European Journal of Risk Regulation (2025), 1–17
doi:10.1017/err.2025.10040

ARTICLE

Regulating Uncertainty: Governing General-Purpose AI Models and Systemic Risk

Samuel Carey

Department of Law, Stockholm University, Sweden
Email: samuel.carey@juridicum.su.se

Abstract

This article critically examines the concept of systemic risk as used in the EU Act in relation to General-Purpose AI Models (GPAIMs). It argues that rather than resolving uncertainty, the Act institutionalises it, transforming systemic risk into a flexible yet uncertain legal category. Drawing on legal theory and sociological perspectives – especially systems theory – this paper shows how systemic risk functions less as a concrete threshold for intervention and more as a proxy epistemic uncertainty surrounding GPAIMs. In the analysis, three interrelated consequences are identified: the institutionalisation of regulatory and scientific uncertainty, the delegation of key decisions about the content of systemic risk to private actors, and a regulatory blind spot created by the Act's conceptual distinction between AI models and AI systems. These developments risk undermining the Act's goal of legal certainty, exposing the paradox of AI governance: that in attempting to mitigate unknown future risks, the law may instead reproduce regulatory uncertainty.

Keywords: AI Act; general-purpose AI models; sociology of risk; systemic risk

I. Introduction

Modernity is characterised by its obsession with risk.[1] This obsession is clear in the discussion of potential harms associated with the development and deployment of General-Purpose AI Models (GPAIM), and especially those that exhibit systemic risk (GPAISR). Charles Perrow, in his study of risks of nuclear power claimed, "we have not given nuclear power generation systems enough time to express themselves … we are only just beginning to uncover the potential dangers that make any prediction of risk very uncertain."[2] A similar point might be made about artificial intelligence. The risks associate with AI, especially those posed by generative systems developed by OpenAI, Google and Anthropic, remain difficult to anticipate, precisely because these technologies have not yet had sufficient time to "express" themselves.

Despite this uncertainty, EU regulators have found themselves in a double-bind: the rapid entanglement of AI within multiple facets of society – seen variously as an

[1] N Luhmann, *Risk: A Sociological Theory* (Routledge 2002), p iiv. See also N Luhmann, "Technology, Environment and Social Risk: A Systems Perspective" (1990) 4 Industrial Crisis Quarterly 223. For an overview of the variety of classifications of risk, *see* O Renn, "Concepts of Risk: A Classification" in S Krimsky and D Golding (eds), *Social Theories of Risk* (Praeger 1992) pp 53–79. See further U Beck, *Risk Society: Towards a New Modernity* (Mark Ritter tr, Sage Publications 1992); A Giddens, "Risk and Responsibility" (1999) 62 Modern Law Review 1.

[2] C Perrow, *Normal Accidents: Living with High Risk Technologies* (Princeton University Press 2011) p 33.

opportunity for unprecedented progress and a source of risk to health, safety, and fundamental rights – leaves regulators and governments with little choice than to attempt to regulate AI's potential risk, despite having little consensus over how these risks will present themselves.[3] In this article, I intend to explore the effects created by the introduction of uncertainty inherent in the concept of systemic risk.

The AI Act is built upon the EU's New Legislative Framework, a regulatory framework traditionally applied to product safety regulation.[4] Despite its institutional pedigree, the AI Act extends beyond conventional product regulation, seeking to reconcile the imperatives of innovation, health, safety and fundamental rights protection, suggesting that the AI Act is a "hybrid regulatory framework" that combines two institutional traditions, product safety regulation and fundamental rights.[5] However, at its core, it is also a risk-based regulation.[6] The Act introduces a proportionate, risk-based framework that applies different regulatory burdens depending on the potential societal harm of AI applications.

The AI Act is also illustrative of a shift in technology regulation towards co-regulation, wherein legally binding obligations are combined with industry led standard-setting.[7] Co-regulation can be understood as the combination of public and non-public actors "intentionally and expressly share responsibility for the drafting and enforcement of rules".[8] While the AI Act provides overarching requirements, it leaves the development of technical standards, compliance mechanisms and risk assessment and management approaches largely to industry and expert bodies.[9] This approach mirrors other EU regulatory instruments, such as the General Data Protection Regulation (GDPR), which employs proactive data risk management. However, unlike the GDPR where risk analysis is not directly tied to the scope of application but rather to obligations imposed on data controllers, the AI Act's risk-based model determines which AI systems fall under regulatory scrutiny, and which ones do not.

[3] This double bind is often referred to as "The Pacing Problem". *See* Gary E Marchant, "The Growing Gap Between Emerging Technologies and the Law" in GE Marchant, BR Allenby and JR Herkert (eds), *The Gowing Gap Between Emerging Technologies and Legal Ethical Oversight: The Pacing Problem* (Springer Netherlands 2011) pp 19–33, 20.

[4] M Almada and N Petit, "The EU AI Act: Between the Rock of Product Safety and the Hard Place of Fundamental Rights" (2025) 62 Common Market Law Review 85.

[5] Ibid.

[6] J Black, "Constitutionalising Self-Regulation" (1996) 59 The Modern Law Review 24; J Black, "The Emergence of Risk-Based Regulation and the New Public Management in the United Kingdom" (2005) Public Law 512; J Black and R Baldwin, "Really Responsive Risk-Based Regulation" (2010) 32 Law & Policy 181; H Rothstein and Others, "The Risks of Risk-Based Regulation: Insights from the Environmental Policy Domain" (2006) 32 Environment International 1056; C Hood, *The Government of Risk: Understanding Risk Regulation Regimes* (Oxford University Press 2001).

[7] R Baldwin, M Cave and M Lodge, *Understanding Regulation: Theory, Strategy, and Practice* (2nd edn, Oxford University Press 2012) pp 146–7, where co-regulation can be differentiated from self-regulation insofar as it is a form of enforced self-regulation. It could also be described as a form of meta-regulation, where the AI Office is tasked with overseeing the risk management system, while delegating the risk control to private entities and corporations.

[8] DD Hirsch, "In Search of the Holy Grail: Achieving Global Privacy Rules through Sector-Based Codes of Conduct Symposium: The Second Wave of Global Privacy Protection" (2013) 74 Ohio State Law Journal 1045. See also J Black, "Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World" (2001) 54 Current Legal Problems 113–22.

