It will be what we want it to be: Sociotechnical and Contested Systemic Risk at the Core of the EU's Regulation of Platforms' AI Systems

by **Mateus Correia de Carvalho** *

Abstract: The EU regulates AI systems of large digital platforms using a risk-based approach developed primarily through the Digital Services Act (DSA) and the AI Act (AIA). The existing literature highlights two main challenges to this regulatory strategy: the potentially unconstrained discretion and informational power of regulated tech companies, and the limited predictive value of risk regulation for less quantifiable forms of harm. This paper describes and systematises how EU law intends to address these challenges and ensure effective AI risk management processes. Through doctrinal analysis of the DSA, AIA, and their implementing laws and soft law, it lays out the integrated risk management framework these regulations establish for platforms' AI systems. It argues that this integrated framework has three main normative commitments: (i) AI systemic risks should be framed sociotechnically, (ii) their management should be methodologically contextual, and (iii) and civil society should be actively involved in identifying and mitigating AI systemic risks. On this last commitment, however, the mechanisms for civil society participation remain especially unclear. This paper thus offers an overview of all formal and informal spaces of participation in this risk management framework, differentiating them by their institutional setup, rationales for civil society intervention, types of expertise sought, and actors involved. Overall, this paper advances the dialogue on the EU's risk-based approach to platform and AI regulation, offering a possible baseline for critique and empirical inquiry into its implementation.

Keywords: AI Systems; Digital Platforms; Systemic Risk; Participation; EU Law

Recommended citation: Mateus Correia de Carvalho, It will be what we want it to be: sociotechnical and contested systemic risk at the core of the EU's regulation of platforms' AI systems, 16 (2025) JIPITEC 35 para 1.

A. Introduction

1 The emergence and increasing integration of AI-driven recommender systems[1] and generative AI[2] on digital platforms create risks of harm to persons' fundamental rights, health, and safety.[3]

* Doctoral Researcher, European University Institute (EUI), Fiesole, Italy. I would like to sincerely thank Deirdre Curtin, Rachel Griffin, Marta Maroni, Estela Lopes, Pankhudi Khandelwal, Renan Bodin, Alex Schuster, Johannes Müller, Marco Almada, Julia Galera Oliva, Mary Greenshields, and Timo Zandstra for commenting on earlier versions. This paper was presented at the Young Digital Law Conference 2024, hosted by Sciences Po (Paris) where it benefitted from the precious feedback of Ilaria Buri, Paddy Leerssen, Jenny Orlando-Salling and Louise Bartolo. I also greatly appreciate the peer review comments which improved the paper greatly. All remaining mistakes are mine.

1 Since this article mainly looks at the EU's Digital Services Act (DSA), it defines AI recommender systems per its Article 3(s) as fully or partially algorithmically driven systems "used by an online platform to suggest" and/or prioritise specific information "in its online interface".

2 Defined as "advanced machine learning models that are trained to generate new data, such as text, images, or audio", which makes them "distinct from other AI models, only designed to make predictions or classifications or to fulfil other specific functions" in Philipp Hacker, Andreas Engel and Marco Mauer, 'Regulating ChatGPT and Other Large Generative AI Models', *2023 ACM Conference on Fairness, Accountability, and Transparency* (ACM 2023) 1113 <https://dl.acm.org/doi/10.1145/3593013.3594067> accessed 20 January 2024.

3 Recitals 81 and 83 DSA and 15-16 AI Act (AIA); Kate Crawford, 'Can an Algorithm Be Agonistic? Ten Scenes from Life in Calculated Publics' (2016) 41 Science, Technology, & Human Values 77, 83–85; Brent Daniel Mittelstadt and others, 'The

Platforms' AI systems[4] also pose broader societal risks to democracy and civic discourse, as they have the potential to manipulate individuals' perception of reality,[5] mediate a significant part of their social interactions,[6] and, therefore, shape how they relate to one another in society.[7] Specifically, they may contribute to increasing polarization of public opinion,[8] and affect the integrity of electoral processes,[9] interfere with people's free access to and exchange of information,[10] and perpetuate long-standing patterns of discrimination and marginalisation of certain individuals and communities.[11]

2 But these are, in the end, just risks. What are, and will be, the specific negative impacts of digital platforms' AI systems on individuals and societies? Even if we may have some idea, no one can claim to know for sure the answer to this question. Indeed, AI's technical complexity and opacity,[12] coupled with its rapid development and varied integration in digital platforms,[13] make it very hard for regulators to gauge the harms it might cause and adopt suitable strategies to address them.[14]

3 In order to cope with these uncertainties and dynamically regulate AI systems, the EU has adopted a risk-based approach.[15] Specifically, it applies

Ethics of Algorithms: Mapping the Debate' (2016) 3 Big Data & Society 9–10.; Brent Daniel Mittelstadt and others, 'The Ethics of Algorithms: Mapping the Debate' (2016) 3 Big Data & Society 9–10.

4 Any reference to the 'AI systems' of digital platforms made henceforth should be understood, unless a more specific distinction is made, as comprising the two different types of algorithmic systems mentioned in footnotes 1 and 2: (i) algorithmic recommender systems; and (ii) generative AI models (hereinafter 'genAI').

5 Recitals 67 DSA and 16 AIA; Rostam J Neuwirth, *The EU Artificial Intelligence Act: Regulating Subliminal AI Systems* (Routledge 2022).

6 Jennifer Cobbe, 'Algorithmic Censorship by Social Platforms: Power and Resistance' (2021) 34 Philosophy & Technology 739, 739–743.

7 Recital 79, DSA; Daniel Yudkin, Stephen Hawkins and Tim Dixon, 'The Perception Gap: How False Impressions Are Pulling Americans Apart' [2019] More in Common 6, 49, 51.

8 Smitha Milli and others, 'Engagement, User Satisfaction, and the Amplification of Divisive Content on Social Media' (arXiv, December 2023) 6–7 <http://arxiv.org/abs/2305.16941> accessed 23 September 2024. Polarization, like many other effects of platforms' AI systems is a product of the entanglement between the latter, platforms interfaces, associated devices and technical infrastructure, individuals, and other social systems. See, to this effect, Sinan Aral, *The Hype Machine: How Social Media Disrupts Our Elections, Our Economy, and Our Health–and How We Must Adapt* (Crown Currency 2021) 3, 56–93; Cass R Sunstein, *#Republic: Divided Democracy in the Age of Social Media* (Princeton University Press 2018) 59–97.

9 European Commission, Directorate-General for Communications Networks, 'Digital Services Act: Application of the Risk Management Framework to Russian Disinformation Campaigns' (Publications Office of the European Union, 2023) 59–63; 'Consultation on Guidelines for Providers of Very Large Online Platforms and Very Large Online Search Engines on the Mitigation of Systemic Risks for Electoral Processes' (European Commission, 2024) paras. 1, 3, 25, and 26, including cited sources.

10 Recital 82 DSA; Rishi Bommasani and others, 'On the Opportunities and Risks of Foundation Models' (arXiv, 2022) 137 <http://arxiv.org/abs/2108.07258> accessed 13 December 2023; Paul Bouchaud and others, 'The Amazing Library: An Analysis of Amazon's Bookstore Algorithms within the DSA Framework' (AI Forensics; Check First 2023) 38 <https://checkfirst.network/wp-content/uploads/2023/12/AIF%20x%20CF%20-%20The%20Amazing%20Library_final.pdf> accessed 23 September 2024.

11 Beatriz Botero Arcila and Rachel Griffin, 'Social Media Platforms and Challenges for Democracy, Rule of Law and Fundamental Rights' (Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, PE 2023) 10; Benjamin Laufer and Helen Nissenbaum, 'Algorithmic Displacement of Social Trust' (Knight First Amendment Institute 2023) 5 <https://s3.amazonaws.com/kfai-documents/documents/a29f3e5731/1.23.24-SocialTrust-Draft.pdf> accessed 16 February 2024.

12 Jenna Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3 Big data & society.

13 Stefan Larsson, Jockum Hildén and Kasia Söderlund, 'Between Regulatory Fixity and Flexibility in the EU AI Act' 3–5 <https://portal.research.lu.se/en/publications/between-regulatory-fixity-and-flexibility-in-the-eu-ai-act> accessed 15 March 2024; Paddy Leerssen, 'Embedded GenAI on Social Media: Platform Law Meets AI Law' (*DSA Observatory*, 16 October 2024) <https://dsa-observatory.eu/2024/10/16/1864/> accessed 22 October 2024; Mathias Vermeulen and Laureline Lemoine, 'From ChatGPT to Google's Gemini: When Would Generative AI Products Fall within the Scope of the Digital Services Act?' (*Media@LSE*, 12 February 2024) <https://blogs.lse.ac.uk/medialse/2024/02/12/from-chatgpt-to-googles-gemini-when-would-generative-ai-products-fall-within-the-scope-of-the-digital-services-act/> accessed 20 February 2024.

