.[4] In other words, policymakers should not pick winners or discriminate between particular technologies, but leave these to competitive markets to determine.[5] Technology neutral regulation is generally expected to be future-proof by allowing the legislation to adapt to the changes in technology and its impacts over time, rather than being tied to specific, possibly obsolete technologies.[6] The principle is a foundational assumption underlying much of the EU regulation since the 1990s.

Despite its dominance, technology neutrality has remained an under-theorised concept and its potential to future-proof regulation has not been analysed in the emerging context of AI.[7] This gap is particularly pressing given that technology neutrality may be ill-suited for future-proof AI regulation, as emergent risks of AI – such as algorithmic biases and technological lock-in – arguably require precautionary regulatory measures rather than a neutral approach focused on competitive market dynamics. AI systems pose more substantial risks to fundamental rights than telecommunications, where the principle initially arose. Moreover, these emerging risks are not necessarily neutral in terms of AI technologies as the larger and more agentic AI models appear inherently riskier than others (see section II.2). As such, policy priorities like explainable AI systems might be at odds with purely technology neutral approaches.

To address the research gap, this article explores whether technology neutrality aids future-proof regulation in the context of AI, by qualitatively analysing the European Union's Artificial Intelligence Act (AI Act) and policy documents surrounding its drafting. I will explore the following research questions: (1) How does AI differ from previous contexts where technology neutrality has been applied such as telecommunications? (2) Is the AI Act technology neutral, and how is this neutrality framed in the policy discourse by different stakeholders? (3) To what extent does technology neutrality render the AI Act more future-proof in anticipating risks of AI systems? The analysis enables one to examine under what conditions the pursuit of technology neutrality might benefit or hinder future-proofing. I consider three main factors that affect future-proof regulation, namely the scope or openness of the regulatory framework, its capacity for risk anticipation and the institutional enforcement of it.[8] These factors directly translate to the definition of AI, the risk-based approach and enforcement mechanisms within the AI Act, all of which are affected by technology neutrality. By emphasising the risks of AI, this analysis

[2] Ibid.

[3] See Y Bengio and Others, "International AI Safety Report" (2025) UK Department for Science, Innovation and Technology, DSIT 2025/001.

[4] BA Greenberg, "Rethinking Technology Neutrality" (2015) 100 Minnesota Law Review 1495; CJ Craig, "Technological Neutrality: Recalibrating Copyright in the Information Age" (2016) 17 (2) Theoretical Inquiries in Law 601.

[5] BJ Koops, "Should ICT Regulation Be Technology-Neutral?" in B-J Koops and Others (eds), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners, IT & Law Series* 9th edn, (The Hague, TMC Asser Press 2006) 77.

[6] Ibid; P Ohm, "The Argument Against Technology-Neutral Surveillance Laws" (2010) 88 Texas Law Review 1685.

[7] E Puhakainen and KE Väyrynen, "The Benefits and Challenges of Technology Neutral Regulation: A Scoping Review" (2021) PACIS 2021 Proceedings 48. Available at https://aisel.aisnet.org/pacis2021/48/.

[8] See N Divissenko, "Regulation of Crypto-Assets in the EU: Future-Proofing the Regulation of Innovation in Digital Finance" (2023) European Papers 665; PI Colomo, "Future-Proof Regulation Against the Test of Time: The Evolution of European Telecommunications Regulation" (2022) 42 (4) Oxford Journal of Legal Studies 1170.

complements prior literature, which has predominantly focused on the benefits of technology neutrality for facilitating future innovations.

The second section gives a brief historical overview of the principle of technology neutrality and its relation to future-proof regulation. It also contrasts the risks of AI with telecommunications as a regulatory context where the principle initially emerged. Based on this, the third section presents the AI Act as a case for examining how the principle of technology neutrality affects future-proofness of regulation in practice. By examining nine documents following a policy framing approach, I unpack how different stakeholders have framed the contested principle and its relation to the AI Act, including its definition of AI, risk-based approach and enforcement mechanisms. The results indicate that while technology neutrality can be beneficial for regulatory flexibility and anticipation of risks, dogmatic adherence to it can also obscure the political choices and democratic participation central to AI regulation. In fact, the AI Act's departures from technology neutrality, such as specific provisions for general-purpose AI models appear to benefit its future-proofness, as noted in the conclusion. Overall, the findings highlight a tension between democratic governance and future-proofing, which often necessitates delegating some regulatory discretion to technocratic bodies.

II. Background

1. *Principle of technology neutrality*

Technology neutrality has become a key regulatory principle in the EU since the late 1990s, further reinforced by the emphasis on digital policy over the past decade. Technology neutrality stands for regulating the use and consequences of technology rather than the technology itself.[9] The law should not name or describe a particular technology, but rather utilise terms that encompass a broader array of possible technologies.[10] As such, the same regulatory principles should apply regardless of the technology used, without specifying technological means to achieve a given objective or picking winning technologies in a discriminatory fashion.[11] The principle is motivated by how technological change can challenge regulation in four ways: (a) need for new laws to ban, restrict or encourage an emerging technology; (b) uncertainty over how existing laws classify and apply to new technologies, (c) over-inclusive or under-inclusive scope of laws; and (d) obsolescence of existing legal rules.[12] A typical example of a technology neutral regulation is an emissions trading system that incentives reduction of carbon emissions without specifying the means to do so.[13]

A key justification for technology neutrality is that it ensures that the regulation is flexible and future-proof to respond to the pace of technological change, without becoming obsolete, distorted or counterproductive. As noted by Puhakainen and Väyrynen,[14] the notion of technology neutrality is closely connected to future-proof regulation, which seeks to make legislation adaptive to technological changes by introducing a degree of flexibility to the regulation. For example, the EU's Better

[9] Koops, *supra*, n 5; Greenberg, *supra*, n 4.

[10] M Birnhack, "Reverse Engineering Informational Privacy Law" (2012) 15 Yale Journal of Law & Technology 24.

