Technology and Regulation

Charting systemic risk management as a regulatory paradigm in EU digital legislation:

features, challenges and directions for future research

Author(s)	Andrea Palumbo
Contact	andrea.palumbo@kuleuven.be
Affiliation(s)	Andrea Palumbo is a doctoral student at the Centre for IT & IP Law, KU Leuven, Belgium.

Keywords	Digital Services Act, AI Act, risk-based regulation, risk management, systemic risk
Published	**Received**: 13 Apr 2025 **Accepted**: 01 Oct 2025 **Published**: 14 Jan 2026
Citation	Andrea Palumbo, Charting systemic risk management as a regulatory paradigm in EU digital legislation: features, challenges and directions for future research, Technology and Regulation, 2026, 1-17 • 10.71265/p7d4nv98 • ISSN: 2666-139X

Abstract

This paper provides a description, analysis and systematic theorisation of systemic risk management obligations as a distinctive regulatory approach under the Digital Services Act (DSA) and the Artificial Intelligence Act (AIA). In particular, it identifies the common features under the DSA and the AIA that characterise systemic risk management as a *sui generis* regulatory approach, that can be distinguished from other risk-based regulatory models in EU law. Based on this analysis, it identifies and discusses uncertainties surrounding the implementation of systemic risk management obligations, as well as potential issues deriving from the reliance on systemic risk management as a regulatory tool to address the societal challenges created by digital technologies. The ultimate objective of the paper is to chart the path for future research that looks at the open questions and challenges of this new and consequential regulatory approach.

1. Introduction

A well-known and largely discussed phenomenon in the digital legislation of the European Union (''EU'') is the so-called ''risk-based approach''. This term has been coined to characterize EU legislation that uses risk to define obligations, delimit the scope of application of the law and target enforcement action,[1] so

1. Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach' (2018) European Journal of Risk Regulation 502, 509.

that it is carefully calibrated to the actual hazard posed by an activity or object.[2] In other words, the risk-based approach entails relying on risk management as the instrument to enhance the responsibility of regulated entities and shape their obligations to protect public or private interests, such as fundamental rights. This approach in the area of digital legislation is part of a larger trend of risk-based regulation that has shaped legislation in various areas in the past decades. In this regard, the risk-based approach is only one of the multiple roles played by risk in regulatory processes.[3] Initially developed to frame obligations to mitigate risks to the environment, human health and safety,[4] risk-based regulation has been introduced in an increasing number of EU policy areas.[5] A consequence of risk-based regulation is the outsourcing of regulatory responsibilities to the managerial expertise and technocratic knowledge of private actors, which denotes a mode of regulation called ''regulatory managerialism''.[6] Bound by risk as a concept that frames accountability relationships and determines the scope of obligations, private actors have been required by law to interpret and implement regulatory requirements through risk management.[7] It is also part of a broader trend of the ''post-regulatory state'', that has been observed in the past decades as a shift away from centralised and traditional forms of regulation towards decentralised and market-based governance mechanisms.[8]

In the area of digital law, the risk-based approach is most evident in three pieces of legislation: the General Data Protection Regulation (''GDPR''),[9] the Digital Services Act (''DSA'')[10] and the Artificial Intelligence Act (''AIA'').[11] In all of these regulations, the risk-based approach is the instrument chosen by the EU legislator to protect fundamental rights and other public and private interests, while taking into account the counterbalancing objective to protect economic freedoms and foster innovation. The *ex ante* risk-based approach can thus be seen as a common thread between the GDPR, the DSA and the AIA, though it finds different declinations across the three regulations.

While part of a broader trend, the risk-based approach finds a unique declination in the DSA and the AIA. This paper is concerned with this specific approach to risk-based regulation, that revolves around the notion of systemic risk and the related risk management obligations. Obligations to assess and mitigate systemic risks appear both in the DSA and the AIA. While the notion of risk, and its role as a proxy to

2. Giovanni De Gregorio, Pietro Dunn, 'The European risk-based approaches: Connecting constitutional dots in the digital age' (2022) Common Market Law Review 473.
3. Julia Black, 'The Role of Risk in Regulatory Processes' in Robert Baldwin, Martin Cave and Martin Lodge (eds), *The Oxford Handbook of Regulation* (online edn, Oxford Academic 2010).
4. Alberto Alemanno, 'Regulating the European Risk Society' in Alberto Alemanno et al. (eds), *Better Business Regulation in a Risk Society* (Springer, 2013); Milda Macenaite, 'The "Riskification" of European Data Protection Law through a Two-fold Shift' (2017) European Journal of Risk Regulation 506, 508-509.
5. Alemanno (n 4), 53.
6. Julie E. Cohen, Ari E. Waldman, 'Introduction: Framing Regulatory Managerialism as an Object of Study and Strategic Displacement' (2023) 86(3) Law and Contemporary Problems.
7. ibid.
8. Julia Black, 'Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World' (2001) 54(1) Current Legal Problems 103; Adam Crawford, 'Networked Governance and the Post-Regulatory State? Steering, Rowing and Anchoring the Provision of Policing and Security' (2006) 10 Theoretical Criminology 449; Colin Scott, 'Regulation in the Age of Governance: The Rise of the Post-Regulatory State' in Jacint Jordana, David Levi-Faur (eds), *The Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance* (Edward Elgar Publishing, 2004).
9. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.
10. 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) [2022] OJ L 277/1.
11. 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) [2024] OJ L 2024/1689.

protect fundamental rights, have been largely discussed in legal scholarship to date,[12] systemic risk is a new concept that still needs to be fully understood in the context of the DSA and the AIA. Moreover, systemic risk management obligations present multiple elements of novelty that are unprecedented in EU law, and that distinguish them from other risk-based obligations. To date, there is no academic contribution that aims to comprehensively describe systemic risk management as a new regulatory phenomenon, looking at both the DSA and the AIA, and that identifies the specific features of this declination of the risk-based approach that pose their own, distinctive challenges. By doing so, this paper aims to provide two main novel contributions to existing scholarship: i) the theorisation of systemic risk management as a single regulatory approach with common features across the DSA and the AIA, ii) the identification of the specific challenges and open questions stemming from the distinctive features of systemic risk management. This paper has the twofold objective to present findings on systemic risk management as a regulatory approach, and to outline a research agenda for the open questions and outstanding challenges that it poses. The second objective of this analysis is thus to chart a path for future research that further investigates the open questions and outstanding challenges of systemic risk management regimes under the DSA and the AIA. In order to pursue its research objectives, this paper answers two research questions: (i) which are the common features of systemic risk management obligations in EU digital legislation that distinguish them as a *sui generis* regulatory approach, as compared to other risk-based regulatory models in EU law?, (ii) which are the unique interpretive and applicative open questions and outstanding applicative challenges deriving from the reliance on systemic risk management to substantiate and protect qualitative and politically-laden interests and values?

The two research questions driving this paper complement each other and are strictly interconnected. Framing systemic risk management as a regulatory approach with its own distinctive features allows to define it as an object of analysis and to adequately identify open questions and outstanding challenges. In turn, outlining the questions and challenges allows to better qualify and understand the distinctive features of systemic risk management.