14 Larsson, Hildén and Söderlund (n 13).

15 Giovanni De Gregorio and Pietro Dunn, 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age' (2022) 59 Common Market Law Review 473, 476; Margot E Kaminski, 'The Developing Law of AI: A Turn to Risk Regulation' (2023) 3 <https://papers.ssrn.com/abstract=4692562> accessed 31 January 2024. For a discussion of other reasons for the adoption of risk-based regulation in digital governance matters, not often stated in policy documents and official communications, see, for example, Rachel Griffin, 'What Do We Talk about When We Talk about Risk? Risk Politics in the EU's Digital Services

such an approach to the regulation of AI systems of very large online platforms and search engines (hereinafter referred to as 'platforms', 'digital platforms' or 'VLOP/SEs'[16]) through the recent Digital Services Act (DSA)[17] and AI Act (AIA).[18]This approach frames AI's potential negative impacts as future risks of harm. It also mandates that private entities responsible for AI systems related to platforms establish processes for the iterative management of these risks.[19] The setting up and implementation of those risk management processes are then overseen by public supervisory authorities.[20]

4 The literature has pointed out that, like all risk regulation, the risk-based approach to AI regulation adopted in the DSA and AIA will face two main challenges. The first is conceptual: risk is often conceived in an actuarial and individual fashion, i.e., it focuses on quantitatively identifying and assessing risks of harm caused to specific individuals or entities.[21] These dominant conceptions of risk, while easier to calculate, fail to fully capture less quantifiable and intangible AI risks – e.g., to democracy, fundamental rights, civic discourse, or of gender-based violence – whose perceptions are contestable and highly subjective but that both the DSA and AIA aim to address.[22] The second challenge is institutional: risk regulation affords significant discretion to private regulated actors to set up risk management processes and strategies,[23] which might lead to ineffective and insufficient risk assessment and mitigation.[24]

5 Against this background, this paper aims to address how the DSA and AIA envision the creation of an effective risk regulatory regime applicable to the AI systems of digital platforms. Answering this question is, first and foremost, a descriptive exercise based on the legal doctrinal method. It requires reviewing the applicable legal sources and systematically describing the AI risk management schemes they institute.[25] In this case, it is important not only to describe the AI risk management provisions of the DSA and AIA, but also the legal acts and soft law instruments that concretise them. These are:

- the Commission Delegated Regulation (EU) 2024/436 of 20 October 2023 laying down rules on the performance of audits for very large online platforms and very large online search engines (hereinafter, the 'Delegated Regulation on Audits', or 'DRA');
- the Commission Implementing Regulation (EU) 2023/1201 of 21 June 2023 on detailed arrangements for the conduct of certain proceedings by the Commission pursuant to the DSA (hereinafter, the 'Implementing Regulation 2023/1021');

Act' (*Digital Services Act Observatory*, 31 July 2024) <https://dsa-observatory.eu/2024/07/31/what-do-we-talk-about-when-we-talk-about-risk-risk-politics-in-the-eus-digital-services-act/> accessed 2 September 2024.

16 In this paper, I rely on the definition of 'digital platforms' used in the DSA's risk management provisions. Therefore, in accordance with art. 33(1) DSA, whenever this paper mentions 'digital platforms', 'platforms', or 'VLOP/SEs', these terms should be understood as referring to very large "online platforms and online search engines which have a number of average monthly active recipients (...) in the Union equal to or higher than 45 million".

17 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), OJ L 277 2022.

18 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), PE/24/2024/REV/1, OJ L, 2024/1689 2024.

19 Gregorio and Dunn (n 15) 476; Daniela Stockmann, 'How Will the European Union Govern Social Media Platforms under the Digital Services Act?' (*Hertie School Centre for Digital Governance*, 16 June 2023) <https://www.hertie-school.org/en/digital-governance/research/blog/detail/content/how-will-the-european-union-govern-social-media-platforms-under-the-digital-services-act> accessed 26 December 2023; Margot E Kaminski, 'Regulating the Risks of AI' [2023] Boston University Law Review 1347.

20 Fiona Haines, 'Regulation and Risk' in Peter Drahos (ed), *Regulatory theory: Foundations and applications* (Australian National University Press Acton, ACT, Australia 2017) 188–192; Martin Husovec, 'The Digital Service Act's Red Line: What the Commission Can and Cannot Do About Disinformation' (2024) 1, 7 <https://papers.ssrn.com/abstract=4689926> accessed 16 January 2024.

21 Kaminski (n 19) 1390–1391; Kaminski (n 15) 14–16.

22 See, e.g., recitals 44d AIA and 75 DSA. See also Kaminski (n 19) 1392–1393; Marco Almada and Nicolas Petit, 'The EU AI Act: A Medley of Product Safety and Fundamental Rights?' (2023) SSRN Paper 18–19; European Commission, 2023 (n 9) 11, 15-18.

23 Julia Black and Andrew Douglas Murray, 'Regulating AI and Machine Learning: Setting the Regulatory Agenda' (2019) 10 European journal of law and technology 4–7; Kaminski (n 19) 1379; Gregorio and Dunn (n 15) 483–488.

24 Kaminski (n 19) 1379-1380; Niklas Eder, 'Making Systemic Risk Assessments Work: How the DSA Creates a Virtuous Loop to Address the Societal Harms of Content Moderation' (2023) 13 <https://papers.ssrn.com/abstract=4491365> accessed 31 October 2023.

25 Jan M Smits, 'What Is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research' in Rob van Gestel, Hans-Wolfgang Micklitz and Edward L Rubin (eds), *Rethinking Legal Scholarship: A Transatlantic Dialogue* (Cambridge University Press 2017) 207, 210.

- the Commission Decision of 24 January 2024 establishing the European AI Office, C(2024) 390 final (hereinafter, the 'AI Office Decision');
- the Commission Draft Delegated Regulation laying down the technical conditions and procedures under which providers of very large online platforms and of very large online search engines are to share data pursuant to Article 40 of Regulation (EU) 2022/2065 (hereinafter, the Access to Data Delegated Regulation);
- the Commission DSA draft guidelines for platforms on mitigating risks for electoral processes (hereinafter, the 'DSA risk mitigation guidelines');[26]
- the 2023 Commission study applying the DSA's risk management framework to Russian disinformation campaigns (hereinafter, the 'DSA Russian disinformation study');[27] and
- the 2022 Strengthened Code of Practice on Disinformation (hereinafter, 'Disinformation Code of Practice').[28]

6 Because it conceives of law as a system, the doctrinal method is adequate to both (i) provide coherence to the many different provisions applicable to a given regulated matter and (ii) extract from those legal texts their normative meaning as ascribed to them by the legislator. In this paper, I thus use the doctrinal method to structure the DSA and AIA's risk management frameworks into a coherent system, all the while trying to understand the broader internal value-based logic that underpins it. This means that, besides simply describing their legal norms and competent institutions, I will also provide an interpretative analysis of the two regulations' own normative commitments and aspirations regarding how their risk management schemes *should* be enforced. Structuring the EU law regime of platform and AI risk management in this way will enable its future intra and extra-legal critique . For one, clearly stating the normative commitments and aspirations of the DSA and AIA's risk management regimes will allow, in time, for a critique of their implementation on the regulations' own terms.[29] In addition, highlighting those normative ambitions can also enable their own critique from extra-legal viewpoints that uncover and scrutinise the interests they serve, produce and help reinforce (and at the expense of whom they do so).[30]

7 Section B. argues that the DSA and AIA were conceived as instituting two different but complementary AI risk management schemes. After clarifying the relationship between the two regulations, I will separately describe the two risk management regimes they establish for platforms' AI systems.

8 Then, in Section C., I distil the commonalities between the two regulations' AI risk regimes that ultimately unify them into, I argue, one integrated EU AI risk governance framework applied to digital platforms. To do so, I combine the legal analysis of the DSA and AIA with insights taken from their *travaux préparatoires*, related policy documents and relevant literature. Particularly, I highlight three overarching normative commonalities of the two regulations' AI risk management schemes: they frame (at least some) AI risks as 'systemic' (C.I.); require that the assessment and mitigation of those risks be socially contextualised (C.II.) and expect civil society actors to be involved in those risk management processes (C.III.) Admittedly, the choice to focus on these three normative objectives of the DSA and AIA has, itself, a certain underlying normativity: it implies that the focus of the analysis of these risk management regimes is put not on their market regulation objectives but instead on their non-market, protective aims.[31] Simply put, I identify the DSA and AIA's three main normative commitments regarding how risk management procedures should be shaped in order to protect such values as fundamental rights, democratic processes, and public health and safety.

9 Of the three highlighted normative ambitions of the DSA and AIA's risk management frameworks, one has a particularly unclear path towards operationalisation: civil society involvement. Notably, the concrete procedures for civil society

26 European Commission, 2024 (n 9).

27 European Commission, 2023 (n 9).

28 'European Commission, The 2022 Strengthened Code of Practice on Disinformation', <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation>.

29 Martijn Willem Hesselink, 'Knowing EU Law : How Epistemic and Ontological Commitments Shape Different Understandings of European Law and Why It Matters' (European University Institute 2024) Working Paper 15 <https://cadmus.eui.eu/handle/1814/76827> accessed 3 May 2024.

30 Ioannis Kampourakis, 'Bound by the Economic Constitution: Notes for "Law and Political Economy" in Europe' (2021) 1 Journal of Law and Political Economy 301; Hesselink (n 29) 15–19.