[11] W Maxwell and M Bourreau, "Technology Neutrality in Internet, Telecoms and Data Protection Regulation" (2015) 21 (1) Computer and Telecommunications Law Review 1.

[12] LB Moses, "Recurring Dilemmas: The Law's Race to Keep up with Technological Change" (2007) 2 University of Illinois Journal of Law, Technology & Policy 239, 276.

[13] V Djakonoff and Others, 'Teknologianeutraliteetti ja yhteiskunnan strategiset tavoitteet tutkimus- ja innovaatiopolitiikassa' [Technology Neutrality and Society's Strategic Objectives in Research and Innovation Policy] (2024) 2024 Publications of the Government's Analysis, Assessment and Research Activities 12.

[14] Puhakainen and Väyrynen, *supra*, n 7.

Regulation Toolbox includes technology neutrality as a regulatory design instrument within the umbrella of "flexibility and future-proofing."[15] In other words, neutrality should help the regulation stand the test of time without the need for frequent revisions.[16] Technology neutrality can future-proof law in at least two senses.[17] First, technology neutral regulation should have a better longevity than easily outdated technology specific legislation and thereby lessen the need for revisions or new laws. Secondly, technology neutrality can facilitate future technological innovations, reducing the chance of the regulation becoming obsolete or counterproductive. Since it is challenging for the regulator to predict adoption of emerging technologies, technology neutrality allows for market-based flexibility in policies.[18] While interrelated, the main focus of this article is the first interpretation of future-proofness as longevity of regulation.[19]

There are multiple instruments by which regulation can be rendered more technology neutral and thereby potentially more future-proof. Generally, this involves drafting regulation in more general and vague terms, with emphasis on broad characteristics such as purpose and function of technologies.[20] More concretely, future-proofing might mean utilising open-ended norms, goal-based regulation and experimental legislation, along with future-oriented impact assessments.[21] Technology neutral and future-proof regulation usually entails delegating more power to standardisation bodies, agencies and courts for interpreting the more vague legislative provisions and enforcing them in practice. Koops[22] also includes multi-level legislation, teleological interpretation and sunset clauses as approaches for implementing technology neutral regulation. Moreover, regulatory sandboxes and technology foresight (including horizon scanning, scenarios, trends analysis) can aid future-proofness of regulation by better anticipating technological development.

However, the pursuit of regulatory flexibility through these instruments is not without drawbacks. A key trade-off is often the reduced legal certainty. This aligns with broader challenges associated with technology neutrality identified by Puhakainen and Väyrynen[23] in their scoping review, such as its ambiguous application, lack of a theoretical basis, enforcement costs and potential misuse by regulators. As such, technology neutrality is subject to contextual and even contradictory interpretations depending on how expansively it is formulated.[24] The principle is arguably subject to different levels of abstraction: technology neutrality primarily functions on a high-level of abstraction in lawmaking, whereas implementation of regulation tends to be more technology specific[25] by necessity.[26] The issue then becomes how the principle is operationalised in pursuit of certain goals, such as future-proofing.

[15] European Commission, "Better Regulation Toolbox" (2023) 176, available at https://commission.europa.eu/law/law-making-process/better-regulation/better-regulation-guidelines-and-toolbox_en

[16] See J Harasta, "Trust by Discrimination: Technology-Specific Regulation & Explainable AI" (2018) 2018 XAILA 2018 Proceedings at JURIX 2; Colomo, *supra*, n 8.

[17] C Reed, "Taking Sides on Technology Neutrality" (2007) 4 SCRIPTed 263, 268.

[18] See Koops, *supra*, n 5; Colomo, *supra*, n 8.

[19] These two perspectives have opposing motives: longevity view aims to expand regulation to new contexts, whereas innovation view seeks to restrict its scope. One can also draw different distinctions about the benefits of technology neutrality. See Puhakainen and Väyrynen, *supra*, n 7; Koops, *supra*, n 5; Greenberg, *supra*, n 4.

[20] Koops, *supra*, n 5; Ohm, *supra*, n 6.

[21] See S Ranchordás and MS van't Schip, "Future-Proofing Legislation for the Digital Age" in S Ranchordas and Y Roznai (eds), *Time, Law, and Change: An Interdisciplinary Study* (Oxford, Hart Publishing Ltd 2020) 347.

[22] Koops, *supra*, n 5; 23–26.

[23] Puhakainen and Väyrynen, *supra*, n 7.

[24] Harasta, *supra*, n 16; Craig, *supra*, n 4.

[25] For example, transparency and explainability requirements for AI systems can be dependent on the specific machine learning algorithms utilised.

[26] See Moses, *supra*, n 12; Birnhack, *supra*, n 10, 49.

2. From telecommunications to AI

The current technological landscape, characterised by AI, is different from the one in which the principle of technology neutrality initially emerged. This raises questions as to whether the principle is still a sound regulatory principle in the light of advanced AI systems. The principle of technology neutrality was first enacted in the EU in the context of telecommunications through Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services. In the regulation technology neutrality was operationalised through minimal intervention, emphasising competitive market outcomes and non-discrimination between competing networks.[27] The legislation explicitly cautions against regulating emerging telecommunication markets and assumes that the sector will be gradually deregulated due to effective competition. To its credit, the regulatory framework for electronic communications has largely managed to adapt to the sector's technological transformations due to its technology neutral approach. Yet, even in this case the commitment to neutral and future-proof principles has waned over time within the EU legislature.[28] Indeed, the hegemonic standing of technology neutrality has come under more criticism in recent years both by scholars and policymakers.[29] Policy priorities like trustworthy AI systems can require technology specific regulation or subsidies, whereas staunch commitment to technology neutrality might inadvertently maintain unsustainable and outdated technological infrastructure due to market incentives.[30] AI and previous technological contexts like telecommunications are also subject to other differences, outlined below.