[9] MC Gamito and CT Marsden, "Artificial Intelligence Co-Regulation? The Role of Standards in the EU AI Act" (2024) 32 International Journal of Law and Information Technology 1; T Goodman, "Thinking Outside the Technical Standardisation Box: The Role of Standards Under the Draft EU Artificial Intelligence Act" (2023) 9 LSE Law Review available at <https://lawreview.lse.ac.uk/articles/10.61315/lselr.579> (last accessed 30 October 2024); C Högberg, "Stabilizing Translucencies: Governing AI Transparency by Standardization" (2024) 11 Big Data & Society 20539517241234298; H Schapel, "The New Approach to the New Approach: The Juridification of Harmonized Standards in EU Law" (2013) 20 Maastricht Journal of European and Comparative Law 521.

https://doi.org/10.1017/err.2025.10040 Published online by Cambridge University Press

The release of ChatGPT in December 2022, almost two years after the European Commission's (the Commission) initial proposal of the AI Act, the EU's legislative processes encountered the fluidity and rapid evolution of technology in real time.[10] The introduction of publicly available large language models using transformer architecture,[11] combined with their ability to perform a diverse array of downstream tasks beyond its original training parameters, catalysed a reaction from the Commission.[12] The negotiations pivoted towards incorporating AI models described as "foundation models" or "frontier models".[13] While these negotiations went on, Open AI's ChatGPT became an increasingly popular service, with an estimated 100 million users by the end of 2023.[14] In the final version of the Act, the legislators settled on GPAIM as a catch all term for high powered models. Accordingly, these models, defined by their broad training data that is capable of being fine-tuned to a wide range of downstream tasks, were included within the Act, but separate from the sector specific high-risk systems, defined as *systemic risk.*[15] Accordingly, systemic risk was proposed to create a flexible, proactive approach to the regulation of GPAISR that is used as a benchmark for additional obligations on providers.[16] Some have suggested that the introduction of the category of general purpose-AI challenges the core logic of the Act, in particular its risk-based approach.[17]

In this paper, I argue that the AI Act's use of systemic risk generates more uncertainty than it resolves. In part, this is due to the complexity and uncertainty inherent in the concept *systemic risk.* In the context of the AI Act, this is amplified using systemic risk as a proxy for uncertainty about the potential impacts of GPAI, rather than as a rigorous or quantifiable category.[18] This lack of clarity, reflexively, produces unintended risks for the regulation and governance of AI. Following Ebers and Kusche. I argue that the AI Act's reliance on risk contributes to a sense of arbitrariness within the AI Act.[19] However, closer inspection of the concept of systemic risk and its hasty incorporation reveals further ambiguities and uncertainties. This paper argues that this uncertainty finds its expression in (at least) three ways. First, through institutionalising regulatory and epistemic uncertainty. Second, through the delegation of risk definition to model providers. Finally, the AI Act's distinction between GPAIM and systems create a regulatory blind spot, whereby systemic risk is acknowledged at the model level but insufficiently addressed at the system level, resulting in a paradox where systems that materialise systemic risk may evade meaningful oversight unless they fall within predefined high-risk categories. This all results in the notion of systemic risk being left as an open-ended and shifting category and

[10] M Coulter, "What Is the EU AI Act and When Will Regulation Come into Effect?" *Reuters* (7 December 2023) available at <https://www.reuters.com/technology/what-are-eus-landmark-ai-rules-2023-12-06/> (last accessed 8 November 2024).

[11] X Amatriain and Others, "Transformer Models: An Introduction and Catalog" (*arXiv*, 31 March 2024) available at <http://arxiv.org/abs/2302.07730> (last accessed 8 November 2024).

[12] N Helberger and N Diakopoulos, "ChatGPT and the AI Act" (2023) 12 Internet Policy Review available at <https://policyreview.info/essay/chatgpt-and-ai-act> (last accessed 29 September 2024).

[13] R Bommasani and Others, "On the Opportunities and Risks of Foundation Models".

[14] OJ Gstrein, N Haleem and A Zwitter, "General-Purpose AI Regulation and the European Union AI Act" (2024) 13 Internet Policy Review available at <https://policyreview.info/articles/analysis/general-purpose-ai-regulation-and-ai-act> (last accessed 8 November 2024).

[15] Ibid. See also B-C Pham and SR Davies, "What Problems Is the AI Act Solving? Technological Solutionism, Fundamental Rights, and Trustworthiness in European AI Policy" (2024) 0 Critical Policy Studies 1.

[16] Pham and Davies, *supra*, note 15.

[17] *Supra*, note 12.

[18] For discussion regarding uncertainty, technology and risk regulation, *see* M Weimer, "The Origins of 'Risk' as an Idea and the Future of Risk Regulation" (2017) 8 European Journal of Risk Regulation 10.

[19] 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; I Kusche, "Possible Harms of Artificial Intelligence and the EU AI Act: Fundamental Rights and Risk" (2024) 0 Journal of Risk Research 1, 10–11.

https://doi.org/10.1017/err.2025.10040 Published online by Cambridge University Press

undermines its own attempts at legal certainty,[20] deferring key risk assessments to private actors while providing thresholds that fail to provide clear prospective guidance. A larger conclusion can be drawn from this problem at the theoretical level, that attempts to regulate uncertain futures resulting in regulatory uncertainty.

Despite the uncertainty produced by systemic risk, this article does not suggest that GPAI should remain unregulated. Given the broad societal implications of these systems, regulation remains essential. Rather, the focus here is on the concept of systemic risk and its limitations as a legal category for addressing the potential harms posed by GPAI.

This paper proceeds in three parts. Firstly, I will lay some conceptual groundwork by unpacking the concept of systemic risk, drawing on the sociology of risk to show how the binary between systemic and non-systemic risk creates tensions, introduces arbitrariness, and deepens uncertainty. Second, I will outline legal mechanisms deployed by the AI Act and their potential shortcomings. Specifically, this section will discuss how these mechanisms attempt and fail to balance flexibility and adaptability, and systemic risk associated with GPAI. Focus is paid to computational thresholds, high impact capabilities, and the delegated powers of the Commission. Finally, I apply the insights from the previous section to argue that the supposed flexibility embedded within the AI Act's conception of systemic risk is ultimately constrained legal system's operational logic. Drawing on systems theory, this section highlights how the concept of systemic risk generates further uncertainty within the regulatory framework, and concludes with a reflection on the broader implications of this dynamic for the governance of transformative technologies such as GPAI.

II. The conceptualisation of systemic risk in the AI act

The near derailment of the AI Act by the introduction of applications such as ChatGPT, Claude, Gemini and Co-Pilot underscore the tension in regulating emerging technologies through risk and the concept of *systemic risk* is an important site of this tension. Systemic risk was incorporated into the AI Act at a late stage in the drafting processes and refers to, in terms of GPAISR, the risks linked to their "high-impact capabilities" which may have widespread consequences across the EU internal market.[21] These risk arise either from a model's broad influence or from the potential for actual harm they may cause to public health, safety, security, fundamental rights, and society at large. Additionally, these risks can spread throughout the entire AI ecosystem ("value chain"), thus amplifying their impact.[22] This section examines how systemic risk is defined both in the broader literature and in the AI Act, highlighting how the concept has changed through its incorporation into the AI Act. I use the notion of high-risk systems as a point of comparison for this discussion. Finally, drawing on sociological understandings of risk, I argue that systemic risk uncertainty is partly linked to how systemic risk is attributed.

Systemic risk is a catch-all term that refers to the increased interconnected, asymmetric and globalised nature of risks.[23] Although it is not entirely clear what systemic

[20] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act) [2024] OJ L168/1, Recital 97.

[21] Art. 3(65), AI Act.

[22] Ibid. Systemic risk is defined as "risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, security, fundamental rights, or society as a whole, that can be propagated at scale across the value chain."