31 As De Gregorio and Dunn (n 15) put it, these EU risk-based regulations seek to find a balance between market objectives, such as technological innovation, and non-market protection, such as fundamental rights protection. For a broader distinction between EU secondary law's market and non-market aims, see Bruno de Witte, 'Non-Market Values in Internal Market Legislation' in Niamh Nic Shuibhne (ed), *Regulating the Internal Market* (Edward Elgar Publishing 2006).

participation in this risk management framework are not defined in law . References to different civil society actors are scattered through the provisions of the two regulations, which mention different rationales and forms of civil society interventions in AI risk management. In addition, legal mobilisation literature points to the fact that civil society might intervene informally - and not just through formal avenues of public participation - in the implementation of EU legislation.[32] However, it is not clear what informal avenues of civil society involvement could be used to influence the implementation of the DSA and AIA's risk governance regimes. Although a full answer to these questions necessarily requires an empirical analysis, this paper takes a necessary first step. Section D. maps (i) what are, in the abstract, the formal and informal avenues of civil society participation in EU's AI risk governance, (ii) which civil society actors are empowered to participate therein, (iii) under what type of institutional setting, and (iv) with what aims. Section E. offers concluding remarks.

B. The DSA and AIA as an integrated risk management framework of platforms' AI systems

10 The development of the EU's Digital Strategy has led to the adoption of numerous new instruments of secondary law updating or adding to the existing EU law *acquis* governing digital governance matters.[33] When it comes to the regulation of the AI models and systems integrated into or whose output is diffused through digital platforms, two regulations are primarily relevant: the DSA and the AIA.[34]

11 In this section, I conceive the DSA and the AIA as instituting an integrated EU risk management framework applicable to platforms' AI systems. Before separately describing the relevant provisions of the DSA (B.I.) and AIA (B.II.), it is important to systematise how they relate to one another. Indeed, the two regulations' AI risk-based regimes apply to digital platforms' AI systems in different but complementary ways. This complementarity is highlighted by the AIA's *travaux préparatoires* and the DSA risk mitigation guidelines, which stress the need to ensure a consistent implementation of the two regulations.[35] But what does that exactly mean?

12 The AIA answers that question by stating that, to the extent that AI systems and models are embedded into VLOP/SEs, the latter should manage the systemic risks of those systems and models through the DSA's framework. Compliance with this framework means that corresponding systemic risk management obligations of the AIA "should be presumed to be fulfilled". The AIA's systemic risk management regime will nonetheless come into play if "significant systemic risks" not covered in the DSA are identified in platforms' AI systems and models.[36]

13 Two conclusions can be inferred from the foregoing. First, the DSA is the primary instrument that governs the risks posed by the AI systems of digital platforms. This means, in essence, that platforms must assess and mitigate emerging AI systemic risks at least once a year and in any event prior to launching any new AI-driven or AI-related feature or functionality of their services (art. 34-35 DSA). Second, the AIA functions as a residual regime for new emerging systemic risks that do not fit the DSA's mould.[37] In view of this communication between the DSA and AIA, some scholars have proposed that systemic risk analyses under the two regulations draw inspiration from each other or, even further, be done in integration, i.e., in one analysis considering platform-specific risks that the DSA focuses on, AI-specific risks addressed by the AIA, and also those risks produced by the entanglement between AI and digital platforms' architecture.[38]

32 Elise Muir, Mark Dawson and Monica Claes, 'A Tool-Box for Legal and Political Mobilisation in European Equality Law' in Dia Anagnostou (ed), *Rights and Courts in Pursuit of Social Change: Legal Mobilisation in the Multi-Level European System* (2014); Lisa Conant and others, 'Mobilizing European Law' (2018) 25 Journal of European Public Policy 1376.

33 European Commission, 'Communication from the European Commission: Report on the State of the Digital Decade 2024' (2024) 7–8.

34 This is not to the exclusion of other previously adopted and still relevant EU digital regulations such as the General Data Protection Regulation. In this sense, see, for example, Margot E Kaminski and Gianclaudio Malgieri, 'Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations' (2021) 11 International Data Privacy Law.

35 European Commission, 2024 (n 9), para. 58; European Commission, AI Act proposal, COM (2021) 206 final, 2021/0106 (COD), 5.

36 Recital 118 AIA.

37 For a similar argument and a broader analysis of the intersections between the DSA and AIA, see Leerssen (n 13).

38 Natali Helberger and Nicholas Diakopoulos, 'ChatGPT and the AI Act' (2023) 12 Internet Policy Review 4; Philipp Hacker, 'The AI Act between Digital and Sectoral Regulations' (Bertelsmann Stiftung 2024) 17–19 <https://www.bertelsmann-stiftung.de/doi/10.11586/2024188> accessed 28 January 2025.

I. The core: the Digital Services Act and systemic risk management

1. Risk assessment

14 As outlined above, the DSA is the main instrument that platforms should take into account when managing the risks of their AI systems in accordance with EU law. The first step that VLOP/SEs need to take in this respect is to engage in risk assessment (art. 34 DSA). In essence, they must identify and assess the impact of any systemic risks in the Union stemming from the design, functioning, or use of their services and, amongst others, related algorithmic systems.[39]

15 For a certain risk to be identified and assessed in the DSA's risk management framework, that risk must be qualified as 'systemic'. Crucially, the DSA contains no clear definition of systemic risk; that much is a consensus of the early literature and research work on the regulation's risk management scheme.[40] I posit, however, that the DSA still gives us several helpful hints to flesh out this concept.

16 To begin with, art. 34(2) DSA lists possible sources of systemic risks and that list includes the design of platforms' recommender systems and 'any other relevant algorithmic system' integrated into or used within platforms' services.[41] In any case, recitals 79 and 84 show that platforms should consider not only the design of their algorithms, but also the latter's functioning and use, and especially so where they lead to the amplification of harmful information. In addition, platforms should be mindful of the 'inauthentic use of their service', namely through the generation and dissemination of synthetic content that is either illegal or may contribute to disinformation campaigns.[42] Such synthetic content nowadays is increasingly produced by genAI[43] and that should also be considered in platforms' risk assessments.

17 Furthermore, art. 34(1) DSA helps determine what negative effects may result from AI systemic risks. There, the EU legislator lists those possible negative effects of AI systemic risks that should always be part of VLOP/SEs' risk assessments. Platforms can, in their risk assessments, uncover other systemic risks but they must, in any case, consider all actual or foreseeable:

- dissemination of illegal content (art. 34(1)(a));
- fundamental rights violations (art. 34(1)(b));
- negative effects on civic discourse, electoral processes, and public security (art. 34(1)(c)); and
- gender-based violence, negative effects on minors' public health, as well as serious negative consequences on any person's physical or mental well-being (art. 34(1)(d)).

18 Despite the above, the DSA still does not answer the questions of (i) what the threshold for a risk to be considered systemic is; and (ii) how a systemic risk could be deemed to exist in concrete cases.[44] Such crucial questions have not, to date, been settled; nor was it the purpose of the DSA to answer them right away, as is implied by its risk-based approach. Indeed, as is common with risk regulation, the DSA does not purport to provide a substantive definition of AI systemic risks, but, differently, institutionalises risk assessment procedures whose output will be the iterative definition of that concept.[45]

19 Such an iterative and process-based definition of systemic risk should be framed by some guiding principles . First, the DSA prescribes that VLOP/SEs take into consideration the severity and probability of the identified risks in their respective risk assessments.[46] This emphasis on the combined effects of the potential negative impacts of a risk (severity) and the likelihood that those negative impacts materialise (probability) is a characteristic of so-called actuarial risk frameworks. These frameworks define risk as the product of quantifiable variables that are measured through a scientific

39 Such risk assessments should be continuous – done at least once a year per art. 34(1) DSA - and iterative, i.e., they should build upon each other and show the evolution of previously identified systemic risks (recital 85 DSA).

40 See, e.g., Anna-Katharina Meßmer and Martin Degeling, 'Auditing Recommender Systems Putting the DSA into Practice with a Risk-Scenario-Based Approach' (Stiftung Neue Verantwortung (SNV) 2023) 14 <https://shorturl.at/viWyd> accessed 17 January 2024; Jason Pielemeier and David Sullivan, 'Unpacking "Systemic Risk" Under the EU's Digital Service Act' (*Tech Policy Press*, 19 July 2023) <https://techpolicy.press/unpacking-systemic-risk-under-the-eus-digital-service-act> accessed 16 May 2024; Oliver Marsh, 'Researching Systemic Risks under the Digital Services Act' [2024] Algorithm Watch 5–7 <https://algorithmwatch.org/en/wp-content/uploads/2024/08/AlgorithmWatch-Researching-Systemic-Risks-under-the-DSA-240726.pdf> accessed 26 August 2024.

41 Art. 34(2)(a) DSA.

42 Recital 84 DSA; European Commission, 2024 (n 9) para. 25.

43 European Commission, 2024 (n 9) para. 25.

44 European Commission, 2023 (n 9) 15.

45 Kaminski (n 19) 1402; Stockmann (n 19); Husovec (n 20) 7; Griffin, 'What Do We Talk about When We Talk about Risk?' (n 15).