2. The notion of systemic risk in the DSA and the AIA: differences and similarities

Both the DSA and the AIA lay down obligations to assess and mitigate systemic risks. In the DSA, the systemic risk management regime is established by Articles 34 and 35. These articles apply only to a subcategory of intermediary service providers, namely very large online platforms[13] and very large online search engines (''VLOPSEs'').[14] On condition that their user base meets certain quantitative thresholds,[15] these providers are subject to additional due diligence requirements. These requirements include the obligation to assess and mitigate the systemic risks stemming from their services' design, functionality, or usage. The obligation should be complied with by conducting cycles of risk management exercises. First, Article 34 prescribes the identification and assessment of systemic risks, by carrying out assessments at least once a year. Second, based on the outcome of such assessments, Article 35 requires providers of VLOPSEs to subsequently adopt measures to mitigate systemic risks. Risk assessment and mitigation are subject to external auditing[16] and take place under the supervision of the European Commission[17], in what has been defined as a model of

12. In particular regarding the implementation of the GDPR, see: Niels van Dijk et al, 'A risk to a right? Beyond data protection risk assessments' (2016) Computer Law & Security Review 286; Raphael Gellert, 'We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection' (2016) European Data Protection Law Review 481; Bart van der Sloot, 'Ten Questions about Balancing' (2017) European Data Protection Law Review 187; Raphaël Gellert, *The Risk-Based Approach to Data Protection* (Oxford University Press, 2020).
13. See Art. 3(i) DSA.
14. See Art. 3(j) DSA.
15. See Section 3.2.1 below.
16. See Art. 37 DSA.
17. See Art. 56(2) DSA.

meta-regulation[18] or a polycentric regulatory model with elements of co-regulation.[19] In the AIA, Article 55(1)(b) requires providers of general-purpose AI models (''GPAIMs'')[20] with systemic risk to assess and mitigate the systemic risks stemming from the development, placing on the market or use of their GPAIMs. Providers of GPAIMs with systemic risk are a subcategory of providers of GPAIMs, which are subject to additional requirements laid down Section 3, Chapter V of the AIA. As in the DSA, systemic risk management under the AIA is directly supervised by the Commission, which is conferred exclusive supervision and enforcement powers.[21] Under both regulations, systemic risk assessment and mitigation are separate but interconnected stages of the risk management cycle. Based on the assessment of systemic risks, mitigations measures are designed and implemented. While risk assessment is instrumental to risk mitigation, the two activities do not necessarily have the same scope. There is no indication that risk mitigation must aim at addressing all the identified risks, as which systemic risks need to be mitigated and how is left to the discretion of regulated entities, under the supervision of the Commission.[22]

These regimes revolve around the central notion of systemic risk. This Section argues that, despite some differences at first sight, the notions of systemic risk in the two regulations share key similarities. This finding is a necessary first step to frame the provisions of the DSA and the AIA as a single regulatory approach centred around the same central notion. The DSA does not provide a legislative definition of systemic risk, but this can be somehow carved out through the indications in Articles 34 and 35 on how systemic risks should be assessed and mitigated. Contrary to the DSA, Article 3(65) of the AIA provides a legislative definition of systemic risks, which is similar to, but does not entirely coincide with, the description drawn from the indications provided in the DSA. The notion appears to have a slightly different meaning in the two regulations, but a closer analysis demonstrates that there may be very little difference in practice.

First, the two regulations mention different protected interests that risk management must be directed at. On the one hand, the category of systemic risks under the DSA appears to be open-ended, and it merely includes the specific risks to the protected interests listed in Article 34(1).[23] As an open-ended category, it may include additional systemic risks, identified on a case-by-case basis.[24] On the other hand, under the AIA systemic risks appear to be exhaustively listed as those with a significant impact on the Union market due to their reach or due to negative effects on fundamental rights, public health, safety, public security and the society as a whole. This legislative definition thus appears to frame the category of systemic risks as closed-ended. However, the broad and vaguely drawn perimeter of systemic risks with negative effects to ''society as a whole'' may render these subcategories effectively open-ended. In this regard, relevant scholarship seems to have assumed an essentially open-ended nature of the definition.[25] Similarly, the Code of Practice for GPAIMs identifies systemic risks that are not listed in the legislative definition.[26] In line with some conceptualisations that identify among the risks posed by AI long-term consequences whose cause-effect nexus with AI deployment may be difficult to ascertain, such as automation of work, unemployment and inequalities,[27] the category of systemic risks is potentially as large and methodologically difficult to constrain as it can be.

Second, while the DSA refers to systemic risks ''in the Union'', the AIA refers to systemic risks having a significant impact ''on the Union market''. This difference in wording may not correspond to a real difference

18. Nicolo Zingales, 'The DSA as a paradigm shift for online intermediaries' due diligence: hail to meta-regulation', in Joris van Hoboken et al (eds), ''Putting the Digital Services Act Into Practice: Enforcement, Access to Justice, and Global Implications'' (2023) Amsterdam Law School Research Paper No. 13, Institute for Information Law Research Paper No. 03, 2023.
19. Martin Husovec, *Principles of the Digital Services Act* (online edn Oxford Academic, 2024).
20. See Art. 3(63) AIA.
21. See Art. 88 AIA.
22. On this interpretation of the systemic risk management obligations under the DSA, see: Martin Husovec, 'The Digital Services Act's red line: what the Commission can and cannot do about disinformation' (2024) 16(1) Journal of Media Law, 47–56.
23. These are categories identified by the EU legislator as they should be 'assessed in-depth': see Recital 80 of the DSA.
24. See Recital 76 DSA.
25. Risto Uuk et al, 'A Taxonomy of Systemic Risks from General-Purpose AI' (2024) arXiv 2412.07780..
26. See the systemic risk taxonomy in Appendix 1.4 of the safety and security chapter: European AI Office, *Code of Practice for General-Purpose AI Models: Safety and Security Chapter* (2025).
27. Anthony Aguirre, 'Close the Gates to an Inhuman Future: How and why we should choose to not develop superhuman general-purpose artificial intelligence' (2023)arXiv 2311.09452

in the perimeter of systemic risks. As the AIA and the DSA have been adopted on the basis of Article 114 of the Treaty on the Functioning of the European Union (''TFEU''),[28] the clause conferring competence on the EU to reduce existing obstacles to the internal market, they should both be interpreted with their internal market objective in mind. There may thus be no difference in reality between larger societal risks that indirectly affect the internal market, and risks that are of direct concern to the internal market. This suggests that the DSA and the AIA are potentially directed at the protection of the same interests with their risk management obligations.

Third, as an inevitable consequence of the differences between the services and products regulated under the DSA and the AIA, the modalities of propagation that characterise systemic risks in the two regulations can also differ. In particular, the different nature of the sociotechnical systems regulated by the two regulations entails that systemic risks can have different nature and dynamics leading to their propagation. The different modalities of propagation are also reflected in the different criteria for the designation of VLOPSEs and GPAIMs and in the legislative definition of systemic risks of the AIA. While the systemic nature of VLOPSEs seems to derive from their reach as intermediaries with a large customer base,[29] for GPAIMs it is about both their high-impact capabilities, including their computational power,[30] and their reach due to the customer base and propagation across the value chain.[31] The reference to high-impact capabilities and computational power indicates that providers of GPAIMs can generate systemic risks even in a situation where they have a small customer base. This marks a significant difference with the systemic risk management regime of the DSA. However, the different modalities of propagation of systemic risks does not entail that the type of impact on protected interests that the two regulations seek to mitigate is equally different. In other words, it does not exclude that the meaning of 'systemic' under the DSA and the AIA is as different as the designation criteria for VLOPSEs and GPAIMs are. Systemic risks can be understood as risks of similar, and at times coinciding, large-scale societal impacts of digital technologies, that entail negative effects to protected individual, collective and societal interests. It can be argued that this is confirmed by the fact that the range of protected interests largely overlaps under the two regulations, and that the legislative text of the AIA acknowledges that systemic risks can coincide with those to be assessed and mitigated under the DSA. As explicitly recognised by the Recitals of the AIA,[32] if AI systems and models are embedded into VLOPSEs, compliance with the systemic risk management obligations of the DSA leads to a presumption of compliance with the corresponding obligations of the AIA, unless significant systemic risks not covered by the DSA emerge and are identified.[33] This is an explicit recognition that there may be an overlap, in practice, of systemic risks under the two regulations that can be mitigated with the same measures.[34] Therefore, while the specific systemic risks covered in practice by the DSA and the AIA may differ, the possibility of overlaps can be read as an indication of the conceptual similarities of the concepts of systemic risk.