First, the role of AI as a general-purpose technology is not facilitative but constitutive in nature, unlike telecommunication which has a clear intended purpose for facilitating communication. AI systems actively shape and redefine social activities and economic structures, affecting fundamental rights in contexts like health care, education and the justice system. Consequently, AI regulation is intrinsically tied to value-laden political choices,[31] concerning fairness, autonomy and power, rather than about operational concerns like network service disruptions typical of telecommunications. Yet, technology neutrality can mask such normative considerations by delegating democratic decisions to market competition. Second, technical architecture and size of AI models directly affects their capabilities and associated risks. Specifically, larger models can exhibit emergent, unpredictable behaviour – capabilities or outcomes not explicitly programmed – making their societal risks difficult to anticipate and govern.[32] These emergent capabilities mean that AI systems can effectively transcend their intended purpose or function, posing issues for purely technology neutral regulation designed for telecommunications. Given these new technological affordances, one cannot assume that treating AI "neutrally" will produce equivalent legal outcomes as with previous technologies.[33] Third, AI can give rise to more significant path dependencies and lock-in effects in terms of social values and harms, going beyond the market-based interoperability concerns in telecommunications. Machine learning is based on extrapolation of existing social patterns into future predictions through data, therefore potentially reinforcing

[27] Colomo, *supra*, n 8, 1175.

[28] Ibid.

[29] Puhakainen and Väyrynen, *supra*, n 7.

[30] Djakonoff and Others, *supra*, n 13.

[31] See M Veale and F Zuiderveen Borgesius, "Demystifying the Draft EU Artificial Intelligence Act" (2021) 22 (4) Computer Law Review International 97.

[32] Bengio and Others, *supra*, n 3, 52.

[33] CJ Craig, "The AI-Copyright Challenge: Tech-Neutrality, Authorship, and the Public Interest" in R Abbot (ed), *Research Handbook on Intellectual Property and Artificial Intelligence* (Cheltenham and Northampton, MA, Edward Elgar Publishing 2022) 134, 141.

discriminatory biases across society.[34] Counterintuitively, technology neutral regulation can exacerbate such lock-in effects by favouring dominant technological infrastructure.[35]

While the differences above should not be overstated, AI does appear to present more emergent risks to fundamental rights that necessitate precautionary and preventive regulatory measures. Moreover, Liu and others warn that reactive, temporary and domain-specific approach – often qualities of technology neutrality – to AI regulation is problematic because: (i) it misconstrues actual severity of AI risks; (ii) treats symptoms of AI rather than the structural causes; (iii) limits anticipatory policies; (iv) overlooks overarching risks of AI; and (v) is ineffective due to rapid technological change.[36] To avoid a regulatory game of a whack-a-mole, future-proof regulation of AI requires more explicit focus on anticipation of emerging risks, which are not necessarily neutral in terms of technology. The above discrepancies in technological contexts call into question whether strict adherence to technology neutrality is compatible with future-proof regulation of AI. Hence, in the next section I will examine whether the AI Act's supposed technology neutrality makes it more future-proof in practice, especially in terms of risk governance.

III. AI Act as a case: translating technology neutrality to future-proofness

This section examines how future-proof the European Union's Artificial Intelligence Act[37] is as a case of technology neutral regulation by examining its definition of AI, risk-based approach and implementation. I will argue that while the principle of technology neutrality is generally a valuable starting point for future-proof AI regulation, the two should not be viewed as synonymous or necessarily aligned with each other. I shall qualitatively analyse how the technology neutral nature of the AI Act affects its future-proofness based on nine policy documents, including the final Act, that all explicitly refer to technology neutrality and/or future-proofness, following the method outlined by Bowen.[38] In doing so, the article also examines how the documents frame technology neutrality and its relationship with future-proofness to identify common narratives, following a policy framing[39] approach: do they articulate the two as the same, how is the purpose of technology neutrality framed, and how is it legitimised? This allows one to better examine influential rhetorical frames, conflicting interpretations and justifications offered for technology neutrality in connection to future-proofness by different stakeholders, such as EU institutions, AI industry and civil society. The documents included in the analysis are listed in the Table 1.

Having come into force in August 2024, the AI Act is the EU's framework for regulation of AI, which seeks to balance safety with innovation, two prominent goals of technology neutral and future-proof regulation. Building on the EU's regulatory strengths the AI Act is

[34] Bengio and Others, *supra*, n 3, 92.

[35] Djakonoff and Others, *supra*, n 13.

[36] HY Liu and Others, "Artificial Intelligence and Legal Disruption: A New Model for Analysis" (2020) 12 (2) Law, Innovation and Technology 205, 211–14.

[37] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

[38] G A Bowen, "Document Analysis as a Qualitative Research Method" (2009) 9 (2) Qualitative Research Journal 27.

[39] M Rein and D Schön, "Frame-Critical Policy Analysis and Frame-Reflective Policy Practice" (1996) 9 (1) Knowledge and Policy 85; C Bacchi, "Policy as Discourse: What Does It Mean? Where Does It Get Us?" (2000) 21 (1) Discourse: Studies in the Cultural Politics of Education 45.

Table 1. AI Act policy documents that reference future-proofness or technology neutrality

Document	Stakeholder
1. Final AI Act: Regulation (EU) 2024/1689	European Parliament and Council
2. Draft AI Act: COM/2021/206 final	European Commission
3. AI Act Q&A (2023; 2024[40])	European Commission
4. Third Draft of the General-Purpose AI Code of Practice (2025)	European AI Office and stakeholders
5. EU AI Act: first regulation on artificial intelligence (2023)	European Parliament
6. An innovation-friendly approach based on European values for the AI Act: Joint Non-paper by IT, FR & DE (2023)	Governments of Italy, France and Germany
7. The AI Act Should Be Technology-Neutral (Grady, 2023)	Center for Data Innovation
8. AI Act: Why Proposed Regulations Miss the Mark on Tech Neutrality and Risk-Based Control (2023)	DOT Europe, BSA, CCIA, Developers Alliance, eco & ITI
9. An EU Artificial Intelligence Act for Fundamental Rights: A Civil Society Statement (2021)	European Digital Rights, Access Now, Panoptykon Foundation, epicenter.works, AlgorithmWatch, European Disability Forum, Bits of Freedom, Fair Trials, PICUM & ANEC

fundamentally product legislation with certain fundamental rights protections to ensure AI systems placed on the EU market are safe for consumers. Based on the new legislative framework (NLF), it employs a risk-based approach, in which the level of regulation is dependent on the risks involved with different uses of AI systems. The European Commission's initial proposal from April 2021 already positioned the legislation as technology neutral and future-proof: *"The proposal sets a robust and flexible legal framework. On the one hand, it is comprehensive and future-proof in its fundamental regulatory choices, including the principle-based requirements that AI systems should comply with"* while adding that its objective is to *"create a legal framework that is innovation-friendly, future-proof and resilient to disruption."*[41]