[23] O Renn, "Systemic Risks: The New Kid on the Block" (2016) 58 Environment: Science and Policy for Sustainable Development 26.

https://doi.org/10.1017/err.2025.10040 Published online by Cambridge University Press

risk encapsulates,[24] and literature on the topic remains sparse to date,[25] the concept of systemic risk has a history of application within the financial sector, where it is often defined by the risk of cascading negative harm on the financial sector as a whole. Kaufman and Scott define financial systemic risk as "the risk or probability of breakdowns in an entire system, as opposed to breakdowns in individual parts or components, and is evidenced by co-movements (correlations) among most or all parts."[26] Financial systemic risk has even been European Parliament and Council as "a risk of disruption in the financial system with the potential to have serious negative consequences for the internal market and the real economy."[27] As a legal concept, it has also been recently introduced into the Digital Service Act – where it applies to very large online platforms and search engines.[28] Unlike in the AI Act, the Digital Service Act does not define systemic risk.

In its 2003 report *Emerging Systemic Risks in the 21st Century*, the Organisation for Economic Co-operation and Development (OECD) defines systemic risk as a risk that impacts critical social systems, including health, transportation, the environment and telecommunications.[29] (OECD report, 2003). The report identifies four potential motors of systemic risk; demographic, environmental, technological and socioeconomic.[30] Regarding technological systemic risk, three key aspects contribute to its development: (1) increased interconnectivity (2) the pace of technological change and (3) the shifts in the nature of technological risk.[31] In terms of connectedness, technologies ability to abbreviate the distance between individuals and organisation enable rapid response to potential dangers, while simultaneously amplifying their effects, noting that technological connectedness "multiplies the channels through which accidents, diseases or malevolent actions can propagate". An example of this is the development of international aviation (technology) that has both allowed for increased ability to respond and mobilise when disasters occur, but at the same time the abbreviation of society caused by aviation technology has allowed disasters and harms to disperse and multiply at higher rates, for example, the spread of COVID 19 during the pandemic.

When reduced to its primary properties, systemic risk can be understood as composed of four primary characteristics: complexity, uncertainty, ambiguity and ripple effects beyond the source of the risk.[32] Complexity refers to the struggle to both identify and subsequently quantify due to the "multitude of potential elements and specific adverse effects."[33] In other words, the potential harm of a systemic risk is made up of competing causal components that to varying degrees lead to its categorisation as systemic. Complexity is increased due to the globalised nature of systemic risk, as well as the interconnectivity of their causal structures.[34] Uncertainty refers to the indeterminacy of potential risks due to the variety of different components that make up the identification/measurement process. In a sense, uncertainty can be traced back to the competency and

[24] T Aven and O Renn, "Some Foundational Issues Related to Risk Governance and Different Types of Risks" (2020) 23 Journal of Risk Research 1121.

[25] O Renn and Others, "Systemic Risks from Different Perspectives" (2022) 42 Risk Analysis 1902, 1906.

[26] GG Kaufman and KE Scott, "What Is Systemic Risk, and Do Bank Regulators Retard or Contribute to It?" (2003) 7 The Independent Review 371, p 371.

[27] Regulation (EU) 1093/2010 of the European Parliament and the Council 2010.

[28] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), Article 33.

[29] Organisation for Economic Co-Operation and Development (ed), *Emerging Systemic Risks in the 21st Century: An Agenda for Action* (OECD 2003).

[30] Ibid, p 44.

[31] Ibid.

[32] Renn and Others, *supra*, note 25, 1904–5 See also A Klinke and O Renn, "Systemic Risks as Challenge for Policy Making in Risk Governance" (2006) 7 Forum Qualitative Sozialforschung/Forum: Qualitative Social Research available at <http://nbn-resolving.de/urn:nbn:de:0114-fqs0601330>.

[33] Ibid.

[34] *Supra*, note 23.

https://doi.org/10.1017/err.2025.10040 Published online by Cambridge University Press

success of certain scientific methods to extract the necessary knowledge based required assess the potential harm/dangers. This is what Renn refers to systemic risks as being "stochastic in their effect structure," meaning that it is hard to predict with precision the occurrence of events and their consequence that relate to a particular risk.[35] Ambiguity, unlike uncertainty, refers to the potential for interpretive differences between the results of scientific knowledge. Finally, ripple effects refer to secondary and tertiary consequences that can have effects on diverse social systems and domains.

The AI Act's conceptualisation of systemic risk departs from its use in the financial sector, where it refers to *endogenous* (internal) failures within the interconnected structures of financial institutions, instruments, and markets.[36] In the financial sector, systemic risk entails cascading failures caused by internal dependencies, where the collapse of one element disrupts the entire system. In contrast, the risks associated with GPAISR emanate both internally and externally. Despite systemic risks to critical infrastructure (for example, air traffic control, train networks, roads and bridges), many of the systemic risks posed by GPAIM refer to its interaction with the social environment in which it is deployed. Therefore, systemic risk in relation to GPAIM refers to both endogenous and *exogenous* (external) risk. This risk is exogenous as it is risk that emerges from how GPAIM's interacts with broader social systems and potential misalignment with societal norms and values.[37] This reconceptualisation of systemic risk widens the scope of risk significantly and shifts focuses from the internal dynamics of interconnected systems to the expansive societal impacts that GPAI potentially propagates.[38] For example, these risks may manifest in the erosion of democratic processes, the reinforcement of structural inequalities, or disruptions to critical sectors like healthcare and public infrastructure. According to Uuk et al., in their taxonomy of systemic risk in the AI Act, systemic risk has thirteen potential causes as well as fifty supporting factors.[39] Unlike systemic risk in financial markets which are well-documented (e.g., the 2008 subprime mortgage crisis)[40] – the systemic risks of GPAIM are speculative, diffuse, and embedded within the socio-technical landscape.[41]

In contrast to systemic risk, high-risk remains undefined. High-risk is neither defined in within Article 3, nor is it conceptually developed within the Recitals. Rather, high-risk AI systems are defined through its *function*: either by the integration into a product as a safety component,[42] a product covered by harmonised legislation in Annex I,[43] or is required to undergo third-party conformity assessment,[44] or the high-risk AI system is used in a

[35] Ibid.

[36] P Smaga, "The Concept of Systemic Risk" (8 August 2014) available at <https://papers.ssrn.com/abstract=2477928> (last accessed 11 November 2024); H Willke, E Becker and C Rostásy, *Systemic Risk: The Myth of Rational Finance and the Crisis of Democracy* (Campus Verlag 2013) available at <https://ezp.sub.su.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=844524&site=ehost-live&scope=site>.

[37] Kusche, *supra*, note 20, pp 10–11.

[38] Ibid.

[39] R Uuk and Others, "A Taxonomy of Systemic Risks from General-Purpose AI" (22 November 2024) available at <https://papers.ssrn.com/abstract=5030173>.

[40] See SL Schwarcz, "Markets, Systemic Risk, and the Subprime Mortgage Crisis" 61 SMU Law Review 209; A Hindmoor, "Systemic Risk Was the Real Culprit in the 2008 Financial Crisis and, with Banks Continuing to Borrow Huge Amounts, the Dangers Are Still There" (*British Politics and Policy at LSE*, 20 December 2013) available at <https://blogs.lse.ac.uk/politicsandpolicy/systemic-risk-was-the-real-culprit-in-the-2008-financial-crisis-and-with-banks-continuing-to-borrow-huge-amounts-the-dangers-are-still-there/> (last accessed 28 November 2024).

[41] J-P Fouque and JA Langsam (eds), *Handbook on Systemic Risk* (Cambridge University Press 2013) available at <https://www.cambridge.org/core/books/handbook-on-systemic-risk/8EA92559AF6649990E609A10A99E31E9> (last accessed 11 November 2024).