The considerations made above provide a comparison of the notions of systemic risk under the DSA and the AI Act, based on the following criteria: protected interests, scope of the relevant risks in the Union, and nature of the risks to be assessed and mitigated. These criteria are relevant for the purposes of this paper because they allow to identify common features of systemic risks that reveal a similar rationale and practical implications. Under both regulations, systemic risks capture EU-wide risks to individual, collective and societal interests that have 'systemic' character. The identification of these similarities is instrumental, as further explained below, to distil the distinctive features of systemic risk management as a single regulatory approach. For instance, as both notions aim to mitigate risks to undefined public values like civic discourse and public security, they present the same methodological challenges of understanding how risks to these values are assessed and mitigated, as well as determining when they assume systemic character. Once

28. It must be noted that the AIA is also based on Art. 16 TFEU.
29. See Art. 33 DSA.
30. See Art. 51(2) and letters a) to e) of Annex XIII AIA.
31. See letters f) and g) of Annex XIII AIA.
32. See Recitals 118, 119 and 136 AIA.
33. See Recital 118 AIA.
34. An example of overlap in the scope of application is the Imagine feature of Instagram and Facebook. See: Paddy Leerssen, 'Embedded GenAI on Social Media: Platform Law Meets AI law' (2024) DSA Observatory https://dsa-observatory.eu/2024/10/16/1864/.

that the notions of systemic risk under the DSA and the AI Act have been described as similar, it must be considered how they relate to the baseline definition of risk. This is discussed in Section 3 below.

3. Systemic risk and ''regular'' risk: *de facto* synonyms or independent concepts?

The most evident novelty brought by the DSA and the AIA in EU digital legislation is the characterisation of risks as ''systemic''. A question that has received little attention in the literature to date is to what extent systemic risks are an independent category that differs from other or ''regular'' risks. This question is of central importance for the purposes of framing systemic risk management regimes as a new regulatory approach, as relating to a risk category that requires an *ad hoc* regime.

The answer lies in the interpretation of the adjective systemic, particularly in its reference to systems. It is through the systems-oriented lens that systemic risks can be identified and distinguished from ordinary risks. The reference to a system is thus the qualifying attribute that complements the baseline legislative definition of risk[35] to form the new notion of systemic risk. Despite the terminological difference, it is however not clear whether it corresponds to a real qualitative difference in the nature of the risks to be assessed and mitigated. In particular, the reference to systems could be understood in two different ways.

On the one hand, it could be interpreted as qualifying the regulated services and products as systems. Risks would thus be systemic because they arise from technological and sociotechnical systems. Under this interpretation, risks would be essentially of the same nature as any other risks, with the only difference of stemming from products and services that have significant reach and/or computational power. For instance, when it comes to protecting fundamental rights, risks to the latter would still be assessed with a focus on individual interests, similarly to how it has been done to date under the GDPR, with the only difference of paying attention to how they stem and propagate through systems.

On the other hand, what makes a risk systemic could be its ability to affect an entire system in society beyond individual cases, e.g. beyond the risks of harm to individual persons.[36] This understanding could be the basis to operationalise the notion of systemic risk to address structural issues[37] and account for collective[38] and societal[39] forms of harm that cannot be reduced to instances of individual harm. Such difference is particularly important in relation to fundamental rights, as it can justify an approach that looks beyond isolated instances of harm and considers how the effects on social systems, such as online information flows and civic discourse, can ultimately erode the effective enjoyment of fundamental rights.

This paper assumes that the reference to systems encompasses both interpretations, as covering both risks stemming from systems and risks to systems. The second interpretation that considers risks to systems seems to be confirmed by a reading of the relevant recitals[40] of the DSA and the AIA, where systemic risks are characterized as those relating to harm that can occur at a large scale and affect systems that are essential to the good functioning of society.[41] This can be interpreted as indicating the intention of the legislator to address structural and collective risks to society. It would also be a plausible explanation for the creation of the new category of systemic risks. If what makes a risk systemic were just its origin in a system there would

35. According to Art. 3(2) AIA, risk means ''*the combination of the probability of an occurrence of harm and the severity of that harm*''.
36. Katharina Kaesling, Annegret Wolf, 'Sustainability and Risk Management under the Digital Services Act: A Touchstone for the Interpretation of 'Systemic Risks' (2025) 74(2) GRUR International 119, 122; Sally Broughton Micova, Andrea Calef, 'Elements for effective systemic risk assessment under the DSA' Centre on Regulation in Europe (CERRE) (2023) 13 https://cerre.eu/wp-content/uploads/2023/07/CERRE-DSA-Systemic-Risk-Report.pdf.
37. Rachel Griffin, 'Rethinking Rights in Social Media Governance: Human Rights, Ideology and Inequality' (2023) 2 European Law Open 30, 44.
38. Michael Veale et al, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 22 Computer Law Review International 97, 99.
39. Nathalie Alisa Smuha, 'Beyond the Individual: Governing AI's Societal Harm' (2021) 10(3) Internet Policy Review
40. See Recitals 76-83 DSA, and Recitals 110-115 AIA.
41. Sally Broughton Micova, 'What's the Harm in Size? Very Large Online Platforms in the Digital Services Act' Centre on Regulation in Europe (CERRE) 2023 https://cerre.eu/wpcontent/uploads/2021/10/211019_CERRE_IP_What-is-the-harm-in-size_FINAL.pdf.

be no reason to create a different category, as any regular risk stemming from a system would in any case need to be assessed and mitigated taking into account how it propagates through the system. This does not mean that the specific modalities of risk propagation through VLOPSEs and GPAIMs as systems should not be taken into account, but rather that these considerations should be integrated in the assessment of risks as relating to structural and collective harm to social systems. As further elaborated in Section 3.2.1. below, VLOPSEs and GPAIMs can be considered as the infrastructures underpinning, at least in part, the social systems that the DSA and the AIA seek to protect, and are thus part of the systems themselves.

In conclusion, this paper understands systemic risk as an independent concept that may refer to risks not only stemming from systems but also affecting systems, thus requiring an approach that looks at structural and collective risks. However, as explained in Section 4.1 below, there are methodological uncertainties surrounding this notion and different interpretations remain plausible, which requires to make choices on the role that systemic risk management should have.

4. Systemic risk management in the DSA and the AIA: framing a regulatory phenomenon

This Section analyses two main features of the systemic risk management obligations in the DSA and the AIA, with the objective to frame the distinctive aspects that characterize it as a unique regulatory approach in EU legislation. The first main feature results from the notion of systemic risk itself, and lies in the concept of ''system''. While the systems where risks arise and are propagated would differ under the DSA and the AIA, the centrality of this concept is a common denominator for both regulations. The second main feature lies in the attribution of systemic risk management responsibilities to regulated entities, that are called on to balance conflicting constitutional interests and operationalise them by relying on systemic risk as a proxy. It is these two common features that frame a single phenomenon in EU legislation, with a common rationale as evidenced by the recitals,[42] regulatory guidance[43] and preparatory documents[44] that call for a consistent implementation of the two regimes.