Technology neutrality might initially appear at odds with regulation of "specific" technology like AI. However, AI is rather a collection of emerging technologies, covering different types of machine learning and logic-based approaches. Moreover, AI regulation can be technology neutral in a narrower sense, by regulating the application of the technology without dictating specific techniques or model details.[42] Indeed, the AI Act's approach to regulating risks of different use cases of AI is largely technology neutral by focusing on the functions of AI systems rather than their underlying technology. The European Commission explicitly links technology neutrality and future-proofness in the Q&A about the legislation: "*The AI Act sets result-oriented requirements and obligations but leaves the concrete technical solutions and operationalisation to industry-driven standards and*

[40] European Commission has published two Q&As, one dated December 12, 2023, and one August 1, 2024.

[41] European Commission, "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts" COM (2021) 206 final, explanatory memorandum 1.1 & 5.2.5.

[42] See W Buczynski and Others, "Hard Law and Soft Law Regulations of Artificial Intelligence in Investment Management" (2022) 24 Cambridge Yearbook of European Legal Studies 262.

codes of practice that are flexible to be adapted to different use cases and to enable new technological solutions."[43]

Based on the existing literature on future-proof regulation,[44] I examine three main factors that affect how future-proof the AI Act is, which technology neutrality can either aid or hinder. Specifically, Divissenko has identified two essential features of future-proof regulation.[45] First, the openness and scope of the regulatory perimeter to flexibly incorporate emerging technologies. This is intrinsically tied to the AI Act's technology neutral definition of AI which can be used to include emerging AI systems flexibly within its regulatory scope. However, I argue that the technology specific regulation of general-purpose AI models still managed to increase the AI Act's scope, without which it would have been outdated given the progress towards more general systems. Second, future-proofness is tied to the regulatory capacity for risk anticipation and addressing the changes in the amplitude and sources of risk. This is closely connected to the AI Act's risk-based approach, which is broadly technology neutral. Nevertheless, I find this technology neutral approach also delegates risk assessment to market forces through standardisation, which might limit its anticipatory capacity. I complement Divissenko's classification with a third feature of future-proof regulation: a lasting supervisory and enforcement structure for the regulation, as emphasised by Colomo.[46] I observe that the AI Act's governance framework supports its future-proofness by allowing flexible legislative amendments in response to technological change. Yet, concerns remain about the undemocratic nature of technology neutral regulation, such as constant amendments without parliamentary debate and ceding regulatory power to unrepresentative standardisation bodies. These three dimensions of future-proof regulation in the AI Act are covered below in light of the analysed policy documents.

1. Definition of AI

The AI Act's capacity to include future AI systems in its scope is intrinsically tied to how technologically neutrally it defines AI systems. Both the European Commission and Parliament advocated for a technology neutral, general definition of AI that is future-proof in the Act. The Commission's proposal for the regulation stated that *"The definition of AI system in the legal framework aims to be as technology neutral and future proof as possible, taking into account the fast technological and market developments related to AI."*[47] In adopting its negotiating position, the European Parliament added that it *"...wants to establish a technology-neutral, uniform definition for AI that could be applied to future AI systems."*[48] Aligned with the OECD's influential definition[49] of AI, the Article 3(1) of the AI Act defines AI systems as machine-based systems with varying levels of autonomy and adaptiveness that infer and generate outputs such as predictions, content, recommendations, or decisions, that can influence their environment after deployment. As such, it broadly covers machine

[43] European Commission, "Artificial Intelligence — Questions and Answers" (*Press Release*, 1 August 2024), available at https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1683 (last accessed 28 December 2024).

[44] See S Ranchordás and MS van't Schip, *supra*, n 21.

[45] Divissenko, *supra*, n 8.

[46] Colomo, *supra*, n 8.

[47] European Commission, *supra*, n 41, explanatory memorandum 5.2.1.

[48] European Parliament, "EU AI Act: First Regulation on Artificial Intelligence" (*Press Release*, 8 June 2023), available at https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (last accessed 28 December 2024).

[49] OECD, "Recommendation of the Council on Artificial Intelligence" (OECD/LEGAL/0449, 2019).

learning and logic- and knowledge-based approaches, while leaving certain simpler systems outside of its scope (Recital 12).[50]

The definition of AI systems was heavily debated during the drafting of the AI Act, with the European Council and AI industry advocating for a narrow, fixed definition based on machine learning to ensure legal certainty and ease regulatory burden.[51] For instance, the Center for Data Innovation claims that the AI Act violates the basic tenets of technology neutrality because *"Instead of addressing unique concerns about uninterpretable machine learning (ML) systems – a subset of AI systems – the Act would apply to a much broader set of AI systems that do not need regulatory intervention."*[52] It is unclear how this supposedly violates technology neutrality, especially as the AI Act primarily regulates certain high-risk AI systems. Such a critique appears to narrowly focus on neutral treatment between AI and other technologies, while disregarding how this forces one to discriminate between different AI technologies (e.g., machine learning versus symbolic reasoning). If one is concerned that the AI Act's broad definition of AI also covers systems that do not pose novel risks, then that appears a call for technology specific regulation, rather than neutrality. Indeed, proponents of the chosen broad approach argued that a narrow definition would have excluded many existing and future AI systems that pose risks to citizens' fundamental rights from the regulation's scope.[53]