46 Recital 79 and art. 34(1) DSA.

or technical frame (usually cost-benefit analyses and/or mathematical assessments multiplying the intensity of the effects of a given harm by its likelihood).[47] Many scholars have pointed out the limited predictive value of actuarial risk frameworks, noting that they fail to fully capture less quantifiable and more socially-dependent risks, instead reducing them to mere technical and mathematical variables.[48]

20 The DSA's risk conception is not, however, purely actuarial. On the contrary, one can find in its articles, recitals, and implementing guidelines several references to the need to contextualise risk assessments by taking into account social and cultural factors that influence the risk perceptions of affected individuals and communities.[49] Although not conclusive, this emphasis on socially and culturally dependent risk assessments is useful to begin gauging the meaning of the 'systemic' in 'systemic risk'. Primarily, it makes clear that the assessment and consequent definition of systemic risk must necessarily extend beyond exclusively quantitative calculations. It should be based on contextual methodologies that locate assessments of risk in their specific social and cultural context.[50] Particularly, platforms must take into account regional and linguistic factors that might affect perceptions and, therefore, assessments of risk,[51] as well as the specific legal, societal and political contexts where systemic risks manifest themselves.[52]

21 In addition, many references to the effects of 'systemic risks' in the DSA suggest that this concept requires a framing that goes beyond identifying isolated instances of harm caused by AI systems. In particular, the DSA's qualification of risk as 'systemic' suggests a reference to the propagation at scale of the negative effects potentially caused by AI systems and digital platforms. That would be only natural since the negative effects of platforms' AI systems are inherently disseminated through the online audiences of large digital platforms.[53] Therefore, the DSA refers to the systemic risks of platforms (including those stemming from their AI systems) by emphasizing collective (as opposed to individual) forms of harm: it mentions, e.g., "societal concerns" and "societal and economic harm", such as risks to the "shaping of public opinion and discourse" through "coordinated disinformation campaigns", as well as of negative effects for "democratic processes", the (non-individualised) "exercise of fundamental rights", and online safety and trade.[54]

22 In the DSA Russian disinformation study, the Commission made the only official attempt to date to densify the concept of systemic risk. It did so through one of the variables of any actuarial risk framework: severity; but gave a distinct sociocultural flavour to that concept. In the Commission's words, for a risk to be systemic its actual or foreseeable negative effects must be 'severe enough'. And a systemic level of severity should be measured as a function of both qualitative and quantitative indicators. Specifically:

> "[s]everity is a function of the relationship between the qualitative assessment of the risk posed by the content in context and a quantitative measure of the reach and/or intensity of exposure of audiences to that content. It follows then that a risk may reach a systemic level in different ways. The higher the level of risk inherent in the content *in context*, the smaller the audience required to reach a systemic level. And by contrast, the lower the level of risk inherent in the content *in context*, the larger the audience required to reach a systemic level."[55]

23 This approach of the Commission to defining 'systemic risk' is not, by the Commission's own admission, set in stone.[56] In any case, it reinforces this paper's argument – to be developed in Section C. - that the DSA normatively aspires to a definition of AI systemic risk that is (i) socially contextualised; and (ii) refers to forms of harm that are propagated at scale and have, therefore, a distinctive collective nature.

2. Risk mitigation

24 After identifying and assessing the systemic risks stemming from their AI systems, platforms must proceed to the second step of the DSA's risk management framework: risk mitigation (art. 35 DSA). As the term 'mitigation' suggests, the endpoint of this stage of risk management is not to necessarily eliminate identified risks, but instead to reduce

47 Haines (n 20) 183-184; Kaminski (n 19) 1392-1393.

48 Jeroen van der Heijden, 'Risk Governance and Risk-Based Regulation: A Review of the International Academic Literature' [2019] State of the Art in Regulatory Governance Research Paper Series 25–26 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3406998> accessed 13 January 2024; Kaminski (n 19) 1354.

49 Recital 79, 90, and art. 34 (2) DSA; European Commission, 2023 (n 9) 10, 13, 15; European Commission, 2024 (n 9) paras. 11-13.

50 European Commission, 2023 (n 9) 15, 63.

51 Art. 34(2) DSA.

52 E.g., European Commission, 2024 (n 9), para. 31, where the Commission stresses the need for platforms to develop election-specific risk profiles in their assessments of systemic risks to electoral processes.

53 Recital 80 DSA; European Commission, 2023 (n 9) 15, 17.

54 Recitals 69, 79-83, art. 34(1) DSA.

55 European Commission, 2023 (n 9) 15.

56 ibid, 13.

their expected impact to acceptable levels.[57] But acceptable to whom? In other words, who is the ultimate decision-maker of what an acceptable AI systemic risk is and, consequently, of which measures are adopted to mitigate that risk? The answer is clear: VLOP/SEs. Similarly to risk assessment, it is for platforms to decide and put in place "reasonable, proportionate and effective mitigation measures" tailored to reduce the impact of previously assessed systemic risks (art. 35(1) DSA).[58] Articles 35 and 45 DSA contain a list of several possible risk mitigation measures which VLOP/SEs may choose from. Some of these measures are specifically relevant to the mitigation of AI risks, namely:

- Adapting the overall design and functioning of platforms' services and their online interfaces, which may in whole or in part be AI-driven (arts. 25 and 35(1)(a) DSA);
- Testing and adapting platforms' AI systems (art. 35(1)(d) DSA), with an emphasis on interventions related to the design of AI systems and finetuning of their parameters;[59]
- Ensuring that fake and deceptive AI-generated content (so-called deepfakes) is distinguishable as such (art. 35(1), k) DSA);[60]
- Adhering to codes of conduct - whose drawing up is promoted by the Commission - containing specific risk mitigation measures (art. 45(2) DSA).[61]

25 Similar to risk assessments, the Commission has also highlighted the need to contextualise risk mitigation measures. Specifically, it acknowledges that harmful high-risk content is not evenly distributed on platforms and might vary in time and/or between some audience segments.[62] Consequently, some individuals and communities might experience more severe levels of risk in certain moments in time. Therefore, the Commission recommends that risk mitigation measures be tailored to specific audiences[63] and time-specific contexts, such as elections/electoral campaigns.[64]

3. Risk management controls in the DSA's ecosystem

26 If, as shown above, VLOP/SEs are the ultimate decision-makers when it comes to systemic risk assessment and mitigation, how does the DSA ensure their accountability for those risk management choices? The response is threefold: platform compliance is monitored through (i) the internal compliance divisions of platforms themselves; (ii) independent audits contracted by platforms; and (iii) Commission or civil society adversarial audits based on DSA-mandated access to information.

a.) Internal compliance function

27 VLOP/SEs should, first and foremost, monitor compliance with the DSA from the inside. According to art. 41 DSA, they should establish an internal compliance division that is independent from their operational functions. This internal compliance division shall be headed by an "independent senior manager" who reports directly to the management body of VLOP/SEs (art. 41(2) DSA). Amongst the many tasks entrusted to it in art. 41(3) DSA, it is relevant in this case to highlight that the internal compliance function shall ensure that systemic risks are properly assessed in line with art. 34 DSA, subsequently reported, and appropriately mitigated in accordance with art. 35 DSA.[65]

b.) Independent audits contracted by platforms

28 In addition to having a compliance division tasked with internally monitoring compliance with the DSA, platforms shall "be subject, at their own expense and at least once a year, to independent audits" that assess their compliance with, amongst others, their

57 Florian M Neisser, 'Riskscapes and Risk Management - Review and Synthesis of an Actor-Network Theory Approach' (2014) 16 Risk Management 88, 90; Kaminski (n 19) 1395, 1397.

58 European Commission, 2024 (n 9) para. 8-10; De Gregorio and Dunn (n 15) 487-488. See also, in art. 35(1) DSA, "[s]uch measures *may* include (...)".

59 Recital 88, DSA; European Commission, 2023 (n 9) 22-23.

60 European Commission, 2024 (n 9), paras. 26, 28, 38.

61 Recital 104 and art. 45 DSA. Interestingly, one voluntary code of conduct pre-dating the DSA, the Disinformation Code of Practice, should be made an official DSA code of conduct. This code of conduct could be particularly relevant in the context of mitigating risks of AI-generated content that is used in coordinated disinformation campaigns. See, to this effect, Recitals 84 and 106, DSA; European Commission, 2022 (n 28), commitments 14-16, p. 15-18; European Commission, 2023 (n 9) 12, 23; European Commission, 2024 (n 9), para. 58.

62 For a similar, related, argument relating to uneven 'online visibility' of certain communities of users, see Rachel Griffin, 'The Law and Political Economy of Online Visibility: Market Justice in the Digital Services Act' (2023) 2023 Technology and Regulation 69, 71–73.