[42] Art. 6(1)(a), AI Act.

[43] Art. 6(1)(a), AI Act; cf Annex I.

[44] Art. 6(1)(b), AI Act.

https://doi.org/10.1017/err.2025.10040 Published online by Cambridge University Press

particular sector specified in Annex III.[45] The blending of differentiated conceptions of risk results in a confusing theoretical approach to how risk is dealt with in the Act. While the integration of AI into critical infrastructure or medical equipment presents tangible risk and thus quantifiable threats to life and safety, threats to democracy and fundamental rights are more abstract, diffuse and difficult to quantify in terms of risk assessment.

This result in the operationalisation of a dualistic understanding of risk within the AI Act, where risk is defined both by its function and its potential. Risk is often framed as the distinction between reality and possibility.[46] However, this seemingly straightforward definition belies the epistemological divergences that underpin its conceptualisation.[47] The dimensions that risk assumes are not neutral but contingent upon the epistemological commitments and theoretical perspectives that inform its interpretation. For instance, realist perspectives posit that risks are objective phenomena – real events "out there" that can be identified and managed with minimal interference from subjective or social influences. In this framework, the act of managing risks becomes an ostensibly technical exercise, divorced from the cultural or political context in which it occurs. Sociological perspectives, however, challenge the neutrality and universality of such claims, emphasising that risk is either sociocultural mediated or socially constructed.[48] Risk in this view merges through the communication and interaction of social actors, shaped by cultural norms, values and power structures. It is a phenomenon that reflects the dynamics of inclusion and exclusion, the privileging of certain epistemologies over others, and the often-unspoken assumptions embedded within regulatory and institutional frameworks.

Following Luhmann, risks are said to be negotiated through decisions.[49] These decisions in turn construct an organisation or a social system's perception of risk. Generally, risk is juxtaposed with the notion of safety, which turns on the idea that if the right decisions are made, a safe future can be ensured. However, the real distinction is between risk and danger.[50] Realist accounts often obscure the situated and contingent nature of risk by presenting it as a fixed and knowable entity, whereas sociological approaches highlight its constructed nature and the social, cultural, and political forces that render it visible.[51] Within legal frameworks, this tension manifests as competing demands for certainty and adaptability, with significant implications for the stabilisation – or destabilisation – of normative expectations. I argue that this causes two issues for the AI Act. First, it falsely attributes safety through the means of trustworthiness for those models that comply with systemic risk obligations. Second, the incorporation of systemic risk merely gives the appearance of regulatory action, while in reality leaving the determination of the actual existence and scope of such risks unresolved.[52]

[45] Art. 6(2), AI Act; cf. Annex III.

[46] JO Zinn, "Introduction: The Contribution of Sociology to the Discourse on Risk and Uncertainty" in JO Zinn (ed), *Social Theories of Risk and Uncertainty: An Introduction* (Blackwell Pub 2008) p 3.

[47] Ibid, pp 4–5.

[48] Ibid, pp 10–14.

[49] *Supra*, note 2, p 4, where Luhmann describes risk as a consequence of decisions:

> This brings to the foreground the question of who or what decides whether (and within which material and temporal contexts) a risk is to be taken into account or not. The already familiar discussions on risk calculation, risk perception, risk assessment and risk acceptance are now joined by the issue of selecting the risks to be considered or ignored.

[50] Ibid, pp 22–3.

[51] AJ Hatfield and KW Hipel, "Risk and Systems Theory" (2002) 22 Risk Analysis 1043, p 1048 where the authors disagreement about risk management and assessment can be traced back to a "implicit and undocumented value-based decisions".

[52] N Luhmann, *Ecological Communication* (Polity Press 1989) p 69.

https://doi.org/10.1017/err.2025.10040 Published online by Cambridge University Press

III. The identification of systemic risk in the AI act

Unlike the tiered classification of AI systems, the regulation of GPAIM instead employs binary classification: models either pose systemic risk or they do not. This shift abandons the central tenant of risk-based governance, particularly the proportionality of risk,[53] and replaces it with a blanket approach that relies on two mechanisms for determining systemic risk: *high-impact capabilities* and *computational thresholds*.[54] The Commission has attempted to embed flexibility into both these mechanisms via *ex officio* decisions (or based on qualified alert of the Science Panel) to determine high-impact capabilities and *delegated acts* that can be used to modify the former as well as the computational thresholds defined in Article 51(2).

Providers of models classified as systemic risk are required to undergo certain compliance duties, such as notifying the Commission without delay including information demonstrating that the requirement has been met. Those models presenting systemic risk that have not been notified to the Commission can be designated as systemic risky *ex officio* according to Article 52(1). At the same time, providers who have meet these thresholds may present arguments to the Commission as to why it should not be classified as systemic risk due to "specific characteristics."[55] The Act provides extensive documentation requirements for developers of GPAISR. First, developers need to publish technical documentation describing the data used for the training of the model. Second, providers are required to develop policies that allow them to comply with relevant copyright legislation. Third, they need to provide and make available technical documentation to those providers of an AI system that wish to integrate the model into their system. Finally, they need to be able to provide the above documentation on request to appointed national oversight authorities and the AI Office. Many of these obligations are already fulfilled by many developers: for example, many provide extensive documentation and detailed instructions.[56] At the same time, some have argued that these requirements remain vague and complex.[57]

1. High-impact capabilities

The first mechanism for identifying systemic risk in a model is its high-impact capabilities.[58] The capabilities of a model are considered high-impact where they "match or exceed the capabilities recorded in the most advanced general-purpose AI models."[59] Annex XIII provides further criteria for the determination of systemic risk due to high-impact capabilities, as well as some guidance on the "indicators and benchmarks." The Commission may determine high-impact capabilities *inter alia* a model's number of parameters, quality or size of its training data, quantity of computation used, input and output modalities, level of autonomy and scalability, reach in the internal market calculated through registered business users, and the number of registered end-users.[60] Parameters refer to the aspects of the model that are learned from the training data. The quality and size of data sets are to be determined through tokens, which refer to the atomisation of text into smaller, manageable parts for easier

[53] Ebers, *supra*, note, p 11.

[54] Art. 51(1)(a)–(b), AI Act.

[55] Art 52(2), AI Act.

[56] Gstrein, Haleem and Zwitter *supra*, note 14.

[57] Ibid.

[58] Art. 51(1)(a), AI Act.

[59] Art. 3(64), AI Act; See also Recital 111.

[60] Annex XIII, subsections (a)–(g), AI Act.

https://doi.org/10.1017/err.2025.10040 Published online by Cambridge University Press

machine processing.[61] Quantity of computing power used can be determined via its floating-points per second (FLOP) scores or "other variables" including the model's training time, cost, and energy consumption.[62] The modality of a model is determined by its potential functions – for example, text to text, or text to image, or speech to text, which is indicative of the type of deep learning methods used. The autonomy and scalability of a model refers to its ability to perform new, distinct tasks without additional training as well as its potential for integration with other tools. Finally, high impact may be determined through the number of registered business users (10000) or number of registered end-users (1000000) in the internal market. It is unclear whether these benchmarks and indicators are to be interpreted exhaustively or selectively, and if selectively, it does not provide any instruction as to how each indicator should be weighed against the other.