The regulation of general-purpose AI (GPAI) models became a key test for the legislation's definition of AI after the rapid proliferation of large language models and generative AI, like ChatGPT, in late 2022. General-purpose models had not been considered in the original AI Act and their versatility across application domains invalidated the initial focus on only regulating specific use cases of AI. A political agreement was eventually reached on a tiered approach, where all general-purpose model providers have to provide transparent technical documentation, instructions, training summary and follow the Copyright Directive (Article 53(1)).[54] More stringent requirements apply to larger and more capable models that are presumed to pose systemic risk, trained with more than 10^25 FLOPs (Article 51(2)) of computing power (including model evaluations, adversarial testing, risk mitigation, incident reporting and cybersecurity protection as per Article 55(1)). This approach was initially opposed by France, Germany and Italy, who stated that a two-tier approach for GPAI (or foundation) models would violate the technology neutral nature of the AI Act and underlined that *"the AI Act regulates the application of AI and not the technology as such."*[55] Similarly, DOT Europe among other industry signatories expressed concern that regulation of GPAI systems is "*. . . not consistent with the AI Act's technology neutral risk-based approach, which regulates the use of AI systems according to risk, not the types of technology being used"*[56] implicitly arguing against

[50] See also European Commission, "Commission Guidelines on the Definition of An Artificial Intelligence System Established by Regulation (EU) 2024/1689 (AI Act)" C(2025) 924 final.

[51] N Kayser-Bril, "European Council and Commission in Agreement to Narrow the Scope of the AI Act" (*AlgorithmWatch*, 23 November 2021), available at https://algorithmwatch.org/en/eu-narrow-scope-of-ai-act/.

[52] P Grady, "The AI Act Should Be Technology-Neutral" (*Center for Data Innovation*, 2023), available at https://datainnovation.org/2023/01/the-ai-act-should-be-technology-neutral/.

[53] NA Smuha and Others, "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act" (2021), available at SSRN: https://doi.org/10.2139/ssrn.3899991; European Digital Rights (EDRi) and Others, "An EU Artificial Intelligence Act for Fundamental Rights: A Civil Society Statement" (2021), available at https://edri.org/our-work/civil-society-calls-on-the-eu-to-put-fundamental-rights-first-in-the-ai-act/.

[54] Although only the last two of these apply to open-source models.

[55] Governments of Italy, France and Germany, "An Innovation-Friendly Approach Based on European Values for the AI Act – Joint Non-Paper By IT, FR and DE" (2023), available at https://logistic-natives.com/wp-content/uploads/2023/11/9aaf68af_2128_4aa6_b8d6_a61212e5fd46_France_German_231122_140916.pdf.

[56] DOT Europe, "AI Act: Why Proposed Regulations Miss the Mark on Tech Neutrality and Risk-Based Control" (27 November 2023), available at https://doteurope.eu/news/ai-act-why-proposed-regulations-miss-the-mark-on-tech-neutrality-and-risk-based-control/ (last accessed 24 May 2024).

technology specific provisions even when faced with more systemic risks of general-purpose models (see section II.2).

Taken together, the broad and technology neutral definition of AI and the specific regulation of GPAI models both appear to render the AI Act more future-proof. The broad definition increases the scope and flexibility of the regulation to respond to technological progress. Simultaneously, the AI Act would have been severely outdated if it did not manage to specifically include GPAI models within its scope. The safety risks and societal impacts of GPAI models are not restricted to specific use cases, arguably necessitating earlier intervention during the development.[57] Even so, the uncertainties and emergent capabilities of such systems make predicting future applications and uses nearly impossible. The critics are right to point out that the provisions for general-purpose models and the FLOP threshold partly violate technology neutrality by regulating the potential risks of a specific subset of AI technologies more strictly. Nevertheless, the key here is that the explicit regulation of GPAI models broadened the scope of the AI Act by expanding its intended-purpose and use case approach to cover more general AI systems. This reduces the chance that certain AI systems or technologies escape the regulation, enhancing its future-proofness in terms of risk regulation. In other words, technology-specific interventions can complement future-proof regulation in so far as they expand its scope and flexibility, at least in the context of AI. As such, the issue for future-proofness is not technology neutrality *per se*, but whether its implementation expands or restricts the regulatory perimeter in response to technological development.

2. *Risk-based approach*

The AI Act's future-proofness is tied to its risk-based approach, which is designed to be technology neutral by focusing on potential risks of AI systems. Regulation of risks is by its nature future-oriented and involves accounting for uncertainty in the type of future harm, its likelihood and severity.[58] Accordingly, the AI Act is built on the distinction between different levels of risks in AI systems: minimal, limited, high and unacceptable, the last of which is prohibited outright (e.g., social scoring). These risk levels are predominantly use case and sector-based following a technology neutral approach. Systems with minimal risks, supposedly covering most AI systems in the market, remain largely unregulated, whereas limited risks systems (e.g., chatbots) only face basic transparency obligations towards the end-users (Article 50). At its core, the regulation targets high-risk AI systems – those posing significant threats to health, safety, or fundamental rights of individuals – which are subject to (self-)conformity assessments to gain access to the EU market (Article 6). High-risk systems include (i) AI systems in products already under EU health and safety harmonisation legislation, and (ii) standalone systems in critical areas listed in Annex III, such as education, law enforcement or migration, unless performing narrow procedural task without affecting decision-making (Article 6(3)).

Under the AI Act, high-risk AI systems must comply with essential requirements covering risk management system, technical documentation, data governance, human oversight, accuracy, robustness, and cybersecurity (Articles 9–15) to enter the market. However, the implementation of this seemingly neutral, risk-based framework reveals potential tensions with democratic and anticipatory practices. The AI Act outsources the crucial task of developing technical standards that operationalise the essential requirements to industry-driven European standardisation organisations (ESOs), namely CEN/

[57] Bengio and Others, *supra*, n 3.