63 European Commission, 2023 (n 9) 21-22.

64 European Commission, 2024 (n 9) paras. 11-12, 37.

65 Art. 41(3)(b) DSA.

risk assessment and mitigation obligations (art. 37(1)(a) DSA).[66] Within the DSA Framework, independent audits are considered an important tool for assessing platform compliance and, consequently, "meaningfully inform regulatory supervision".[67]

29 Independent audits may either be holistic, i.e., looking at how audited platforms assessed and managed all possible systemic risks listed in art. 34 DSA; or granular, i.e., focusing only on certain specific types or sources of systemic risks.[68] An audit might be more granular if it focuses only on how platforms have managed systemic AI risks stemming from the design and functioning of platforms' algorithms (recital 3 and art. 10(5)(b) and (c) DRA); or, even more specifically, those risks posed by a specific type of AI model or system (e.g., recital 25 DRA talks about auditing large language models).[69] They may also focus on certain types of systemic risks, e.g. those posed to fundamental rights.[70] Conversely, an audit may also have a more holistic focus if it examines how AI systems interact with a platform's overall design and thus contribute, in general, to the emergence of the different systemic risks covered by the DSA.

30 An example of a more holistic approach is the DSA Russian Disinformation study that was carried out by the Commission.[71] Despite not constituting a fully-fledged DSA audit (it was carried out in anticipation of the DSA's entry into force and so still with limited access to information),[72] this study is a good example of an analysis of platforms' systemic risks that holistically examines all sources of those risks in a specific context (i.e. Russian disinformation campaigns), including those risks stemming from AI systems.[73]

31 The output of each audit will be a report containing main findings, an overall opinion of the auditor on the platforms' compliance with the DSA,[74] and, if need be, operational recommendations for platforms to fully achieve compliance with the DSA.[75] These operational recommendations do not have to be necessarily followed by the audited platform, who has the discretion to determine the risk management measures they will implement (art. 37(6) DSA).[76]

c.) Commission and civil society adversarial audits

32 It is not particularly groundbreaking to state that, despite the effort of the DSA and DRA to secure the independence of the auditors contracted by platforms,[77] the risk of regulatory capture and/or ineffectiveness of audits still remains.[78] Indeed, there is huge potential for conflicts of interest and the development of pro-platform biases to surface in a scheme where auditors are contracted by platforms and will be, for a set period of time, contacting and collaborating directly with the personnel of VLOP/SEs .[79] Hence, it is worth exploring whether similar auditing exercises can, in the framework of the DSA, be carried out in a setting that is institutionally

66 These audits must be carried out by independent auditing organisations with proven expertise in the area of risk management, as well as objectivity and professional ethics (art. 37(3) DSA). These organisations are contracted by platforms (art. 2(1) DRA) and will most likely be private consulting companies. See Giovanni De Gregorio and Oreste Pollicino, 'Auditing Platforms under the Digital Services Act' [2024] Verfassungsblog <https://verfassungsblog.de/dsa-auditors-content-moderation-platform-regulation/> accessed 25 September 2024; Alexander Hohfeld, 'DSA: Risk Assessment & Audit Database - First Round' (*Google Docs*, November 2024) <https://shorturl.at/STVQe> accessed 5 December 2024; Petros Terzis, Michael Veale and Noëlle Gaumann, 'Law and the Emerging Political Economy of Algorithmic Audits', *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency* (Association for Computing Machinery 2024) 1262–1263 <https://dl.acm.org/doi/10.1145/3630106.3658970> accessed 27 January 2025.

67 Recital 1 DRA.

68 The dichotomy between holistic or granular audits is not one of mutual exclusion, but rather of gradation. In simpler words, audits might be more or less granular.

69 See recital 29 and arts. 2(17) and (18), 13(2) and 14(2) DRA for the types of audit exercises that auditors should carry out, namely so-called 'tests' and 'substantive analytical procedures'.

70 European Commission, 2023 (n 9) 1, 12-13, 34, 48, 59-63.

71 This audit was not carried out by an auditing organisation but the Commission stated its ambition to set, with this study, a baseline analytical framework to be used and iteratively improved by researchers and auditors; see European Commission, 2023 (n 9) 13.

72 ibid 1, 12.

73 ibid 34, 48, 59-63.

74 This opinion might be 'positive', 'positive with comments' recommending specific but not major improvements, or 'negative'.

75 Art. 37(4) DSA and art. 8 DRA.

76 They may follow the operational recommendations; or, conversely, justify the reasons not to do so and set out other alternative measures. These choices must be featured in an implementation report produced by platforms within one month of receiving the audit report.

77 Art. 37(3)(a) DSA; recital 2 and art. 4 DRA.

78 De Gregorio and Pollicino (n 66).

79 Meßmer and Degeling (n 40) 36; Martin Senftleben, 'Human Rights Outsourcing and Reliance on User Activism in the DSA' (*Verfassungsblog*, 21 February 2024) <https://verfassungsblog.de/human-rights-outsourcing-and-reliance-on-user-activism-in-the-dsa/> accessed 21 February 2024.

independent from platforms.

33 In this sense, one can find several hints in the DSA and related implementing law towards the possibility of other audits beyond those contracted out by platforms. I qualify those as 'adversarial audits', meaning more or less issue-specific risk audits or audit-like review exercises carried out by public authorities or civil society actors on the basis of publicly available or legally accessed information. Adversarial audits aim to scrutinise platforms' systemic risk management policies, actions and choices. In the DSA framework, I argue, adversarial audits can be conducted by (i) the Commission alone; (ii) the Commission in collaboration with civil society researchers ('collaborative adversarial audits'); or (iii) by civil society organisations and/or researchers themselves.

34 Firstly, conducting a risk adversarial audit could conceivably be one of "the necessary actions to monitor the effective implementation and compliance" with the DSA that the Commission may take in art. 72 DSA.[80] Interestingly, the Commission is able to appoint external experts and auditors to support the exercise of the aforementioned supervisory tasks (Art. 72(2) DSA, and recital 3 and art. 3(5)-(7) Implementing Regulation 2023/1021).[81] One can, therefore, deduce from these provisions the possibility of both Commission adversarial audits and collaborative adversarial audits.

35 Similarly, civil society organisations and independent researchers may, by themselves, conduct adversarial audits using information on platforms' risk management choices accessed through the mechanisms established in arts. 40 and 42 DSA.[82] By virtue of art. 40(4) and (8) DSA, certain researchers may be approved by national DSA supervisory authorities (so-called Digital Service Coordinators or 'DSCs') as 'vetted researchers'. These vetted researchers must, upon a request approved by a Digital Service Coordinator (art. 40(8) and (9) DSA), have access to data stored by VLOP/SEs that are needed for research that contributes to the detection, identification and understanding of systemic risks in the Union. This research may prove crucial to assess platforms' compliance with the risk assessment and mitigation obligations of arts. 34 and 35 DSA (recitals 96-98 and art. 40(4) DSA). It may point, for example, to certain emerging systemic risks overlooked by platforms, or to the insufficiency of their risk mitigation actions. Crucially, the output of vetted researchers' work must, per art. 40(8)(g) DSA, be made publicly available free of charge.[83]

36 To obtain vetted researcher status and have access to VLOP/SEs data, applicants must, in essence, (i) be affiliated with a research organisation within the meaning of art. 2(1) of Directive 2019/790 and (ii) have a project whereby they conduct research on platform-related systemic risks in the Union. The interpretation of these requirements and, therefore, the access of civil society actors to vetted research status depends on the case-by-case decisions of DSCs. These decisions will, in practice, determine to a significant extent who gets a meaningful possibility to carry out adversarial audits in the context of the DSA, meaning who gets sufficient access to data for in-depth systemic risk research.[84]

80 Although information about the Commission's monitoring actions related to the DSA's systemic risk management scheme is not widely available to the public, one can see some references to Commission audits of platforms' compliance with such risk management scheme in, for example, 'Commission Opens Formal Proceedings against Facebook and Instagram under the Digital Services Act' (*European Commission*, 30 April 2024) <https://ec.europa.eu/commission/presscorner/detail/en/IP_24_2373> accessed 7 May 2024; 'Commission Opens Proceedings against TikTok under the DSA' (*European Commission*, 22 April 2024) <https://ec.europa.eu/commission/presscorner/detail/en/IP_24_2227> accessed 7 May 2024; 'Commission Sends Requests for Information to YouTube, Snapchat, and TikTok on Recommender Systems under the Digital Services Act' (*European Commission*, 2 October 2024) <https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-youtube-snapchat-and-tiktok-recommender-systems-under-digital> accessed 29 October 2024.

81 See another form of collaboration between the Commission and individual experts in reviewing platform compliance under the DSA in 'Commission Sends Preliminary Findings to X for Breach of DSA' (*European Commission*, 12 July 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3761> accessed 12 July 2024: "Based on an in-depth investigation that included, among others, the analysis of internal company documents, interviews with *experts* [N.B. emphasis added by author], as well as cooperation with national Digital Services Coordinators (...)". Similarly, but mentioning "third parties" and not "experts", see 'Commission Opens Formal Proceedings against Temu under DSA' (*European Commission*, 31 October 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5622>.

82 A similar argument pointing out this possibility is made in De Gregorio and Pollicino (n 66): (...) civil society organisations, which, considering the lack of reference in the delegated acts [N.B. on platform-contracted audits], are now looking more into the possibility of participating in this process and more generally to policy involvement in the DSA, also accessing data from online platforms".