This determination is, paradoxically, only possible *post* the model being placed on the internal market or after developers interact with the model. Furthermore, this definition is recursive – high-impact capabilities are those that are higher than what they are now. Pre-emptive assessments of such capabilities are simply "approximations," emphasising the uncertain nature of these determinations.

2. Computational threshold

The nature of high-impact capabilities, reliant on approximations and post-hoc evaluations, stands in sharp contrast to the peremptory *computational threshold* imposed by Article 51(3). A GPAISR is presumed to pose systemic risk where the cumulative computation used for training the model exceeds a floating-point per second score (FLOP) of 10^25. Floating-point operations per second, or FLOP, is a measure of computational effort required for a model to perform a task. FLOPs are calculated by identifying the number of layers in a model, the types of operations performed at each layer and adding up all the FLOPS for each layer to compute the total FLOP count for a single pass forward. However, the level of computation being thrown at these models seems to be going beyond Moore's Law in the era of foundational models. Since 2010, computation effort has increased four times as fast over the past decade.[63] The Commission is empowered through delegated acts described in Article 51(3) to adjust and amend this threshold to reflect any potential shifts in computational training. However, given the rate of increase of compute power, these delegated acts will seemingly be used often.

The AI Act's threshold includes all computational instances used to enhance the model, including pre-training, synthetic data generation and fine-tuning.[64] This means that regardless of the potential high-impact capabilities, all GPAISR that breach this threshold are classified as systemic risk. As of 2025, the number of models that have exceeded this threshold are suggested to be around twenty-five models, all from private companies.[65] However, as of December 2024, a total of sixty-three models had a FLOP score of 10^24.

The use of computational thresholds for determining the capabilities of a model is controversial. While some have argued that computational thresholds insinuate a false

[61] SJ Mielke and Others, "Between Words and Characters: A Brief History of Open-Vocabulary Modelling and Tokenization in NLP" (*arXiv*, 20 December 2021) available at <http://arxiv.org/abs/2112.10508> (last accessed 25 September 2024).

[62] Discussed in Section II(2).

[63] J Sevilla, "Training Compute of Frontier AI Models Grows by 4–5x per Year" (*Epoch AI*, 28 May 2024) available at <https://epoch.ai/blog/training-compute-of-frontier-ai-models-grows-by-4-5x-per-year> (last accessed 28 November 2024).

[64] Recital 111, AI Act.

[65] *Supra*, note 63.

https://doi.org/10.1017/err.2025.10040 Published online by Cambridge University Press

equivalence between computational power and potential impact, essentially using computation as "a proxy for capabilities," others have argued that it serves as one tool in the potential governance toolbox.[66]

3. Delegated and implementing acts

Given how broad interpretive scope of high impact capabilities and the rigidity inherent in computational thresholds, the AI Act incorporates mechanisms designed to provide flexibility in response to technological developments. This flexibility is embodied in the Commission's implementation and authority to issue *delegated acts* as well as to make *ex officio decisions* to recalibrate the mechanisms for determining systemic risk.

According to Article 53, and in accordance with Article 97, the Commission can adopt *delegated acts* to amend and adapt the mechanisms of computational threshold and high impact capabilities. Delegated acts are provided for by Article 290 of the TFEU and allow the Commission to non-legislative acts to amend or supplement the non-essential elements of legislation.[67] These delegations can only be implemented under strict conditions – delegated acts, including that the delegated act cannot amend or change an essential element of the legislation.[68] Given the fast-evolving nature of technology, the use of delegated acts is unsurprising: as levels of computation rise and the impact of these technologies becomes more known, the AI Act wants to ensure that it is flexible to catch these emerging technologies. Delegated acts are prepared by the Commission based on dialogue between the Commission and national authorities, expert groups, research etc – however the precise processes involved remain ill defined.[69]

The use of delegated acts is not unusual in EU regulation, and the rationale for the use of delegated acts seems in line with the overall approach of adaptability and flexibility.[70] In accordance with Article 51(3), the Commission can adopt delegated acts to amend the high-impact capabilities and FLOP threshold described in paragraph 1 and 2 to keep up with technological development. Here, the Act is thinking specifically about the development of more efficient algorithms as well as hardware efficiency. In addition, the Commission can amend the benchmarks and indicators described in Annex XIII.[71] Essentially, the threshold limits provided by the FLOP score and the ambiguity of potential high impact capabilities can be amended and modified based on new state of the art. At the same time, the Commission can make decisions on the systemic risk of models on their own volition (ex officio) or based on advice from a qualified alert from the Scientific Panel of Independent Experts. Regarding the former, the AI Act allows for the establishment of a Scientific Panel support enforcement activities through an implemented act.[72]

[66] S Hooker, "On the Limitations of Compute Thresholds as a Governance Strategy" (*arXiv.org*, 8 July 2024) accessed 3 October 2024; D Fernández-Llorca and Others, "An Interdisciplinary Account of the Terminological Choices by EU Policymakers Ahead of the Final Agreement on the AI Act: AI System, General Purpose AI System, Foundation Model, and Generative AI" (2024) Artificial Intelligence and Law accessed 19 November 2024; M Pistillo and Others, "The Role of Compute Thresholds for AI Governance" (2025) 1 George Washington Journal of Law and Technology 26; L Heim and L Koessler, "Training Compute Thresholds: Features and Functions in AI Regulation" (*arXiv*, 6 August 2024) accessed 29 April 2025; G Sastry and Others, "Computing Power and the Governance of Artificial Intelligence" (*arXiv*, 13 February 2024) accessed 14 March 2025.

[67] T Christiansen and M Dobbels, "Non-Legislative Rule Making after the Lisbon Treaty: Implementing the New System of Comitology and Delegated Acts" (2013) 19 European Law Journal 42.

[68] Ibid. See also LA Campo, "Delegated versus Implementing Acts: How to Make the Right Choice?" (2021) 22 ERA Forum 193.

[69] *Supra*, note 67, pp 50–3.

[70] S Larsson, J Hildén and K Söderlund, "Implications of Regulating a Moving Target: Between Fixity and Flexibility in the EU AI Act" (April 09, 2025) *Law, Innovation and Technology* (forthcoming) available at <https://ssrn.com/abstract=5211101> pp 12–13.

[71] Art. 52(4), AI Act.

[72] Art. 68 and Art. 90, AI Act.

https://doi.org/10.1017/err.2025.10040 Published online by Cambridge University Press

IV. Uncertainty institutionalised: consequences of systemic risk in AI governance

So far, I have examined the uncertainty surrounding systemic risk in the AI Act and detailed how the AI Act attempts to detect and categorise it. In this section, I elaborate on the consequences of systemic risk's uncertainty, and I argue that the uncertainty produced by the AI Act gives rise to three primary issues. The first issue is what I have identified as the institutionalisation of uncertainty. Rather than eliminating uncertainty, the AI Act's introduction of systemic risk instead recognises and incorporates uncertainty within its rules and practices. I argue that this occurs on at least two different levels: scientific and regulatory. Second, the lack of certainty in the Act means that the responsibility for defining the nuances of systemic risk is delegated to private entities – which is itself a risk. Third, the distinction between AI Models and AI Systems is artificial and conceals the unity of systems and models, and that their interplay is important for the expression of systemic risk.