4.1 Protecting social systems through risk management: the central and slippery notion of ''system''

Defining the notion of ''system'' in the context of systemic risk management obligations is a question that has already interested scholars in the area of financial regulation.[45] As the first legal framework where the concept of systemic risk was introduced by the EU legislator,[46] defining systemic risk for the purposes of prudential oversight over financial institutions proved to be a very complicated task.[47]

Given the centrality of the notion of system for the implementation of the DSA and the AIA, the question arises as to how the relevant systems should be identified. However, due to the fact that this term has been used for the first time for the risks posed by digital technologies to individual and societal interests, the answer is far from straightforward. A first step would be to locate the interests that the EU legislator intended to protect in the DSA and the AIA. Both regulations aim to mitigate the systemic risks of societal harm,[48] but with no indications as to which are the relevant social systems. However, some of the interests that systemic risk management should seek to protect have been identified by the legislative provisions. It can be

42. See Recital 118 AIA.
43. European Commission, Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Art. 35(3) of Regulation (EU) 2022/2065 [2024] OJ C/2024/3014, paras. 38, 77.
44. European Commission, AI Act proposal, COM (2021) 206 final, 2021/0106 (COD), 5.
45. George Kaufman, Kenneth E. Scott, 'What is systemic risk, and do bank regulators retard or contribute to it?' (2003) 7(3) The Independent Review 371; Ortwin Renn et al, 'Things are different today: The challenge of global systemic risks' (2019) 22(4) Journal of Risk Research 401.
46. See Regulation (EU) No 1092/2010 of the European Parliament and of the Council of 24 November 2010 on European Union macro-prudential oversight of the financial system and establishing a European Systemic Risk Board [2010] OJ L331/1.
47. Micova and Calef (n 36) 16 https://cerre.eu/wp-content/uploads/2023/07/CERRE-DSA-Systemic-Risk-Report.pdf.
48. See Recital 79 DSA and Recital 110 AIA.

noted that these are all interests that find some recognition in the EU constitutional framework. For all the interests explicitly protected by systemic risk management regimes it is possible to find a connection with principles and values enshrined in EU constitutional law, as is the case for fundamental rights,[49]democracy[50] and public health.[51] It is thus in relation to EU primary law, and the public and private interests protected therein, that some guidance can be found on the relevant ''systems'' that the DSA and the AIA seek to protect. After all, these regulations are part of EU secondary law and should be interpreted in light of EU primary law. Along these lines, the EU constitutional framework can provide interpretive guidance, in two respects: i) clarify the meaning of the protected interests listed in the relevant provisions of the DSA and the AIA, ii) identify additional protected interests that are not listed in the regulations, but for which systemic risks may arise that are part of the open-ended category of the DSA and of the (essentially) open-ended category of the AIA. This can be done by looking at the additional constitutional interests enshrined in EU primary law that may be implicated by the risks generated by VLOPSEs and GPAIMs, such as sustainability.[52]

While EU primary law is a clear starting point, the concrete definition of the relevant systems is surrounded by uncertainty. As an essentially open-ended category, there is much left to decide as to what in concrete would fit in it. Not all the interests protected under EU primary law may be relevant, and the most plausible criterion for their identification is indeed whether they relate to a social system. As systemic risk management obligations aim at large-scale risks that do not solely affect individual cases, it is the reference to a system that warrants protection of a constitutional interest in systemic risk management. The establishment of a link between protected interests and systems is important also for the systemic risks that are explicitly listed in the AIA and the DSA. While their explicit mention in the legislative text shows that the link has already been established by the EU legislator, the question remains as to how they relate to systems, and which ones. For instance, as fundamental rights are by definition intended to afford protection to individuals, to which social systems do they relate? In which cases a risk to individual interests becomes systemic?[53]

These questions do not find an easy answer due to the methodological uncertainties on the identification of social systems. In particular, systemic risks to the social systems covered by the AIA and the DSA are currently still an undefined regulatory object. Systemic risk is a concept that finds multiple and differing formulations in different disciplines, such as finance,[54] medicine, ecology, environmental and disaster risk science.[55] The study of dynamical systems and catastrophe theory offer the most valuable insights,[56] as it provides findings that are not domain-specific (such as finance and medicine) but can be adapted to different domains. In this context, a ''system'' is understood as a set of interconnected components that function as a single unit,[57] and systemic risks relate to interdependent, cascading failures in the system composed of interconnected units.[58] However, for the first time in the history of EU law, the notion of systemic risk has been used in relation to social systems and values such as fundamental rights and democracy. It has been argued that the conceptualisation of systemic risk with regard to social systems is challenging, due to the absence of a unified theory of systemic risk for society as an interconnected system.[59] A theory that explains how digital phenomena, such as content dissemination on online platforms and ubiquitous output generation by GPAIMs, trigger systemic risks to the relevant interests protected in EU constitutional law is needed as a first methodological starting point for consistent and verifiable risk management. The absence

49. As enshrined in the Charter of Fundamental Rights of the European Union [2012] OJ C 364/01.
50. See Art. 2 Treaty on European Union.
51. See Art. 168 TFEU.
52. Kaesling (n 36), 122.
53. For a discussion on large-scale and systemic risks to fundamental rights, see: Sue Anne Teo, 'How Artificial Intelligence Systems Challenge the Conceptual Foundations of the Human Rights Legal Framework' (2022) 40(1) Nordic Journal of Human Rights, 216.
54. Thomas Ilin, Liz Varga, 'The uncertainty of systemic risk' (2015) 17 Risk management, 240; Viral V. Acharya et al, 'Measuring systemic risk' (2017) 30(1) The Review of Financial Studies 2; Renn et al (n 45),.
55. Janna Sillmann et al, 'Systemic Risk' (briefing note of ISC-UNDRR-RISK KAN, 2022), https://council.science/wp-content/uploads/2020/06/Systemic-risk-briefing-note_WEB.pdf.
56. Michele Loi et al, 'Regulating the Undefined: Addressing Systemic Risks in the Digital Services Act (with an Appendix on the AI Act)' (2025) 38(2) Philosophy and Technology 1.
57. ibid.
58. Dirk Helbing, 'Globally networked risks and how to respond' (2013) 497 Nature 51.
59. Loi (n 56).

of such theoretical roots creates an epistemic gap,[60] which in turn poses a challenge from a methodological standpoint. Even existing regulatory guidance under the DSA does not provide a theory for the definition of systemic risks, but rather assumes a common understanding of the concept.[61]

The considerations made above lead to two preliminary conclusions: i) the EU constitutional framework can serve as the basis to identify and understand the relevant systems to be protected through systemic risk management, but ii) there is not sufficient research nor a unified theory to assess how these social systems are threatened by digital phenomena, to the extent that the notion of systemic risk cannot be adequately formalized. This raises questions that still need to be answered, as is further examined in Section 5.1 below.

4.2 The normative and regulatory dimension of systemic risk management: a form of quasi-regulation

4.2.1 Digital infrastructures and social systems: the role of systemic risk managers

Systemic risk management obligations are imposed only on certain regulated entities that are placed in a pre-defined legislative category based on their risk profile. The DSA and the AIA provide for criteria and a procedure to follow for the designation of the VLOPSEs and GPAIMs that fall under this category.

VLOPSEs are designated by a decision of the Commission[62] on the basis of the number of average monthly active recipients of their services in the Union.[63] The distinguishing feature of this category is thus the reach of the service. GPAIMs with systemic risk are designated following a notification to, or a decision by, the Commission.[64] A GPAIM is classified as having systemic risk if it has high impact capabilities evaluated on the basis of appropriate technical tools and methodologies, or if the Commission finds that it has equivalent capabilities or impact based on the criteria set out in Annex XIII.[65] It can be noted that the criteria for classification relate to both the computational power and the reach of a GPAIM, as the conditions for classification can be met based on varied factors such as the cumulative amount of computation used for their training,[66] and the service's reach in the internal market due to the number of registered business and end-users.[67]

An analysis of the criteria for the designation of VLOPSEs and GPAIMs reveals a similar rationale for the creation of these risk categories. They both aim to identify products and services that play a significant intermediary role in society or otherwise display capabilities that increase the ability to affect social systems. Under this light, the rationale can be found in the role that they play as infrastructures enabling or significantly affecting the functioning of consequential societal systems. The DSA and the AIA never use the term infrastructure in relation to VLOPSEs and GPAIMs, but describe the role of the latter as central to the operation of multiple social systems.[68] Moreover, the Commission described very large platforms as ''*de facto* public spaces'',[69] playing a ''systemic role for millions of citizens and businesses''.[70] The role of online platforms as informational and social infrastructure has been well acknowledged by relevant scholarship,[71]

60. ibid.
61. Commission Guidelines(n 43) .
62. See Art. 33(4) DSA.
63. See Art. 33(1) DSA.
64. See Arts. 51 and 52 AIA.
65. See Arts. 51 and 52 AIA.
66. See Art. 51(2) AIA.
67. See letters f) and g) of Annex XIII AIA.
68. See Recitals 75 and 76 DSA, and Recital 110 AIA.
69. European Commission, Commission Staff Working Document, 'Impact assessment accompanying the document proposal for a regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC', paras. 27, 85, 89, 277, 287.
70. ibid, Annexes, 62, 64.
71. Sabeel Rahman, 'Regulating informational infrastructure: Internet platforms as the new public utilities' (2018) 2 Georgetown Law Technology Review 234; Sabeel Rahman 'The new utilities: Private power, social infrastructure, and the revival of the public utility concept' (2018) 39 Cardozo Law Review 1621; Sabeel Rahman 'Infrastructural regulation and the new utilities' (2018) 35 Yale Journal on Regulation 911.

to the extent that they have been defined as 'digital publics',[72] while there is no comprehensive research on the infrastructural role of GPAIMs.