83 This research output might, interestingly, feed into the independent audits contracted by platforms, as it is one of the information sources that those auditing organisations must take into account per arts. 13(4) and 14(4) DRA.

84 In Marsh's words, DSCs' decisions may also become a sort of "quasi case law" regarding both what are 'systemic risks'

37 Another hint towards the possibility of civil society adversarial audits is contained in recital 1 DRA, which alludes to the "enhanced scrutiny" of transparency reports of platforms. Indeed, per art. 42 DSA, platforms must make certain reports publicly available, including the results of their risk assessment and mitigation processes, as well as their audit reports and implementation reports (art. 42(4) DSA).

38 All in all, one can wonder whether the data accessed by vetted researchers, coupled with the data contained in transparency reports and other DSA access to information mechanisms,[85] may provide an overall level of insight into platforms' risk management processes that would allow the Commission and civil society to meaningfully scrutinise platforms' AI risk management. Similar regulatory scrutiny in tech regulation is often hampered by informational asymmetries between regulated actors and the public that favour the former and which they seek to preserve by citing trade secrecy and other commercial interests.[86] The enhanced access to information that arts. 40 and 42 DSA provide to public authorities and civil society actors is, therefore, key to concretising the unique public oversight promise of this regulation, as it may decisively tilt the regulatory balance towards information disclosure and consequently allow for evidence-based scrutiny of platforms' AI risk management.

39 Early reports on researcher access to information suggest that the corresponding DSA mechanisms might take a long time to be implemented properly.[87] But even those reports underline the potential of such access to information provisions: without them, researchers and civil society organisations will have a hard time auditing platforms' risk management based on high-quality and up-to-date information.[88]

II. Filling in the gaps: the AI Act

40 The AIA complements the DSA's systemic risk management framework. It does so in two distinct ways: through the institutionalisation of a residual risk management regime and by setting obligations that are relevant to how VLOP/SEs manage systemic risks related to the dissemination of inauthentic AI-generated content.

1. A residual risk management regime

41 Even if compliance with the DSA's systemic risk management framework creates a presumption that the corresponding AIA obligations have been fulfilled, the AIA is still relevant to manage newly identified "significant systemic risks" of platforms' AI systems and models that are not covered in the DSA (Recital 118, AIA). It is, therefore, useful to understand what AI systemic risks are not covered by the DSA and can, *a contrario*, be managed through the AIA. These will be, in essence, those systemic risks posed by AI systems and models that are not a possible source of systemic risks per the DSA.

42 In this respect, it should be clarified that the DSA *prima facie* applies to the algorithmic systems of platforms and any related systems (art. 34(1) DSA), meaning both the AI systems that are embedded in a platform's service and are thus behind its operation; and AI systems which *are* the service's digital infrastructure, which is typically the case of AI-powered search engines such as ChatGPT or Google

under art. 34 DSA and what is a 'vetted researcher' for these purposes; see Marsh (n 40) 6–7. For more information on DSA data access requests, see arts. 3, 7 – 13 of the Access to Data Delegated Regulation.

85 Referring to the need to combine several data access points and transparency mechanisms to research platforms' compliance with the DSA, see Rishabh Kaushal and others, 'Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database' (arXiv, 2024) 14 <http://arxiv.org/abs/2404.02894> accessed 6 April 2024.

86 Cary Coglianese, 'Regulating New Tech: Problems, Pathways, and People' 5 <https://scholarship.law.upenn.edu/faculty_scholarship/2753>; Madalina Busuioc, Deirdre Curtin and Marco Almada, 'Reclaiming Transparency: Contesting the Logics of Secrecy within the AI Act' (2023) 2 European Law Open 79, 82, 88; Marta Maroni, '"Mediated Transparency": The Digital Services Act and the Legitimisation of Platform Power' in Päivi Leino-Sandberg, Maarten Zbigniew Hillebrandt and Ida Koivisto (eds), *(In)visible European Government: Critical Approaches to Transparency as an Ideal and a Practice* (Routledge, 2023).

87 Marsh (n 40) 13–14; Julian Jaursch, Jakob Ohme and Ulrike Klinger, 'Enabling Research with Publicly Accessible Platform Data: Early DSA Compliance Issues and Suggestions for Improvement' (Weizenbaum Institute 2024) <https://www.weizenbaum-library.de/handle/id/572> accessed 28 November 2024; Mateus Correia de Carvalho, 'Researcher Access to Platform Data and the DSA: One Step Forward, Three Steps Back' (*Tech Policy Press*, 31 May 2024) <https://techpolicy.press/researcher-access-to-platform-data-and-the-dsa-one-step-forward-three-steps-back> accessed 27 September 2024; Philipp Darius, 'Researcher Data Access Under the DSA: Lessons from TikTok's API Issues During the 2024 European Elections' (*Tech Policy Press*, 24 September 2024) <https://techpolicy.press/-researcher-data-access-under-the-dsa-lessons-from-tiktoks-api-issues-during-the-2024-european-elections> accessed 26 September 2024.

88 ibid.

Bard.[89] Consequently, the AIA risk management framework applies to any AI systems and models producing systemic risks, but that are not considered as embedded or integrated in a platform's service per the DSA. This is, for example, the case of AI systems and models whose content is diffused or amplified by platforms' recommender systems. Through the AIA, the companies that develop those AI systems (AI providers) and those that are placing them on the market (AI deployers) might be called upon to manage their systemic risks.

43 Having clarified the scope of application of the AIA's systemic risk management scheme, a new question arises: how does the AIA define and purport to manage systemic risks? According to art. 3(65) AIA, an AI systemic risk may solely stem from a specific type of AI model, i.e., a general-purpose AI model (hereinafter 'GPAI'), which is an AI model that can competently perform a wide range of distinct tasks, being typically trained with a large amount of data (art. 3(63) AIA). More specifically, a GPAI can only be a source of systemic risk if it displays either (i) 'high-impact capabilities' - meaning those capabilities that, according to some computational metrics, match or exceed those recorded in the most advanced GPAIs[90]; or, alternatively, capabilities or an impact deemed by the Commission to be equivalent to 'high-impact capabilities'.[91]

44 For a GPAI to present a systemic risk, its high-impact capabilities must negatively affect at least one of a number of protected issues (i.e., public health, safety, public security, fundamental rights or other goods that benefit societies as a whole), with a reach and propagation at a scale that is significant enough to warrant the qualification of 'systemic'.[92] It is the Commission who will ultimately decide, either ex officio or following a qualified alert issued by a scientific panel of independent experts (arts. 52(4), 68, and 90 AIA), whether a given GPAI presents a systemic risk (art. 52 AIA).[93]

45 If a GPAI is deemed to present new systemic risks, then their providers must comply with a set of product safety and risk management obligations listed in art. 55(1) AIA. Of most relevance here are the obligations for GPAI providers to perform model evaluations and testing in order to identify, assess and mitigate emerging systemic risks (art. 55(1)(a), (b) AIA). The AIA offers two main ways to simplify compliance with these obligations: (i) the compliance by the GPAI provider with a European harmonised technical standard (arts. 40 and 55(2) AIA);[94] or (ii) the adherence to codes of practice drawn up at EU level and containing several measures aimed at assessing and managing systemic risks of GPAI models (arts. 55(2) and 56 AIA).[95]

89 Vermeulen and Lemoine (n 13).

90 Arts. 3(64) and (67); art. 51(1)(a) AIA. The computational metric privileged in the context of this assessment is the number of floating operation points (FLOP) of an AI system, see art. 51(2) AIA.

91 Art. 51(1)(b) and Annex XIII AIA. See, Charlie Bullock and others, 'Legal Considerations for Defining "Frontier Model"' (Institute for Law & AI, LawAI Working Paper Series, No 2-2024 2024) 13 <https://law-ai.org/wp-content/uploads/2024/09/Legal-Considerations-for-Defining-Frontier-Model.pdf> accessed 29 January 2025, pointing out that the AIA's systemic risk regime may become underinclusive of certain GPAIs if it overemphasizes computational metrics in this classification. Also criticising this regime for its uncertainty and potential underinclusive nature, Cornelia Kutterer, 'Regulating Foundation Models in the AI Act: From "High" to "Systemic" Risk' (AI-Regulation Papers 2024) 6–7 <https://ai-regulation.com/wp-content/uploads/2024/01/C-Kutterer-Regulating-Foundation-Models-in-the-AI.pdf> accessed 29 January 2025.

92 Per art. 3(65) AIA, a "'systemic risk' means a 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, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain".

93 Annex XIII to the AIA contains a (non-exhaustive) set of criteria that the Commission shall take into account when designating that a GPAI presents systemic risk, such as indicators related to the design and ability of the AI model (e.g., number of parameters, size of dataset, autonomy to perform new tasks), the number of registered end-users of the GPAI, as well as the reach of the GPAI in the internal market, which shall be presumed when the model has at least 10.000 registered business users in the Union.