1. Uncertainty becomes normative: the institutionalisation of uncertainty

Institutionalised uncertainty, as I have conceptualised it, refers to uncertainty becoming a stable and normative part of the legal system. This section elaborates on how institutional uncertainty is caused through the incorporation of systemic risk within the AI Act on two different levels: scientific and regulatory. First, regarding the scientific level, systemic risk creates epistemic problems considering (i) the legal systems need to construct scientific knowledge within its own normative scheme and (ii) the AI Act's institutional heritage as a risk-based regulation. Risk-based regulation relies significantly on scientific expertise to provide boundaries of potential risks.[73] The novelty of GPAISR infers that science may not be in a "sufficiently advanced state" to provide satisfactory answers to the potential risks.[74]

King and Thornhill, drawing on Luhmann's system theory, present a parallel example of this issue, specifically drawing from the EU's environmental regulations.[75] To safeguard fishing stocks, the EU enacted regulation that stipulated the maximum mesh size permissible in fishing nets. This law was underpinned by the scientific premise that ensuring the survival of smaller fish during capture would prevent overfishing and habitat destruction. However, as it later transpired, scientific consensus shifted, and experts questioned the practice of catching larger fish over smaller ones. The removal of larger fish resulted in a diminished genetic stock that was more likely to breed and produce larger fish in the future. As it currently stands, the literature on the potential harms of GPAISR remain unclear and uncertain.

Another unexpected feature of the legal system's transformation of risks into norms is that the legal system must subsequently "discover" expert knowledge regarding this harm.[76] When it comes to systemic risk caused by AI Models, this is an entirely novel area that has been introduced through the political bargaining. To determine what systemic risk is, beyond the definitions of the Act and subsequent descriptions in the voluntary Codes of Practice, the operative organisations (such as courts, public authorities, and regulators) involved in decision-making processes will need to source and uncover potential experts in order to inform its own deliberations over what systemic risk is, and in particular how systemic risk may take shape in society given the use of AI Models. This knowledge is not passively perceived by the legal system, rather constructed by it, either

[73] Rothstein and Others, *supra*, note 6; Black and Baldwin, *supra*, note 6.
[74] Rothstein and Others, *supra*, note 6, p 1057.
[75] M King and C Thornhill, *Niklas Luhmann's Theory of Politics and Law* (Palgrave Macmillan UK 2003) p 200.
[76] Ibid.

https://doi.org/10.1017/err.2025.10040 Published online by Cambridge University Press

through its own self-reference or through the processes of seeking, validating and subsequently institutionalising new scientific claims.[77] At the same time, organisations affected by the requirements related to systemic risk will also need to distinguish and produce expertise in order to manage these risks.

The second issue relates to the institutionalisation of uncertainty at regulatory level. Black argues that risk-based regulation can be "paradoxical" as it operates on the premise that certain social complexities can be "rationalised, ordered, managed, and controlled."[78] While detailed rules and procedures are intended to provide certainty, their rigidity hinders regulators' ability to adapt to unforeseen and unpredictable futures.[79] Accordingly, the "inevitable inability to predict" becomes institutionalised within the regulatory framework. At the same time, the opposite is true: the less detailed the rules and procedures are, or the more these decisions are deferred and delegated, the more uncertainty is created, which inhibits not only the regulators' ability to adapt, but also those being regulated with the ability to anticipate. For example, in the case of the AI Act, the introduction of new categories of AI, such as ChatGPT and its derivatives, demonstrated how the rigid commitment to the risk-based regulatory framework inhibited the ability of the lawmakers to react and deal with emerging categories of technology.

Risk-based regulation operates on an implicit assumption of cause and effect; that certain actions today may lead to dangers in the future, and that by mitigating those actions in the present, a certain level of certainty and knowability of the future is attainable. However, systemic risk, as defined in the AI Act, is all encompassing, including both technical and social risks that operate at the border of scientific knowledge, especially in relation to its potential social impacts. As the AI Act attempts to transform GPAIM into something controllable, it does so in such a way (due to its reliance on a conception of risk that lacks clear boundaries), where these large-scale risks become institutionalised into the regulatory framework. This is particularly problematic when we consider the scale of these risks, especially regarding democratic values and institutions.

The reliance on systemic risk, with its lack of clear boundaries, is also problematic from the perspective of the law's primary function: the stabilisation of normative expectations by regulating how they are generalised over time, factual and social dimensions.[80] In the case of the AI Act, the use of flexible methods for regulating GPAIM counterintuitively results in increased uncertainty. This is exemplified by the reliance on post-hoc assessments in determining systemic risk, particularly the use of computation thresholds and high-impact capabilities. Both the computational threshold and high-impact capabilities defined in the AI Act do not provide prospective certainty as they rely on retrospective observation, using past models as benchmarks for categorisation. The computational threshold of 10^25, which only around twenty-five models currently exceed, provides no certainty and is equivalent to what Luhmann called an "empty formula-like obscurity" which provides no substantive guidance as to systemic risk.[81] There are two reasons for this: First, it erroneously assumes that models below this threshold lack the potential for systemic risk. Second, it assumes that risks scale proportionately in combination with computing power. However, this is not necessarily the case: as models develop, changes in model training, context, as well as the amount of

[77] S Jasanoff, *Science at the Bar: Law, Science, and Technology in America* (Harvard University Press 2009) available at <https://www.degruyter.com/document/doi/10.4159/9780674039124/html> (last accessed 26 February 2025).

[78] Black, "The Emergence of Risk-Based Regulation and the New Public Management in the United Kingdom," *supra*, note 6.

[79] Ibid.

[80] N Luhmann, *Law as a Social System* (Oxford University Press 2004) p 148.

[81] *Supra*, note 52, p 69.

computation per training phase may change. For example, more time and computational power might be used at the inference stage of model development, which may decrease the total amount of computational effort, whilst increasing the model's ability to perform "a wide range of distinct tasks" autonomously. Moreover, the rigidity of the computational threshold makes misclassification a real possibility. The amount of computation has direct causal relation between a model's level of computation and its risk. Models trained with less computational effort can also pose systemic risks. For example, a model trained using less than 10^25 FLOPs could still pose a systemic risk if integrated into critical infrastructure, while other models with higher computational effort may pose no systemic risk at all.