Scholars of the public utility doctrine have largely discussed the issue of private power stemming from the control over infrastructure, highlighting how it is not only a problem of market power but also of other forms of power, such as political power.[73] This perspective can help understand the social relevance of digital infrastructures like VLOPSEs and GPAIMs and the rationale for their regulation. Frischmann established a link between infrastructures and systems, casting infrastructures in a role as the underlying frameworks for systems, including economic, cultural, social and legal systems.[74] This understanding of the rationale for the imposition of systemic risk management obligations can help frame the nature of the tasks attributed to providers of VLOPSEs and GPAIMs as systemic risk managers.

4.2.2 Situating systemic risk management as a quasi-regulatory task

This Section aims to identify common features between the DSA and the AIA that can help frame a single model in the delegation of systemic risk management responsibilities and in the design of the related architecture for supervision and enforcement by the Commission. It is important to underline that drawing a single model does not exclude that there are differences between the two frameworks, nor that there are other features in common besides the ones identified in this Section. Rather, the three features described below are selected to outline a regulatory approach that can be distinguished from other regulatory set-ups in EU law, and that poses the common challenges discussed in Section 5.2 below.

The first feature is the reliance on the notion of systemic risk as a proxy to frame questions that do not relate solely to the interpretation of legal standards and principles, such as fundamental rights, but also of politically contested concepts such as public security and civic discourse. It is not a novelty in EU law to rely on risk for the responsibilisation of regulated entities, to frame accountability relationships and to concretise legal standards.[75] The risk-based approach has characterized for several years regulatory frameworks in the areas of financial law, environmental law and digital law.[76] However, the novel element introduced by the DSA and the AIA is the use of risk to shape obligations protecting public values that are not stand-alone legal concepts and standards – as opposed to e.g. fundamental rights. While they can be related to EU constitutional principles, these values are largely undefined[77] and politically contested.[78] This feature of the regulatory model is unprecedented in EU digital legislation, and in EU law more broadly. While there are other pieces of EU legislation that require regulated entities to assess and mitigate risks to value-laden and qualitative interests, such as fundamental rights, the unique feature of systemic risk management lies in the essentially undefined, politically relevant and controversial nature of some of its protected interests. Several other pieces of legislation require to assess risks and impacts of regulatees' activities to fundamental rights, as is the case of the GDPR, the Corporate Sustainability Due Diligence Directive,[79] some provisions of the AI Act[80] and the ETIAS Regulation.[81] However, fundamental rights are

72. Danah Boyd, 'Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications' in Zizi Papacharissi (ed) *A Networked Self: Identity, Community, and Culture on Social Network Sites* (Routledge, 2010).
73. Sabeel Rahman 'The new utilities: Private power, social infrastructure, and the revival of the public utility concept' (2018) 39 Cardozo Law Review 1621, 1629; Jean-Christophe Plantin et al, 'Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook' (2018) 20 New Media & Society 293; Jedediah S. Purdy et al, 'Building a Law-and-Political-Economy Framework: Beyond the Twentieth-Century Synthesis' (2020) 129 Yale Law Journal 1784.
74. Brett M. Frischmann, *Infrastructure: The Social Value of Shared Resources* (Oxford University Press, 2012), 11.
75. Black(n 3).
76. On the description of this trend, see: Cohen and Waldman (n 6).
77. Contrary to the GDPR, where the source of risks to the fundamental right to data protection is better defined, a broad room of manoeuvre is left to providers of VLOPSEs and GPAIMs for systemic risk management.
78. Rachel Griffin, 'Governing Platforms through Corporate Risk Management: The Politics of Systemic Risk in the Digital Services Act' (2025) European Law Open, 1–31.
79. Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859 [2024] OJ L 2024/1760.
80. See Articles 9, 10, 14 and 27 AIA.
81. Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 [2018] OJ L 236/2018.

legally established concepts and, although protecting them through risk-based provisions raises its own challenges due to their intrinsically qualitative nature, they are not as vague and politically-laden as public security, civic discourse and so on.[82] Public security, civic discourse, electoral processes, public health and societal well-being as a whole carry political significance. This distinctive feature indicates the importance given to systemic risk management as the process to define, at least in part, the meaning and standards of protection of politically contested public values. As a result, the managerial and technocratic activity of risk management assumes the role of framing value-laden and political questions. A consequence of this feature is the delegation of responsibilities to regulated entities to make normative choices of a unique nature for EU law. While it could be said that all risk management obligations lead to the attribution of decision-making responsibilities, the intrinsically qualitative and political nature of the normative choices to be made is a novelty in risk-based EU regulation.

The second feature can be named as the legal allocation of powers to systemic risk managers to influence, based on their own judgment, the factual or legal entitlements of third parties, including the enjoyment of fundamental rights, in a manner that can be functionally compared to the legislative and administrative powers of public authorities. The peculiar aspect that characterizes these powers lies in the fact that the duty of providers of VLOPSEs and GPAIMs to decide on restrictions to the fundamental rights of third persons has its basis in a legal obligation. Therefore, the basis of the restriction is not solely the factual power enjoyed by the regulated entities,[83] but also the role that they have to fulfil under the DSA and the AIA by virtue of their legal obligations. This feature is most evident in the DSA. Under the DSA, providers of VLOPSEs may be required to regulate the behaviour of their users, and, if need be, to restrict their enjoyment of the right to freedom of expression, when necessary to mitigate systemic risks to conflicting public interests. This reflects a broader approach, named ''new school speech regulation'', where private powers are regulated for the end goal of regulating individuals,[84] which is not unique to the DSA.

The distinctive feature of the DSA, however, is that it can be implemented in a way that leaves regulated entities with the choice to decide whether or not legal speech should be restricted, without any other legal basis providing for such restriction. This constitutes a new and unique declination of new school speech regulation. An illustrative example in this regard is the case where disinformation is restricted to mitigate systemic risks to civic discourse and electoral processes, due to the amplification-based harm[85] created by the dissemination of disinformation. When legal online content is deemed harmful because it qualifies as disinformation, providers of VLOPSEs rely on risk as a proxy for the balancing of conflicting constitutional interests:[86] the freedom of expression of users, public interests harmed by systemic risks, and the freedom to conduct a business of private entities. This balancing substantiated in risk management constitutes the justification for the restriction of a fundamental right, and the existence of such justification stems almost entirely from a risk management decision of providers of VLOPSEs.[87] It must be noted, however, that the obligation of VLOPSEs to restrict legal content under the DSA, and the ability of the Commission

82. The only other provision that may be seen as requiring to protect a politically-laden value is Article 3(c) of Directive 2011/92/EU, which mandates an environmental impact assessment on the effects of a project on, among others, 'cultural heritage'. However, the mention of cultural heritage alongside 'material assets' suggests that this term refers to material damages to assets that are part of the cultural heritage, rather than cultural heritage as an immaterial value, such as monuments, and thus requires a more quantitative assessment.