94 European harmonised standards are technical standards developed by private standardisation organisations at the request of the Commission and containing technical specifications on how to comply with the requirements set in EU secondary law. Voluntary compliance with these standards will grant an AI provider a presumption of conformity with the obligations set out in art. 55(1) AIA. See Regulation 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation art. 2(1); Annalisa Volpato, 'The Legal Effects of Harmonised Standards in EU Law: From Hard to Soft Law, and Back?', *The Legal Effects of EU Soft Law* (Edward Elgar Publishing 2023).

95 Codes of practice are drawn up in a collaborative process coordinated by two new governance bodies created by the AIA to support the Commission in its enforcement actions, i.e., the AI Office and the AI Board, and involving GPAI providers, national competent authorities, civil society organisations, researchers, and other stakeholders (art. 56(3) AIA). The first code of practice on GPAI systemic risk management is already started being drafted, see Nuria Oliver and others, 'First Draft of the General-Purpose AI Code of Practice' (European Commission 2024) <https://shorturl.at/irQTc> accessed 19 November 2024.

46 Although according to the AIA, the DSA systemic risk management framework of platforms' AI systems is to be primarily complemented by the AIA provisions on systemic risk management of GPAIs described up until this point, some other AIA requirements are relevant for platforms as deployers of AI models and systems. Indeed, the AIA systemic risk regime focuses on risks stemming from AI models and systems *as a whole* (i.e., a given GPAI presents, in itself, a systemic risk that should be managed accordingly). In addition, however, the AIA creates two distinct legal regimes for certain *practices* or *uses* of all AI systems (including GPAIs[96]): those that (i) present unacceptable risks considering the EU's values (art. 5 AIA); or that (ii) are used for high-risk purposes (art. 6 AIA). How are these two additional risk regimes relevant for the risk management of platforms' AI systems?

47 Looking first at the prohibited AI practices of art. 5 AIA, these are said to be "particularly harmful and abusive" and should, according to the EU legislator, be prohibited in the EU, since they "contradict Union values of respect for human dignity, freedom, equality, democracy and the rule of law and Union fundamental rights" (recital 28 and art. 5 AIA). It would, therefore, be contradictory to prohibit certain AI practices in the AIA because of a fundamental misalignment with the EU's core values and, at the same time, not extend that prohibition to AI practices of VLOP/SEs in the DSA. Some of these prohibited practices should be considered by platforms when designing and integrating AI systems into their services. Namely, they should consider the prohibition of deployment of manipulative or deceptive subliminal techniques operating beyond a person's consciousness, with the objective or effect of materially distorting a person's or a group of persons' behaviour by appreciably impairing their ability to make an informed decision (art. 5(1)(a) AIA). This links well with certain provisions of the DSA that prohibit the design of platforms' services in a way that materially distorts or impairs individuals' ability to make free and informed decisions (recitals 37, 79, 81, 83 and arts. 25, 34(2) DSA).

48 At the same time, any AI systems and models integrated or diffused in platforms (and not covered by the DSA) might also be classified as high-risk AI systems if they are used for any of the purposes mentioned in art. 6 and Annex III to the AIA. Even if these AIA provisions do not mention the AI systems of online platforms explicitly, the Commission may, theoretically, add them to that list by adopting a delegated act that modifies Annex III (art. 7 AIA). In any event, there might already be leeway in Annex III to classify as high-risk certain AI systems integrated or used in platforms, namely those that are "intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda" (Annex III, point 8(b)).

49 Should an AI system (including a GPAI, per art. 25(1)(c) AIA) be used for high-risk purposes in accordance with art. 6 AIA, then its providers and deployers will be subject to a host of legal requirements destined to ensure the safety of the AI system in question and a related adequate level of fundamental rights protection.[97] Amongst those requirements, some are particularly relevant in the context of risk management. According to Art. 9 AIA, AI providers and deployers should establish a risk management scheme that first, regularly and systematically identifies the (high-level) risks of AI systems and, subsequently, mitigates or eliminates them. This risk management scheme focuses particularly on risks posed by high-risk AI systems to health, safety and fundamental rights (art. 9(2)(a) AIA). It is worth nothing that art. 9 AIA does not require AI providers and deployers to mitigate or eliminate all identified high-risks, but only to do so up to a *reasonable* extent (art. 9(3) AIA) and through specific courses of action: either the better design and development of the high-risk AI systems *or* the provision of adequate technical information. In addition, articles 10 to 15 AIA contain a number of AI safety requirements that can conceivably be implemented as risk mitigation measures, e.g., ensuring the quality of the data sets used for training, validation and testing of AI systems (art. 10 AIA), human oversight requirements (art. 14 AIA), or ensuring an appropriate level of cybersecurity of AI systems (art. 15 AIA).

50 Crucially, however, it is for AI providers and deployers themselves to judge whether high-risk mitigation is sufficient. Although art. 9 AIA prefers to formulate most risk management requirements in the passive voice,[98] it is clear from the logic of the article and related provisions (e.g., recital 46, and arts. 6(4) and 8(1) AIA) that it is for AI providers and

96 GPAIs are in fact subject to both the systemic risk management framework of articles 51-55 AIA, as well as to the prohibitions and requirements flowing from certain unacceptable or high-risk uses of such models. This is made clear in art. 25(1)(c) AIA, points out the possibility for a GPAI – which can, as seen above, be classified as presenting systemic risk - to be classified as presenting high-risk pursuant to art. 6 AIA.

97 Similarly to compliance with the obligations imposed on providers of GPAIs with systemic risk, compliance with the requirements imposed on providers and deployers of high-risk AI systems will be presumed through adherence to harmonised standards (art. 40 AIA).

98 E.g., 'A risk management system shall *be established* (...)'; 'The risks (...) *may be* resonsably *mitigated or eliminated*'; or 'The risk management measures shall be such that the relevant residual risk (...) is *judged* to be acceptable'.

deployers to implement a risk management system and ultimately decide, with considerable flexibility, whether identified risks have been reduced to an acceptable level.[99]

2. The AIA's other DSA-relevant provisions: of deepfakes and sandboxes

51 Aside from the AIA risk regimes that were discussed, other provisions are relevant for VLOP/SEs as they seek to manage the systemic risks of their AI systems pursuant to the DSA.

52 Namely, the Commission's DSA risk mitigation guidelines state that VLOP/SEs should pay particular attention to the "creation (...) and large-scale dissemination of generative AI content" and that the AIA contains particularly relevant obligations of watermarking and labelling of 'deep fakes' and synthetic AI content.[100] This is a clear reference to art. 50 AIA, which requires that, on the one hand, providers of genAI ensure that the outputs of those models are marked as artificially generated and manipulated; and that, on the other hand, deployers of genAI use state-of-the-art technical solutions to disclose that synthetic AI content was artificially generated (recital 120 and art. 50(2) AIA). These requirements are, as stated in recital 120 AIA, particularly relevant for the effective implementation of the DSA when it comes to mitigating systemic risks to democratic processes and civic discourse.

53 One final note should be made to reference AI regulatory sandboxes, which the AIA institutes (arts. 3(55) and 57 AIA) as a controlled framework set up by a supervisory authority where current or prospective AI providers can develop their AI systems with a view to identifying potential risks to fundamental rights, health and safety of future users. Regulatory sandboxes are often referred to as a valuable feature of any risk regulation toolbox, due to their experimental nature and related potential to gauge and anticipate emerging risks of AI systems.[101] VLOP/SEs could conceivably use this AIA-institutionalised framework when developing or adapting their AI systems.

C. What they have in common: sociotechnical and contested systemic risk

54 In the previous section, I have described the AI risk management regimes of the DSA and the AIA applicable to platforms' AI systems. That, however, is not enough to answer the main question guiding this paper: how do the DSA and AIA foresee creating an effective risk regulatory regime applicable to the AI systems of digital platforms? In other words, how do these regulations intend to address the typical challenges of any risk-based approach?

55 As laid out in the introduction, two main typical challenges are posed to effective risk regulation, especially in the field of AI. Firstly, its excessively quantitative and actuarial focus might make platforms and public authorities overlook less quantifiable AI risks whose impact is not reduced nor explained through single instances of harm caused to individuals. A second challenge is that AI risk regulation gives significant discretion to private regulated actors regarding how they identify, measure and mitigate emerging AI risks. If not adequately controlled, platforms and other AI providers or deployers might exercise this discretion in self-serving ways, by overlooking certain emerging AI risks, underestimating their impact, and/or putting insufficient measures in place to adequately mitigate those risks.

56 In this section, I argue that both the DSA and AIA contain similar guiding ideas for how to address the abovementioned challenges. Besides the foreseen complementarity between the two regulations' AI risk management schemes, they have in common three main normative commitments and aspirations as to how AI risks should be managed. In particular, AI risks should be framed as systemic (I.); their identification, assessment and mitigation should be done through methodologies that socially contextualise the impact of those risks (II.) and civil society should be actively involved in the corresponding risk management processes (III.). These three main commonalities between the DSA and AIA's risk management regimes give further credence to the argument, advanced at the beginning of Section B., that one integrated EU AI

99 See, to this effect, in recital 46: '(...) providers of a product that contains one or more high-risk AI systems (...) should have flexibility with regard to operational decisions on how to ensure compliance of a product that contains one or more AI systems with all applicable requirements of the Union harmonisation legislation in an optimal manner'; and in art. 9(5) AIA: 'The risk management measures (...) shall be such that the relevant residual risk (...) as well as the overall residual risk of the high-risk AI systems is judged to be acceptable'.