[58] ME Kaminski, "Regulating the Risks of AI" (2023) 103 Boston University Law Review 1347.

CENELEC.[59] Providers of high-risk AI systems then demonstrate compliance with these harmonised standards, either through self-assessment or certification by private conformity assessment bodies, with limited public oversight. Entrusting opaque and private standardisation bodies to interpret the vague ethical and social requirements risks regulatory capture and violation of fundamental rights, and has already drawn criticism for conflicting with EU treaties.[60] Delegating regulatory authority is especially problematic given the social and value-laden nature of AI systems, where normative political decisions can be concealed in technocratic language.[61] Despite aiding regulatory flexibility, technology neutral standardisation can thereby result in a democratic deficit where crucial decisions about risks and safety occur outside accountable public processes. This industry dominance can also undermine the credibility of the AI risk assessment process itself, subvert the regulatory goals and hinder proactive risk anticipation and mitigation by AI companies. As noted by Divissenko, technology neutral frameworks tend to largely delegate risk assessment to the market actors and data they report, which can create perverse incentives to under-report risks, thereby hurting the anticipatory capacity of the regulation.[62]

The only explicit mention of future-proofness in the final AI Act links it to capacity for risk anticipation via mechanisms like regulatory sandboxes: *"To ensure a legal framework that promotes innovation, is future-proof and resilient to disruption, Member States should ensure that their national competent authorities establish at least one AI regulatory sandbox at national level to facilitate the development and testing of innovative AI systems under strict regulatory oversight before these systems are placed on the market or otherwise put into service."* (Recital 138). Regulatory sandboxes (Article 57) can help the anticipation of AI risks and co-evolution of regulation by allowing pre-deployment testing of AI systems in controlled environments. Although promising, this is also dependent on the rationale underlying the use of sandboxes, which are often dominated by fast market adoption rather than thorough risk mitigation. More centrally, the mandated risk management system for high-risk AI (Article 9(2)), though framed in general, technology-neutral language spanning the AI lifecycle, is inadequately anticipatory and precautionary. The legal requirements focus on identifying and mitigating "reasonably foreseeable risks" from both the intended use and misuse (Article 9(2)) and rely heavily on reactive post-market monitoring (Article 72) after AI systems are deployed.[63] When pre-deployment requirements exist, they are not particularly broad or binding, such as the fundamental rights impact assessments of potentially affected individuals for public service high-risk AI deployers (Article 27). This coupled with the lack of explicit technology foresight or forecasting mechanisms render the AI Act's technology neutral approach limited in anticipating more systemic and emergent AI risks.

In essence, while the AI Act's risk-based approach is by its nature future-oriented, its operationalisation through technology neutrality reveals significant tensions in terms of risk anticipation. The challenges detailed above, including the democratic deficits inherent to standardisation and the reactive risk management system focused on "foreseeable risks" restrict the future-proof potential of the AI Act's risk-based approach. These

[59] S de Vries, O Kanevskaia and R de Jager, "Internal Market 3.0: The Old 'New Approach' for Harmonising AI Regulation" (2023) 8 (2) European Papers-A Journal on Law and Integration 583, 596.

[60] Ibid., 608; Veale and Zuiderveen Borgesius, *supra*, n 31, 105; R Schmidt and C Scott, "Regulatory Discretion: Structuring Power in the Era of Regulatory Capitalism" (2021) 41 (3) Legal Studies 454.

[61] M Cantero Gamito and CT Marsden, "Artificial Intelligence Co-Regulation? The Role of Standards in the EU AI Act" (2024) 32 (1) International Journal of Law and Information Technology eaae011; H Fraser and Others, "Should Australia Follow Europe's Approach to AI Standards and Regulation?" (2025) 5 (1) ANU Journal of Law and Technology 96, 112–115; Veale and Zuiderveen Borgesius, *supra*, n 31.

[62] Divissenko, *supra*, n 8, 683.

[63] de Vries, Kanevskaia and de Jager, *supra*, n 59, 594.

https://doi.org/10.1017/err.2025.10024 Published online by Cambridge University Press

Table 2. Potential positive and negative impacts of technology neutrality on the future-proofness of the AI Act

Future-proof aspects in the AI Act	**1. Definition of AI:** *Openness and scope of the regulatory perimeter*	**2. Risk-based approach:** Regulatory capacity for risk anticipation	**3. Implementation and enforcement**: *Lasting governance structure*
	• *Prohibited AI practices, high-risk AI systems, GPAI models (Art 2, 5, 6, 51)*	• *Risk management, regulatory sandboxes (Art 9–27, 57–63)*	• *Delegated acts, AI Office, AI Board, national authorities, Codes of Practice (Art 56, 64–70, 97)*
Positive effects of technology neutrality	• Technology neutral definition of AI can flexibly incorporate new AI systems	• Risk regulation neutral by its nature, enables the assessment of future AI risks	• Capacity to review, amend and update the legislation
		• Regulatory sandboxes facilitate anticipatory testing of AI technologies	• Stakeholder and expert interaction through standards likely to aid regulation's flexibility
Negative effects of technology neutrality	• Narrow focus on intended purpose of AI systems, requiring exceptions for GPAI models	• Delegates power to private standard bodies, risking regulatory capture	• Standard-setting and legislative amendments without renewed legislative process undemocratic
	• Disregards qualities of specific AI technologies	• Risk management not adequately anticipatory, but based on market monitoring	

limitations are further exacerbated by the reliance on a pre-defined, static list of high-risk AI areas in Annex III, that restricts the regulation's flexibility, even if partly amendable.[64] This is especially so if some AI technologies, such as more agentic AI systems are taken to pose inherently greater systemic or emergent risks that transcend specific application domains. This means technology neutral and risk-based approaches can also diverge under certain circumstances.