83. Scholars have for long studied how private ordering of certain providers of digital services can mimic the asymmetrical power relations between public authorities and private citizens. See: Nicolas Suzor, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms' (2018) 4(3) Social Media and Society 1; Edoardo Celeste, 'Digital Constitutionalism: A New Systematic Theorisation' (2019) 33(1) International Review of Law, Computers & Technology 76; Giovanni de Gregorio, *Digital Constitutionalism in Europe: reframing rights & powers in the algorithmic society* (Cambridge University Press, 2022); Oreste Pollicino, 'The quadrangular shape of the geometry of digital power(s) and the move towards a procedural digital constitutionalism' (2023) 29 European Law Journal 12472.

84. Husovec (n 19); Jack M. Balkin, 'Free Speech is a Triangle' (2018) 118 Columbia Law Review 2011.

85. On the notion of amplification-based harm, see: Daphne Keller, 'Amplification and its discontents: why regulating the reach of online content is hard' (Knight First Amendment Institute at Columbia University, section on essays and scholarship, 2021) https://knightcolumbia.org/content/amplification-and-its-discontents.

86. De Gregorio and Dunn (n 2), 17-18.

87. Andrea Palumbo, 'A Medley of Public and Private Power in DSA Content Moderation for Harmful but Legal Content: An Account of Transparency, Accountability and Redress Challenges' (2024) 15 JIPITEC 246.

to require so, result from a specific interpretation of Article 35 of the DSA. European courts have never confirmed this interpretation, and it has been argued that Articles 34 and 35 of the DSA should be seen as a ''limited risk management'' regime that cannot be interpreted as requiring the imposition of new concept-specific restrictions.[88] While it is too early to confirm which is the correct interpretation, even in a limited risk management regime the adoption of content-neutral systemic risk mitigation measures can lead to interferences with freedom of expression and entail the regulation of the conduct of online users. For instance, it may be difficult to design risk mitigation measures for the systemic risks posed by disinformation that do not somehow discriminate against certain content, and VLOPSEs may decide to restrict legal content as part of their systemic risk mitigation strategies even if that is not required under the DSA. A reading of the transparency reports on systemic risk management by major VLOPs confirms that restrictions to legal content are already being reported as systemic risk mitigation measures.[89]

The third feature is the commingling of public and private orderings in conducting systemic risk management, under the supervision of the European Commission as the EU-wide meta-regulator. This has been noted by relevant scholarship in relation to the DSA and the public-private decision-making that shapes the content moderation policies of VLOPSEs' providers.[90] As argued by Schulz and Ollig, the regulatory model of the DSA goes beyond simple co-regulation where private actors implement public regulation, but entails a commingling of public and private content moderation policies that the authors named ''hybrid speech governance''.[91] This trend was noted in relation to soft law and more ''informal'' public-private collaborations on content moderation before the DSA,[92] but is now formalized in the systemic risk management regime of Articles 34 and 35. The Commission has several *ex ante* and *ex post* regulatory instruments to influence and redirect how providers of VLOPSEs conduct systemic risk management, and ultimately how they take consequential decisions on online content curation and moderation.[93] Moreover, there may not always be transparency about the avenues through which the Commission participates in the decision-making of providers of VLOPSEs. While this commingling has been discussed only in relation to the DSA to date, it can be observed also with regard to the AIA, that confers on the Commission the responsibility to supervise over compliance by providers of GPAIMs with their obligations. As under the DSA, the Commission can influence, both *ex ante* and *ex post*, systemic risk management by providers of GPAIMs. In essence, the third feature consists of a meta-regulatory model where public and private ordering can be commingled, to the extent that it may be difficult to distinguish between the two when looking at the outcomes of systemic risk management.

Looking at the three features outlined above, the regulatory model being examined can be described as follows: reliance on systemic risk as a proxy to protect and balance interests of constitutional and political relevance, including the protection of politically contestable values and how the latter can justify restrictions to fundamental rights, by attributing risk management responsibilities to private actors under the supervision of the Commission in a meta-regulatory model where public and private ordering can become indistinguishably commingled. Based on this description of the model, this paper labels the power attributed to providers of VLOPSEs and GPAIMs as ''quasi-regulatory'', as they entail the exercise of discretion that is typically reserved, in the EU legal order, to the EU legislature and the EU executive. This model, as illustrated below, raises specific questions that will need to be answered for its proper implementation.

88. Husovec (n 19) ; Husovec (n 22).

89. In relation to disinformation and misinformation see, among others, sections 6.2.2.8 and 6.2.2.14 of theMeta, *Systemic Risk Assessment and Mitigation Report for Facebook* (2024) EU DSA SRA Report 2024_Facebook_Meta https://panoptykon.org/sites/default/files/2024-12/systemic-risk-assessment_facebook.pdf .

90. Wolfgang Schulz, Christian Ollig, 'Hybrid Speech Governance New Approaches to Govern Social Media Platforms under the European Digital Services Act?' (2023) 14 JIPITEC 560.

91. ibid.

92. Rachel Griffin, 'The Politics of Algorithmic Censorship: Automated Moderation and its Regulation', in James Garratt (ed), *Music and the Politics of Censorship: From the Fascist Era to the Digital Age* (Brepols, 2025); Rocco Bellanova, Marieke de Goede, 'Co-Producing Security: Platform Content Moderation and European Security Integration' (2022) 60 Journal of Common Market Studies 1316; Michael D. Birnhack, Niva Elkin-Koren, 'The Invisible Handshake: The Reemergence of the State in the Digital Environment' (2003) 8(6) Virginia Journal of Law and Technology; Derek E. Bambauer, 'Against Jawboning' (2015) 100 Minnesota Law Review 51; Niva Elkin-Koren, 'Government–Platform Synergy and its Perils' in Edoardo Celeste et al (eds) *Constitutionalising Social Media* (Hart Publishing, 2022), 177–198.

93. Palumbo (n 87).

5. Systemic risk management in practice: open questions and outstanding challenges

5.1 Open questions: methodological challenges to operationalize a new concept

As discussed in Section 4.1 above, the novelty of the concept of systemic risk to social systems, and its novel use for the risks posed by complex technologies such as AI systems and large intermediary infrastructures, raises methodological questions for which there is not yet consensus on the answers.[94] The quest for a methodological approach can take different paths. For instance, a specific methodology may be promoted, or there may be a phase where methodological diversity is tolerated.[95] When a specific methodological approach is promoted, this could focus on the sociotechnical dimension of digital technologies and how they generate risks, or be less sensitive to the collective and dispersed risks caused by AI to typically individual interests, such as fundamental rights. As sociotechnical systems, VLOPSEs and GPAIMs not only enable systems, but constitute themselves systems with potentially deep political, economic, cultural and social impact. The risks they pose do not stem solely from their technological design as such, but also from how they dynamically interact with society.[96] On the one hand, AI models embed forward-looking policies,[97] with potentially large-scale effects,[98] that may be influenced by existing social patterns. The way in which values, biases and politics are entangled in AI systems requires new approaches that account for their ability to affect key social systems, and to be conversely shaped by social systems themselves.[99] Similar considerations can be made for large online platforms and search engines, for which there is even more copious literature about their role as infrastructures underpinning the functioning of social systems, especially as concerns freedom of speech, access to information, and civic discourse more generally.[100] Therefore, it could be argued that a sociotechnical approach is needed to appropriately account for the type of impact these technologies can have on individual, collective and societal interests.