Because these thresholds are derived from the performance of prior models, these thresholds remain subject to change and revision. Nevertheless, any such revision is necessarily post-hoc and based on retrospective observations rather than proactive risk mitigation. This results in a de-temporalisation of the law's normative effect: the inherent instability of these thresholds means that the law has been created with the purpose of changing based differing social facts, thus only maintaining a type of procedural predictability.[82] This instability operates on two levels. First, the thresholds themselves remain provisional and contingent upon future observations. Second, any future observation will inevitably be retrospective, as the law cannot evolve at the same pace as technological change. This creates a paradox: the thresholds are structured as forward-looking, future-proof regulatory tools, yet they are permanently anchored in the past. Furthermore, the arbitrariness of the threshold as defined means that no decision has really been made, but rather the decision is deferred to the future. This deferral of genuine decision-making in terms of risk only compounds regulatory uncertainty, ensuring that systemic risk remains an open-ended and continuously shifting category rather than a stable point of reference for effective regulatory intervention. This is what Luhmann meant by the increase in arbitrariness producing "empty-like obscurities . . . [that] leave all decisions problems open and merely give the impression that something is happening, at least on the verbal level."[83] The thresholds and subsequent obligations of the AI Act are "empty" insofar as they tell us nothing about what the systemic risk is, nor any distinction about what risks the law envisions preventing.[84]

2. *Delegating risk definition to private entities through codes of conduct*

A central feature of the AI Act's co-regulatory approach is the delegation of decision-making responsibility to private actors. The definition, scope and identification of systemic risk has been delegated from the legislature to over a thousand interested stakeholders, ranging from private companies, model developers and civic society in a multi-stakeholder consultation process.[85] This delegation is achieved through the creation of a voluntary Code of Practice stipulated in Article 56 of the Act that is currently being drafted as well as being supported by the Act's approach to socio-technical standards.[86] This means that the private organisations responsible for developing and deploying GPAISR with systemic risk

[82] I-J Sand, "The Interaction of Society, Politics and Law: The Legal and Communicative Theories of Habermas, Luhmann and Teubner" in C Thornhill (ed), *Luhmann and Law* (Routledge 2017) pp 58–9.

[83] *Supra*, note 52, p 69. As Luhmann notes, "[I]f the law has to resort to such formulas then a technically informed arbitrariness is not the worst solutions. It is just not a specifically legal one."

[84] Ibid.

[85] "AI Act: Participate in the Drawing-up of the First General-Purpose AI Code of Practice | Shaping Europe's Digital Future" available at <https://digital-strategy.ec.europa.eu/en/news/ai-act-participate-drawing-first-general-purpose-ai-code-practice> (last accessed 29 April 2025).

[86] L Colonna, "Complex Normativity: Understanding the Relationship between Human Oversight by Design and Standardization in the Context of AI Development and Deployment" in S Nusselder and E Kosta (eds), *Data*

https://doi.org/10.1017/err.2025.10040 Published online by Cambridge University Press

are integrated into the decision-making processes of these risk. In that sense, the deferral of fixed decisions at the level of the AI Act are transformed into delegated decisions, insofar as the open-endedness of the thresholds and categorisations of the Act delegate the mitigation of systemic risk to those who produce the possibility of systemic risk. This is not that unusual in terms of risk regulation; however, it is arguably somewhat unusual given the severity and expansiveness of systemic risk.

As with the institutionalisation of uncertainty described in **section IV(2)**, I argue this causes two issues that operate at two different levels. First, the determination of systemic risk is largely entrusted to the GPAISR developers through risk management procedures, such as model evaluations, adversarial testing, and risk assessment and mitigation.[87] On the surface, this appears reasonable, as these entities possess the technical expertise necessary to assess whether their models meet the benchmarks and indicators outlined in Annex XIII. However, these technical benchmarks provide no substantive criteria for identifying the specific systemic risks associated with fulfilling them, nor do they indicate how such risks should be mitigated. Instead, the practical responsibility for both mitigation and identification of systemic risk is deferred to the Code of Practice outlined in Article 56, in conjunction with harmonised standards (Article 40), or alternatively, with an approach deemed acceptable by the Commission. Therefore, as those with the primary expertise in the field, GPAISR developers may be able to delimit the scope of what is included as systemic risk. This means that what is included within the scope of mitigating systemic risk will be those risks that can be quantified and modelled via technical means. For example, the regression to quantifiable risks can be seen in the demotion of systemic risk to fundamental rights to "other types of risk for potential consideration in the selection of systemic risk" section of the Code of Practice, in contrast to the "selected systemic risks" that GPAISR develops must be considered in accordance with Commitment II.3 of the Code of Practice.[88]

The other issue is that the Code of Practice can be co-opted to develop industrial morality. Codes of Practice are ubiquitous within all forms of organisation, from trade unions, non-profits and large multinationals.[89] However, Codes of Practice, as Casey has argued regarding the online gambling industry, can be used as mechanisms that "seek to develop an industry morality and cultural infrastructure".[90]

It is further important to note that the Codes of Practice remain voluntary for GPAISR providers. Both the second and third draft of the Code of Practice have extended and elaborated on the number of factors that might affect systemic risk, including, velocity (rapid escalation beyond mitigation), cascading effects (propagation across systems), irreversibility, asymmetric impact. This leads to the second level. The role of AI Model producers in the very development and codification of both the Codes of Practice and harmonised standards. (footnote) The Codes of Practice, which are currently under development, through a multi-stakeholder process that includes academics, experts, civil society organisations as well as the AI Model providers whose models exhibit systemic

Protection, Privacy and Artificial Intelligence: To Govern or to be Governed, That is the Question (Hart Publishing 2025) 77–113, p 83.

[87] Art. 55(1)(a)–(b), AI Act.

[88] Code of Practice, 3rd Draft, Appendix 1.2 available at <https://code-of-practice.ai/?section=safety-security#appendix-1-2-other-types-of-risks-for-potential-consideration-in-the-selection-of-systemic-risks>. See also LLCHL Caroli and D Evan, "Human Rights Are Universal, Not Optional: Don't Undermine the EU AI Act with a Faulty Code of Practice | TechPolicy.Press" (*Tech Policy Press*, 28 March 2025) available at <https://techpolicy.press/human-rights-are-universal-not-optional-dont-undermine-the-eu-ai-act-with-a-faulty-code-of-practice> (last accessed 30 April 2025).

[89] Black, *supra*, note 6.

[90] D Casey, "Reproducing Responsible Gambling through Codes of Conduct: The Role of Trade Associations and Codes of Conduct in Shaping Risk Regulation" (2024) 15 European Journal of Risk Regulation 447, 458–60.

https://doi.org/10.1017/err.2025.10040 Published online by Cambridge University Press

risk.[91] In effect, those responsible for creating potentially systemic risks are also directly involved in defining the parameters of their own regulatory obligations. This reflexivity not only complicates the legitimacy of systemic risk but also raises concerns about whether these frameworks genuinely function as risk-mitigating mechanisms or merely reinforce self-regulatory governance under the guise of compliance.[92]

3. Unity of a distinction: the AI act's unstable model-system distinction

One of the most obvious ambiguities in the AI Act's treatment of GPAISRs is in relation to GPAI systems. While the Act distinguishes between the two, its regulatory focus is disproportionately placed on models. This results in a regulatory "blind spot," where systemic risk is defined at the level of model, but left uncertain at the level of system. This blind spot is exemplified by an abundance of obligations for providers of GPAISR, while GPAI systems that are built upon GPAISR are only responsible for providing certain transparency obligations unless they fall under the heading of high-risk systems.[93]

Broadly, the AI Act distinguishes between systems and models, reflecting its dual objective of addressing sector-specific risks and broader systemic concerns. The AI Act specifically differentiations between model and system in order to increase "legal certainty."[94] AI systems are implicitly defined as products, consistent with the Act's heritage as a product liability framework under the New Legislative Framework.[95] These systems are designed to be placed on the internal market, either in specific high-risk sectors (healthcare, administration of justice, etc), or more generally across various domains.