3. Implementation and enforcement

Ultimately, how future-proof the AI Act proves to be depends on its implementation and enforcement, supported by the capacity to update the legislation through amendments and flexibility provided by standard-setting. Fundamental challenge for future-proof regulation is to ensure the continued political commitment of legislatures and institutions to the regulation.[65] AI Act's reliance on standards and guidelines (Article 96) emphasises the role of enforcement bodies in interpreting and implementing its technology neutral provisions. Most notably, the European AI Office is established within the European Commission as a central regulatory body to provide expertise and coordinate harmonised implementation and enforcement of the AI Act across member states (Article 64). Given sufficient resources, the AI Office should strengthen long-term commitment to the regulation, despite concerns about its limited autonomy within the Commission.[66] The AI Office also facilitates the drafting of the GPAI Codes of Practice (Article 56) that details the obligations for general-purpose AI model providers to demonstrate compliance with the AI Act, in collaboration with nearly 1000 stakeholders.[67] The third draft of the Codes of Practice names future-proofness as one of its guiding principles and underlines the importance of a *"balance between specific commitments on one hand, and the flexibility to update rapidly in light of technological and industry developments on the other."*[68] Indeed, the GPAI Codes of Practice includes more anticipatory risk assessments practices than the Article 9 despite its voluntary nature. Aside from national authorities[69] that are the main enforcers of the regulation, an AI Board, an AI Advisory Forum and a Scientific Panel are also established to bring a wider set of expert stakeholders from EU member states to guide the implementation of the Act (Articles 65–68), potentially aiding regulatory commitment and feasibility.

Importantly, the AI Act can be amended and updated through implementing and delegated acts (Article 97). This procedural flexibility is key to responding to technological change. For instance, new high-risk systems can be added to the list of high-risk AI application areas in Annex III, although only as long as they fall within the scope of the existing areas (Article 7(1)). The European Commission highlights amendments in connection to future-proofness in December 2023 version of AI Act Q&A: "*In addition, the AI Act can be amended by delegated and implementing acts, including to update the FLOP threshold*

[64] See M Ebers, "Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU's AI Act" (2024) European Journal of Risk Regulation 1, 9.

[65] Colomo, *supra*, n 8.

[66] See C Novelli and Others, "A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities" (2024) European Journal of Risk Regulation 1.

[67] European Commission, "General-Purpose AI Code of Practice" (30 April 2025), available at https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice (last accessed 24 May 2025).

[68] European Commission, "Third Draft of the General-Purpose AI Code of Practice" (11 March 2025), available at https://digital-strategy.ec.europa.eu/en/library/third-draft-general-purpose-ai-code-practice-published-written-independent-experts (last accessed 21 April 2025).

[69] Member states have to establish at least one notifying authority and one market surveillance authority (Art 70).

(delegated act), to add criteria for classifying the GPAI models as presenting systemic risks[70] *(delegated act), to amend modalities to establish regulatory sandboxes and elements of the real-world testing plan (implementing acts).*"[71] Delegated acts can also be issued to update the definition of AI, conformity assessment procedure and documentation requirements for high-risk and GPAI systems, but this flexibility also has its shortcomings. For example, civil society has criticised that the AI Act's future-proofness and capacity to respond to emerging risks for fundamental rights is compromised by how it "*provides no scope for updating 'unacceptable' (Art 5) and limited risk (Art 52 [sic]) lists.*"[72] These concerns were partly alleviated in the final regulation, as the Article 112 mandates the Commission to regularly evaluate and review the regulation to the Parliament and Council in light of technological advances. Annually, the need for amendments to the list of high-risk AI systems in Annex III and prohibited practices in Article 5 will be assessed, continuing with high-risk area headings, transparency measures (Article 50) and the governance system every four years.

Overall, the AI Act's governance framework, shaped by delegating power to enforcement and standardisation bodies in technology neutral fashion appears aligned with its future-proof implementation, even if some have criticised its overlapping and contradictory enforcement structures with other EU legislation.[73] The reliance on co-regulation is a general tendency in technology neutral regulation that empowers agencies like the European AI Office, regulated industries and courts (ultimately the CJEU) to interpret and apply the rules.[74] This likely aids the feasibility and flexibility of the Act by ensuring its implementation is informed by technical realities of AI. Most importantly, the multiple ways of amending the legislation along with periodic reviews should make the AI Act more future-proof by allowing it to flexibly adapt to rapid AI development. However, the broad capacity of the Commission to propose amendments through delegated acts without renewed legislative process and parliamentary oversight can also be seen as undemocratic, once again highlighting the tension between technology neutrality and democratic governance. Similar to standard-setting, amendments make the AI act more future-proof by increasing its regulatory flexibility but remain democratically problematic. Ohm[75] has argued that in many instances we want technology specific laws to ensure more regular democratic oversight and reconsideration of the legislation in parliaments. Sunset clauses that force periodic reassessment of regulation's effectiveness and relevance in response to technological development could be utilised to this end.[76] This suggests that in some instances technology specific regulation could better ensure democratic ends in future-proof AI regulation.

As seen with all the three aspects of future-proof regulation in the AI Act, technology neutrality can simultaneously both support and undermine future-proofness, as summarised in Table 2. While the principle of technology neutrality is generally valuable starting point for future-proof AI regulation, the two should not be viewed as synonymous or necessarily aligned with each other. This is despite the fact that technology neutrality has been framed as an essential tenet of the AI Act and largely synonymous with future-proofness in the analysed policy documents. Different stakeholders have supported the principle as a pretext for their interests without further defining it.[77] The discourse around

[70] Capacity to update the criteria for systemic risks is arguably important given emerging low-compute models such as DeepSeek-R1.

[71] European Commission, "Artificial Intelligence – Questions and Answers" (*Press Release*, 12 December 2023), available at https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1683 (last accessed 24 May 2024).

[72] European Digital Rights (EDRi) and Others, *supra*, n 53.

[73] Ebers, *supra*, n 64, 14.

[74] See R Crootof and BJ Ard, "Structuring Techlaw" (2021) 34 Harvard Journal of Law & Technology 347, 407; Birnhack, supra, n 10, 39; Cantero Gamito and Marsden, *supra*, n 61.