The example of fundamental rights is instructive in understanding how different the outcomes of risk management exercises could be depending on the approach taken and how systemic risks are conceptualized. As individually-oriented rights, should fundamental rights be protected by directing risk management towards the prevention of individual harm and the violation of rights in individual cases? Or, should risk management attempt to mitigate risks of collective and structural negative effects affecting the societal systems on which the effective enjoyment of fundamental rights is premised? If the second approach is taken, how do you assess and mitigate systemic risks to individual rights, i.e. when are individual rights challenged on a systemic level? The purpose of this paper is not to provide an answer on which interpretation should be preferred. This example on fundamental rights is made to demonstrate that the interpretation of systemic risk management obligations entails important normative choices on the standard of protection that they aim to afford to protected interests. The choice of the path to take would depend on the role to be conferred to systemic risk management in addressing the risks of digital infrastructures. This is a choice that still needs to be made, and it will have significant repercussions on how risky digital technologies are regulated in the EU, as well as on the social function attributed to the risk managers.

Before a specific methodology for the operationalization of systemic risk management is developed, it is thus essential to first determine what systemic risks are, and which is the rationale of the related obligations

94. Regarding the diversity of views on systemic risk management under the DSA, see: Oliver Marsh, 'Researching Systemic Risks under the Digital Services Act' (2024) https://algorithmwatch.org/en/researching-systemic-risks-under-the-digital-services-act/.
95. Loi et al. (n 56).
96. Brian J. Chen , Jacob Metcalf, 'Explainer: A Sociotechnical Approach to AI Policy' (2024) Data & Society, https://datasociety.net/library/a-sociotechnical-approach-to-ai-policy/;Mariano-Florentino Cuéllar, Aziz Z. Huq, 'Toward the Democratic Regulation of AI Systems: A Prolegomenon' Public Law and Legal Theory Working Papers No. 753(2020), http://dx.doi.org/10.2139/ssrn.3671011.
97. Hideyuki Matsumi, Daniel J. Solove, 'The Prediction Society: AI and the Problems of Forecasting the Future' (2025) Illinois Law Review 1.
98. Smuha (n 39).
99. For instance, scholars have argued for more participatory and democratic governance models for AI, see: Linnet Taylor, 'Can AI governance be progressive? Group interests, group privacy and abnormal justice' in Andrej Zwitter, Oskar Gstrein (eds) *Handbook on the politics and governance of big data and artificial intelligence* (Edward Elgar Publishing, 2023); Cuéllar andHuq (n 96).
100. See, among others: Natali Helberger et al, 'Regulation of news recommenders in the Digital Services Act: empowering David against the Very Large Online Goliath' Internet Policy Review https://policyreview.info/articles/news/regulation-news-recommenders-digital-services-act empowering-davidagainst-very-large; Jean-Christophe Plantin, Aswin Punathambekar, 'Digital media infrastructures: pipes, platforms, and politics' (2018) 41(2) Media, Culture & Society 163.

laid down in the DSA and the AIA. Once again, the example of fundamental rights is instructive. On the one hand, systemic risks to fundamental rights could be understood as risks stemming from digital technologies as systems, and that affect individual rights as such and not due to their interconnection with a social system. On the other hand, systemic risks can be conceptualized as risks to societal systems on which the enjoyment of fundamental rights is predicated. The proper functioning of these societal systems is a precondition for the effective enjoyment of fundamental rights, and for this reason even collectively dispersed harm that affects them should be prevented through systemic risk management. As evidenced by scholarship acknowledging the dispersed, subtle, aggregate and collective impact of digital technologies on fundamental rights,[101] focusing solely on individual cases does not allow to properly measure the risks posed by complex sociotechnical systems like AI and online platforms.[102] It is under this light that the rationale for the management of systemic risks to fundamental rights can be found in distributive justice. Distributive justice is about the allocation of life opportunities[103] and risks,[104] and focuses on public interests.[105] When adopted as underlying rationale for a duty of care, this duty is understood as directed also towards the public at large rather than solely single individuals. The relationship between distributive justice and the regulation of digital technologies has been conceptualised from a philosophical standpoint,[106] but distributive justice has also been proposed as a conceptual framework to interpret obligations to protect fundamental rights.[107]

The considerations made above show how the new legislative phenomenon that relies on systemic risk to frame obligations and regulatory objectives raises normative questions that are still to be answered. These questions are not only about legal interpretation, but should also be answered considering the larger political, regulatory and societal expectations about this new regulatory model and the ways it should tackle the risks of large digital infrastructures in modern society. In other words, a normative choice is still to be made that goes beyond the interpretation of legal texts. This conclusion about the uncertain interpretation and implementation of systemic risk management obligations is an important factor that must be taken into account also to frame the nature of quasi-regulatory responsibilities of the entities involved in systemic risk management. The absence of a clear methodological basis, and the need to make normative choices that go beyond legal interpretation, qualifies the nature of the responsibilities that actors involved in the implementation of these regimes are entrusted with. This is an important starting point for the discussion on the outstanding challenges for legitimacy and the rule of law made below.

5.2 Outstanding challenges: legitimacy and the rule of law

Section 4.2 above outlines a number of common features of the systemic risk management regimes in the DSA and the AIA, that characterize the powers entrusted to regulated entities as quasi-regulatory, i.e. presenting some commonalities with the powers typically entrusted to public bodies. The purpose of this paper is not to exhaustively discuss the legal concerns raised by the delegation of such powers to private actors, but rather to outline them as outstanding challenges that will need to be addressed. This is in line with the research question and objective of this paper, i.e. to frame the regulatory model and the questions it raises, paving a path for future research.

101. Sue Anne Teo, 'The Unbearable Likeness of Being: How Artificial Intelligence Challenges the Social Ontology of International Human Rights Law' (2025) 2 The Journal of Cross-Disciplinary Research in Computational Law; Taylor (n 99); Linnet Taylor et al (eds), *Group Privacy: New Challenges of Data Technologies* (Springer Cham, 2016); Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30 Philosophy & Technology 475; Karen Yeung, 'A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework', (Council of Europe Report DGI(2019)05, 2019).

102. Linnet Taylor stated that '*making sense of technology and rights through a lens of individual applications and related harms makes very limited sense, and we now require a vocabulary and an imaginary that can make sense of the relationship of systematic technologies to systematic problems*'. See: Taylor (n 99).

103. Amartya Sen, *The Idea of Justice* (Harvard University Press, 2009).

104. Marc Loth, 'Corrective and distributive justice in tort law: On the restoration of autonomy and a minimal level of protection of the victim' (2015) 22 Maastricht Journal of European and Comparative Law 788.

105. Vladislava Stoyanova, 'Common law tort of negligence as a tool for deconstructing positive obligations under the European convention on human rights' (2020) 24 The International Journal of Human Rights 642.

106. Iason Gabriel, 'Toward a Theory of Justice for Artificial Intelligence' (2022) 151 Daedalus 218.

107. Stoyanova (n 105).

There are two outstanding challenges faced by this regulatory model: can private actors be delegated the quasi-regulatory responsibilities they are entrusted with, and if yes, is this regulatory model compliant with the rule of law?

First, the fact that private actors interpret, protect and balance constitutional values, some of which have political relevance, through the notion of risk has already been flagged as problematic. Concerns have been voiced around legitimacy, reinforcement of corporate power and technocratic management of questions that need democratic deliberation.[108] These problems can be connected with the broader regulatory trend that Cohen and Waldman have branded as regulatory managerialism, and pose questions of whether the increasing outsourcing of regulatory tasks to private actors leads to desirable outcomes – especially considering the conflict of interest of these actors to pursue risk management policies that are commercially most convenient.[109] This alone can be a political, regulatory and social problem, but there is also the question of whether it is a legal problem. The delegation to private actors of powers to frame regulatory questions through risk management, and consequent technological design[110] choices, needs to be thoroughly examined in light of EU legal standards. In the landmark *Meroni* judgment,[111] the Court of Justice of the European Union elaborated a principle of ''balance of powers'' to examine the legality under the Treaties of delegating powers to private law bodies. The *Meroni* doctrine, that has been developed over the years on the basis of that judgment, still presents some unclear aspects to date for which it has been criticized. However, it is clear that it imposes limitations as to what can be delegated by the EU legislature to other actors, in order to preserve a reserve to the legislature of political choices. A reconstruction of the *Meroni* doctrine in light of the delegation of powers in systemic risk management is warranted.