The AI Act does not, however, define what a model is in general – only what constitutes a General-Purpose AI Model. Nevertheless, models are not the same as systems. Systems, which may include models, also include other components necessary to perform tasks and interact with users. In contrast, a model is a "mathematical model that generates an inference or prediction based on input data."[96] This means a model on its own is inherently incomplete – it cannot perform any tasks without first being integrated into a system. Models can be integrated into systems in different ways: remotely for example through an API or locally through a library.[97] The GPAI that are integrated into systems are defined as *general-purpose AI systems*. However, the only direct obligations for these systems are detailed in Article 50 and Article 74, which requires that outputs of a general-purpose AI system need to be marked in machine readable format and identifiable as artificially generated or manipulated, and that system is deployed for at least one purpose that is considered high-risk and are required to cooperate with the AI Office in cases of non-compliance. It is unclear to what extent the obligations of the model travel down the value chain into deployers of general-purpose AI systems. However, it should be noted that the author posits that any system that integrates a systemically risky model is necessarily imbued with said systemic risk. The AI Act does not provide specific mechanisms for the regulation of GPAI systems, however any GPAI system that is deployed in a sector considered high-risk, will get the same obligations as other AI systems under Article 6.

Accordingly, one might ask: if systemic risk is embedded in the model itself, should AI systems incorporating these models also be subject to closer regulatory oversight

[91] AI Office, "Multi-Stakeholder Consultation Future-Proof AI Act: Trustworthy General-Purpose AI".

[92] G Teubner, "After Legal Instrumentalism? Strategy Models of Post-Regulatory Law" in G Teubner (ed), *Dilemmas of Law in the Welfare State* (De Gruyter 2011) 299–325, pp 316–19.

[93] Art.50(2), AI Act.

[94] Recital 97, AI Act.

[95] *Supra*, note 66.

[96] Ibid.

[97] Ibid.

https://doi.org/10.1017/err.2025.10040 Published online by Cambridge University Press

regarding systemic risk? The Act suggests that GPAI systems may be high risk "by themselves or as components of other high-risks systems."[98] This assertion creates further uncertainty however: how can GPAI systems independently qualify as high-risk when they do not fall within the designated high-risk sectors? This ambiguity is intensified by the way systemic risk is "transferred" from models to the systems that integrate them. Even if a GPAI system is not classified as high-risk, it may inherit and operationalise the potential for *systemic risk* embedded in its model. This suggests an ontological distinction: whereas models generate the potential for systemic risk through the possibility of inference, systems instantiate and materialise that risk in real-world applications. Systems, in effect, give voice to the systemic risk latent in models. Consequently, systems that integrate models with systemic risk may themselves exert significant influence on fundamental rights and social structures, even when they are categorised as minimal or low risk. The distinction between model and system was made by the Act to ensure legal certainty. However, this distinction conceals a unity of difference: models and systems are interdependent on one another to materialise and instantiate systemic risk.

This results again in a regulatory paradox. Under the AI Act's framework, an AI system may be classified as minimal risk and thus not require additional oversight, while still actualising systemic risks associated with its model. This paradox exposes a fundamental inconsistency exemplified through the AI Act's acknowledgment of systemic risk at the model level without corresponding obligations at the system level unless the system falls into the predefined high-risk category. As a result, an AI system that is not explicitly designated as high-risk can nevertheless function as a critical vector for systemic risk, exerting significant influence on legal norms, markers, and social institutions without being subject to the same degree of scrutiny.[99]

This regulatory blind spot contributes to the AI Act's inability to resolve the inherent uncertainty surrounding systemic risk and AI. While obligations remain with the model provider, the absence of a clear regulatory mechanism to address systemic risk at the system level presents a critical oversight. Without resolving this paradox, the AI Act risks enabling a form of regulatory arbitrage where deployed systems circumvent obligations by deploying powerful models within nominally minimal risk systems, thereby operationalising systemic risk without triggering the regulatory safeguards intended to mitigate it.

However, addressing this blind spot is not straightforward. While the current regulatory scheme poses risk, alternative regulatory solutions themselves carry risk. For instance, since systemic risks manifest at the level of system, imposing greater obligations on downstream providers or businesses that fine-tune models could help contain or manage the potential spread of these risks. Yet this approach carries its own dangers. For example, this may result in disproportionately burdening smaller actors with onerous compliance requirements. Moreover, the strategies for identifying and managing potential risks may become distributed and difficult to maintain. In doing so, it risks falling into the other side of the paradox identified by Black, where regulation becomes overly rigid and inflexible.

V. Conclusion

How does the incorporation of systemic risk within the regulation of GPAISR's in the AI Act produce more uncertainty than it resolves? To answer this question, I have traced the systemic risk functions as a novel legal category whose borders are still being identified

[98] Recital 85, AI Act.

[99] This is particularly relevant where a model is fine-tuned by a systems provider. Fine tuning is the process of training a pretrained model on new training data that is more specific or related to the potential downstream tasks. Cf Recital 97, AI Act where it states that "models may be further modified or fine-tuned into new models."

https://doi.org/10.1017/err.2025.10040 Published online by Cambridge University Press

and refined, both within legal instruments as well as within the risk literature. Furthermore, I have identified three primary issues that are caused by its inclusion. First, it institutionalises uncertainty surrounding the effects of GPAISR within the legal framework for governing and mitigating risks by relying on vague and ill-defined definitions. As I have elaborated, this vagueness contributes to both legal and scientific uncertainty. Second, by leaving the scope and identify of systemic risk vague and uncertain, the Act relies on outside actors to "fill out" its own uncertain definition. This leads to a technical scope of systemic risk, that avoids dealing with the difficult principle-based discussion of applying systemic risk to fundamental rights. Finally, while attempting to differentiate between system and model, the Act misunderstands their fundamental connection between each other, causing a regulatory "blind spot" where models become the focus of regulation, and systemic risk produced by systems built on GPAISR's goes largely untouched.

As Black has noted, "[r]egulators do not know where the next big failure will come from, but they must act as if they do."[100] The inclusion of systemic risk in the AI Act reflects a pre-emptive gesture towards managing the uncertainty of the "next big failure." However, its broad scope and attempt to include fundamental rights within its ambit introduces more uncertainty than it resolves. Paradoxically, the Act's attempt to mitigate systemic risk may itself constitute a systemic vulnerability through its creation of "empty-like formulas."

Acknowledgments. A draft of this paper was presented at the IT and Cyberspace stream at the Socio-Legal Studies Association's Annual Conference 2025 held at the University of Liverpool. I am grateful to the participants for their thoughtful comments and suggestions. I am also grateful to Professor Peter Wahlgren, Professor Mauro Zamboni and Assistant Professor Liane Colonna for their comments and suggestions on earlier versions of this article.

Financial support. This work was partially supported by the Wallenberg AI, Autonomous Systems and Software Program – Humanity and Society (WASP-HS) funded by the Marianne and Marcus Wallenberg Foundation and the Marcus and Amalia Wallenberg Foundation.

Competing interests. WASP-HS has not placed any restrictions on publishing other than that they be acknowledged as a source of support. I have no other competing interest to declare.

[100] Black, "The Emergence of Risk-Based Regulation and the New Public Management in the United Kingdom," *supra*, note 6, p 549.

Cite this article: S Carey, "Regulating Uncertainty: Governing General-Purpose AI Models and Systemic Risk". *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2025.10040