[75] Ohm, *supra*, n 6, 1686.

[76] Ibid., 1710; Koops, *supra*, n 5, 104.

[77] This reflects the concept's undertheorised nature; see Greenberg, *supra*, n 4; Puhakainen and Väyrynen, *supra*, n 7.

the AI Act reflects Reed's[78] two perspectives by which technology neutrality can enhance future-proofness: (a) improving regulatory longevity or (b) enabling technological innovations. While both policy framings can be components of future-proof regulation, they are motivated by different interests, leading to diverging interpretations. In the documents analysed, the AI industry predictably highlighted the latter perspective on efficient market competition whereas civil society stressed the former view on future-proofing the AI Act itself, especially in safeguarding fundamental rights. EU institutions appeared to balance between both views by leveraging instruments like regulatory sandboxes.

Yet even when technology neutrality aligns with future-proof regulation, the two can still come into conflict with democratic governance. The vague and flexible provisions of technology neutral legislation delegate power downwards to agencies and industry to interpret the law, at the expense of democratically elected representatives.[79] Given the potentially transformative societal impacts of AI and the associated risks, its regulation should not be purely a technical exercise, but requires greater democratic scope, deliberation and political steering.[80] Therefore, future-proof AI regulation cannot be restricted to paths already laid down by market-driven technological development in an undemocratic fashion. This can be a problem for technology neutral policies, which tend to be reactive and ineffective in changing or steering the technological environment itself, especially under the market and innovation interpretation. Despite its benefits for regulatory flexibility, strict adherence to technology neutrality can thereby obscure the democratic choices and agency central to AI regulation. Regulators can and should stress certain outcomes, such as risks of opaque AI systems to steer AI development towards socially and democratically acceptable directions, potentially violating strict technology neutrality.[81] This might entail a step away from the current AI paradigm, characterised by increasingly large and unexplainable neural networks. In essence, achieving the future-proof objectives of technology neutral law may sometimes require technology specific legislation.[82]

IV. Conclusion

This article has analysed the potential of technology neutrality to render regulation more future-proof in the context of the European AI Act. While technology neutrality is widely recognised as a key regulatory principle in the EU, its relationship with future-proof regulation is subject to different framings by stakeholders, ranging from facilitating market-based innovations to ensuring longevity of the regulation itself. I have argued that future-proof AI regulation requires more emphasis on societal risks compared to previous instances of technology neutral legislation like telecommunications. I identified three key issues that determine how future-proof the AI Act is: (i) its definition of AI, (ii) risk-based approach and (iii) institutional enforcement, analysing how technology neutrality affects these based on relevant policy documents. While technology neutrality can aid future-proof application of the AI Act with respect to all three dimensions, whether by incorporating new AI systems into its definition or through flexibility provided by standard-setting, it can also undermine it. For example, the technology specific provisions

[78] Reed, *supra*, n 27.

[79] See Veale and Zuiderveen Borgesius, *supra*, n 31, 106.

[80] A Buhmann and C Fieseler, "Deep Learning Meets Deep Democracy: Deliberative Governance and Responsible Innovation in Artificial Intelligence" (2023) 33 (1) Business Ethics Quarterly 146.

[81] See Harasta, *supra*, n 16.

[82] M Hildebrandt and L Tielemans, "Data Protection by Design and Technology Neutral Law" (2013) 29 (5) Computer Law & Security Review 509.

for GPAI models and their systemic risks greatly increased the scope of the regulation and thereby its future-proofness in terms of risk anticipation. As such, technology specific interventions can complement future-proof AI regulation by expanding its regulatory perimeter and flexibility. Hence, technology neutrality and future-proofness should not be viewed as synonymous despite the prevalence of such framings. Even when technology neutrality does appear aligned with future-proofness, it can still come into conflict with democratic governance central to AI regulation. This suggests that both technology neutral and specific provisions should be used as instruments for future-proof regulation of AI risks,[83] while still retaining democratic oversight.

The analysis of the AI Act underscores that the crucial issue for future-proofness is not technology neutrality *per se*, but whether its implementation broadens or narrows the scope of the regulation in light of technological progress. The extent to which neutrality contributes to future-proofness depends on contextual factors such as regulatory capacity, whether the regulation seeks to promote or restrict the technology and the specific risks at question.[84] From the perspective of future-proof regulation, technology neutrality should not be approached as a mere statutory drafting technique, but rather as property of the broader legal system to ensure that the normative objectives underpinning regulation are realised technology neutrally.[85] Given this context, the concern that regulators gradually depart from a technology neutral approach over time seems overstated.[86] As noted, technology neutrality mainly operates on a higher level of abstraction, and as AI systems and our understanding of them mature, the regulation should also become more specific. The AI Act as a case also cast doubt on the common claim that technology neutrality leads to overinclusive regulation enforcing unwanted objectives whereas specific legislation leads to underinclusion.[87] Ultimately, the *de jure* future-proofness of the AI Act is merely potential. Its actual resilience depends on *de facto* implementation and enforcement – factors highly vulnerable to the current deregulatory political climate, which may ultimately pose the greatest challenge to the AI Act enduring the test of time.

Financial support. This paper was supported by the KT4D project, which has received funding from the European Union's Horizon Europe program under grant agreement No 101094302.

Competing interests. The author declares none.

[83] See A Cordella and F Gualdi, "Regulating Generative AI: The Limits of Technology-Neutral Regulatory Frameworks. Insights from Italy's Intervention on ChatGPT" (2024) 41 Government Information Quarterly 101982.
[84] Birnhack, *supra*, n 10, 48.
[85] Moses, *supra*, n 12; Craig, *supra*, n 32.
[86] See Colomo, *supra*, n 8, who identifies this as a key issue.
[87] See e.g., Crootof and Ard, *supra*, n 74; Ohm, *supra*, n 6; Craig, *supra*, n 4, for this claim.

Cite this article: A Ojanen, "Technology Neutrality as a Way to Future-Proof Regulation: The Case of the Artificial Intelligence Act". *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2025.10024