While the delegation of powers to private actors and administrative authorities is not new nor unique to systemic risk management regimes, these regimes present new features, as described above, that introduce new and unique concerns. On the one hand, as discussed above,[112] it is a unique case where the values to be substantiated and protected through risk assessment and mitigation are not quantifiable nor legally defined concepts like fundamental rights, and may also entail the exercise of political discretion. While it may be challenging to define what is a political choice in the EU legal order, systemic risk management raises this question that needs to be addressed for the first time in the context of EU risk-based regulation. Second, another salient feature of systemic risk management, as identified above,[113] lies in the fact that regulated entities may be called on to decide on whether it is justified to restrict a fundamental right in light of conflicting public interest objectives. This is also a new, unique feature of risk-based regulation, that before the DSA had solely entrusted private actors with the task to protect fundamental rights through risk management, and not to decide on whether and how they should be restricted. Therefore, it is important to understand how the choices delegated to private actors, as well as the Commission as the meta-regulator, could qualify as 'political' choices that should be reserved to the EU legislature in the EU legal order. This would lead to a legal analysis that engages with the legitimacy concerns raised thus far, but grounding such concerns in primary EU law.

Second, a related but separate issue concerns the compatibility of the regulatory model under analysis with the EU rule of law. In particular, the commingling of public and private action may challenge the public-private divide on which the rule of law is premised.[114] This feature requires an analysis using the rule of law, as understood in the EU legal order, as an evaluative framework. While it is not clear which is the prescriptive value of the rule of law as a standalone legal standard in the EU legal order, it is a foundational

108. Griffin (n 78); Carsten Orwat et al, 'Normative Challenges of Risk Regulation of Artificial Intelligence' (2024) 18 Nanoethics 18; Cohen andWaldman (n 6).
109. Martin Senftleben et al, 'How the EU Outsources the Task of Human Rights Protection to Platforms and Users: The Case of UGC Monetization' (2023) 38 Berkeley Technology Law Journal 933.
110. On the delegation of normative choices through regulation by design, see: Marco Almada, 'Regulation by Design and the Governance of Technological Futures' (2023) 14 European Journal of Risk Regulation 697.
111. Court of Justice of the European Union, Joined Cases C-9/56 and C-10/56 *Meroni v High Authority* [1957/1958] ECR 133.
112. See Section 4.2.2.
113. See Section 4.2.2.
114. Andrea Palumbo, Charlotte Ducuing, 'The Blurring of the Public-Private Dichotomy in Risk-based EU Digital Regulation: Challenges for the Rule of Law' (2025) available on SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5397112.

value of the EU[115] and a legally binding constitutional principle.[116] Frictions with the rule of law created by secondary legislation would thus raise concerns, at least as a matter of internal consistency in EU law. The rule of law is considered as the foundation of several general principles of EU law,[117] and it is in light of those that systemic risk management regimes should be evaluated. Existing literature has already identified challenges arising from public-private collaboration in shaping content moderation policies in relation to transparency and accountability of, and access to justice against, public action.[118] These challenges can implicate three constituent principles of the rule of law, namely transparency, accountability and access to justice. However, the regulatory model should also be analysed under the lens of other principles, such as separation of powers, prevention of arbitrariness and abuse of power. By looking at the regulatory model for systemic risk management of the DSA and the AIA as a whole it is possible to understand how the blurring of the public-private divide that this model entails fares in relation to a basic principle of the EU legal order.

Further research is needed in relation to the questions highlighted above. While it is beyond the scope of this paper to address them, this section aims to demonstrate that systemic risk management regimes should be examined as a standalone regulatory model that may challenge the constitutional order of the EU as traditionally understood. Besides the points of frictions that can be identified on the basis of the legislative text alone, empirical research is also needed to understand how the practical implementation of the DSA and the AIA confirms or exacerbates such frictions.

6. Conclusions

This paper has analysed systemic risk management as a new phenomenon in EU digital legislation. The underlying research was thus directed at the description, analysis and systematic theorisation of the new obligations on systemic risks laid down in the DSA and the AIA. In order to frame a new stand-alone regulatory approach, the commonalities between systemic risk management regimes in the DSA and in the AIA have been examined. This analysis has shown that the two regimes share a similar rationale, the central notion of systemic risk and key features in the overall regulatory model.[119] The overlapping scope of application and rationale has also been acknowledged in the legislative text and other policy documents. This paper has rationalized and conceptualized the commonalities by identifying two overarching common features, on the basis of which it is possible to characterise a single regulatory approach: i) the notion of system and how it relates to the digital infrastructures operated by regulated entities, ii) the nature of the responsibilities delegated to regulated entities and the surrounding supervisory and enforcement architecture.

Framing systemic risk management regimes as a single regulatory approach allows to provide an overview of their distinctive features as well as of the outstanding questions and challenges that they pose. Moreover, the overview provided in this paper is intended to help identify connections between features, open questions and challenges, facilitating the formulation of questions for future research. For instance, the precise meaning to be ascribed to systemic risks, and how the related duties of care for risk management should be constructed, is a question that should be answered taking into account how the conferral of certain powers to private actors challenges the rule of law. Conversely, if any safeguards had to accompany systemic risk management to align the DSA and the AIA with rule of law principles, these would contribute to shaping the actions and methodology adopted in risk management exercises. For instance, the safeguards could take the form of transparency requirements, or of measures to increase contestability and democratic participation

115. See Art. 2 of the Treaty on European Union.
116. European Commission, 'A new EU Framework to strengthen the Rule of Law' [2014] COM(2014) 158 final; Marc Bungenberg, Angshuman Hazarika 'Rule of Law in the EU Legal Order' (2019) 22 Zeitschrift für europarechtliche Studien, 383.
117. Theodore Konstadinides, 'The rule of law as the constitutional foundation of the general principles of EU law', in Katja S. Ziegler et al, (eds) *Research Handbook on General Principles of EU Law: Constructing Legal Orders in Europe* (Edward Elgar Publishing, 2022).
118. Daphne Keller, 'Who Do You Sue? State and Platform Hybrid Power over Online Speech' (2019) Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1902 https://www.lawfareblog.com/who-do-you-sue-state-and-platform-hybrid-power-over-online-speech ; Palumbo (n 87).
119. See Sections 2 and 4.

in systemic risk management.[120] A second example is the relationship between the digital infrastructures managed by regulated entities and social systems. More research is needed to understand what makes certain products and services riskier for social systems and society as a whole, and how the different nature of the risks posed justifies a different approach to risk management. An understanding of these aspects as intertwined and connected to the same features of an emerging regulatory approach hopefully contributes to the advancement of research on the implementation of the crucial and vague requirements of the DSA and the AIA analysed in this paper.

As a final concluding remark, it was noted above that systemic risk management regimes represent an absolute first in EU law. For this reason, they inevitably pose questions that have never been asked or answered before. Moreover, this regulatory approach also attempts to tackle new problems of governance over consequential digital infrastructures that have never arisen before, or at least that the EU legislator has not aimed to address in such organic manner. Given the novelty of both modes of regulation and the problems to be addressed through regulation, proposals for the way forward should go beyond a purely legalistic approach. Rather, they are an opportunity to make normative choices on where it is most desirable for society to go in regulating digital technologies, and in particular the digital infrastructures operated by so-called ''BigTech''. This is not only a legal, but also a political and ethical, question.

120. Contestability and stakeholders' participation in AI risk management have been proposed as elements of a sociotechnical perspective. See: Merel Noorman, Tsjalling Swierstra, 'Democratizing AI from a Sociotechnical Perspective' (2023) 33 Minds & Machines 563.