100 European Commission, 2024 (n 9) paras. 25-30.

101 Sofia Ranchordas and Valeria Vinci, 'Regulatory Sandboxes and Innovation-Friendly Regulation : Between Collaboration and Capture' (2024) <https://papers.ssrn.com/abstract=4696442> accessed 5 March 2024; Kaminski (n 19) 1371.

risk management framework applicable to digital platforms with similar normative foundations can be distilled from the two regulations.

57 In the remainder of this section, I will detail these three main normative commonalities. Before proceeding, it is important to underline that this section's argument should not be interpreted to mean that *only* three commonalities exist between the DSA and AIA. Instead, they are argued to be the normative commitments that most acutely and specifically impact how AI risk management processes should be carried out in EU law. For example, one could also note that both the DSA and AIA place a special emphasis on fundamental rights protection as one of their main aims.[102] This point logically extends to the two regulations' systemic risk provisions.[103] Such an emphasis on fundamental rights requires that this risk management framework be interpreted in light of the EU Charter and the ECHR, as an integrated attempt to protect fundamental rights through risk in the AI context.[104]

I. The emphasis on systemic risk: a sociotechnical frame

58 One first commonality that can be distilled from the description of the DSA and AIA's respective AI risk management regimes is that they frame the risks of digital platforms as 'systemic'. Furthermore, as laid out above, the two regulations foresee the complementary of their systemic risk management regimes.[105] Therefore, there should be some communication between the concept of systemic risk adopted in the AIA and DSA. This is an important insight since the DSA does not define the concept of systemic risk. As pointed out in Section B.I., there is no clear indication in the DSA of when an AI risk should be considered to be systemic. To answer this question, one can look at the corresponding AIA definition (contained in art. 3(65) and Annex XIII AIA). The AIA considers that an AI risk is considered systemic if it has "a significant impact on the internal market due to its reach, (...) with actual or reasonably foreseeable negative effects (...) that can be propagated at scale".

59 This conceptualisation of systemic risk as implying a considerable reach and propagation at scale of the effects of AI systems aligns well with the fact that both the DSA and AIA conceptualise the negative effects of AI systemic risks by reference to forms of collective - rather than individual - harm. In fact, both the DSA[106] and the AIA[107] refer to the societal negative effects of platforms' AI systems on democratic processes such as elections and civic discourse; public health, safety and security; or widespread gender-based violence and negative effects on fundamental rights and mental health. The AIA even mentions "negative effects (...) on society as a whole" (art. 3(65) AIA). This also means that AI risks are not just seen in these regulations as actuarial, quantitative and reduced to individual instances of harm. Therefore, and although the literature rightly points out the possibility that these regulations may be implemented with an exclusive (or, at least, predominant) focus on individual[108] and quantifiable[109] interests, there is potential for the DSA and AIA to also take into account collective, societal or cumulative[110] forms of AI harm that are not explainable nor reducible to singular instances of individualised harm.[111]

60 Despite all the foregoing indications regarding the meaning of 'AI systemic risk', many conceptual questions remain:

- Is an AI risk systemic only if it affects societal systems, structures and collective goods, such as democratic processes,[112] the free access to

102 De Gregorio and Dunn (n 15) 493-498; Almada and Petit (n 22) 17-18. See also the Commission's explanatory memorandum in the AIA proposal in European Commission, 2021 (n 35) 1-4; recitals 3, 9, 36, 40, 41, 47, 51, 52, 63, 79, 81, 86, 87, 107, 109, 111, 153, 155, and arts. 1, 14(4), 34(1)(b), 35(1) DSA; and recitals 1, 2, 3, 5, 6, 7, 8, 10, 28, 32, 43, 46, 48, 52, 65-66, 93, 96, 118, 139-140, and arts. 1, 3(65); 6(3), (6)-(8); 7(1)(b), 2(e) and (i), 3; 9(2)(a); 10(2)(f), (5); 13(3)(b)(iii); 14(2); 40(3); 41(1)(a)(iii); 57(6); 58(2)(i), (4); 77; 82(1) AIA.

103 Recitals 79, 81, 86, and arts. 34(1)(b), 35(1), (3) DSA; recital 118 and art. 3(65) AIA.

104 This fundamental rights-friendly interpretation is mentioned specifically in recitals 153 DSA and 2, 7 AIA. See also European Commission, 2021 (n 35) 4.

105 See Section B.; and recital 118 AIA; European Commission, 2024 (n 9) paras. 26-30.

106 See Section B.I.1. and, in particular, *supra* footnote 54.

107 Art. 3(65) AIA.

108 Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 22 Computer Law Review International 97, 99; Rachel Griffin, 'Rethinking Rights in Social Media Governance: Human Rights, Ideology and Inequality' (2023) 2 European Law Open 30, 42–46.

109 Kaminski (n 19) 1391–1393.

110 By cumulative, I mean forms of harm that are caused in successive instances over time 'without a single event tripping a threshold of seriousness, leaving it difficult to prove', as defined in Veale and Borgesius (n 108) 99.

111 Making a similar argument with regard to the DSA, Eder (n 24) 3. For an overview of the different forms of AI harm that AI regulations may address, see Nathalie A Smuha, 'Beyond the Individual: Governing AI's Societal Harm' (2021) 10 Internet Policy Review 4–12.

112 Barbara Zmušková, 'Progressive Slovakia Becomes Target of AI Misinformation, Tops Polls' (*Euractiv*, 28

information and exchange of ideas in public fora,[113] or the environment?[114]

- Or also if it harms so many individuals at a scale (due to a platform's reach) that makes it systemic as, for example, in the case of widespread potential effects of platforms' AI systems promoting or heightening the risk of generating mental addiction[115] or gender-based violence?[116]

- Or even if AI recommender systems and genAI threaten to harm a few select individuals but with such a big reach that such harm attains a significant level of propagation across societies, as for example in the case of targeted deepfake porn campaigns towards female figures that are prominent opposers of Vladimir Putin's regime?[117]

- Or all of the above?

- Relatedly, how should one conceive and measure systemic AI risks – which, at least in part, allude to negative *collective* effects on social and political structures - when it comes to affected legal goods, such as fundamental rights, that are traditionally conceived as belonging to individuals and protected through *individual* remedies that address specific instances of harm?[118]

- Or, differently, an AI risk is systemic not (or not just) because of its systemic effects on societies and individuals, but (also) because those risks arise from systems, e.g. the digital public spaces created by digital platforms, their mediation through AI systems integrated therein, or the system-level content moderation policies of platforms that are, in turn, implemented by automated systems?[119]

61 A recent report found that researchers working on the DSA systemic risk provisions struggle to answer these and other related questions since they have very different views on whether different specific

September 2023) <https://www.euractiv.com/section/politics/news/progressive-slovakia-becomes-target-of-ai-misinformation-tops-polls/> accessed 23 September 2024; Joy Hyvärinen, 'Hostile Information Campaigns Could Test a Divided Finland' (*Tech Policy Press*, 30 May 2024) <https://techpolicy.press/hostile-information-campaigns-could-test-a-divided-finland> accessed 31 May 2024; Victoria Oldemburgo de Mello, Felix Cheung and Michael Inzlicht, 'Twitter (X) Use Predicts Substantial Changes in Well-Being, Polarization, Sense of Belonging, and Outrage' (2024) 2 Communications Psychology 1.

113 Laufer and Nissenbaum (n 11) 5–6; Article 19 and others, 'Civil Society Open Letter to Commissioner Breton' (17 October 2023) <https://www.article19.org/wp-content/uploads/2023/10/Civil-society-open-letter-to-Commissioner-Breton.pdf> accessed 9 October 2024.

114 Rachel Griffin, 'Climate Breakdown as a Systemic Risk in the Digital Services Act' (*Hertie School Centre for Digital Governance*, 7 September 2023) <https://www.hertie-school.org/en/digitalgovernance/news/detail/content/climate-breakdown-as-a-systemic-risk-in-the-digital-services-act> accessed 19 February 2024.

115 Aksha M Memon and others, 'The Role of Online Social Networking on Deliberate Self-Harm and Suicidality in Adolescents: A Systematized Review of Literature' (2018) 60 Indian journal of psychiatry 384; Amandeep Dhir and others, 'Online Social Media Fatigue and Psychological Wellbeing—A Study of Compulsive Use, Fear of Missing out, Fatigue, Anxiety and Depression' (2018) 40 International Journal of Information Management 141; Ashlee Milton and others, '"I See Me Here": Mental Health Content, Community, and Algorithmic Curation on TikTok', *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Association for Computing Machinery 2023) <https://doi.org/10.1145/3544548.3581489> accessed 15 February 2024.

116 Silvia Semenzin and Lucia Bainotti, 'The Use of Telegram for Non-Consensual Dissemination of Intimate Images: Gendered Affordances and the Construction of Masculinities' (2020) 6 Social Media + Society 2056305120984453; Thiago Dias Oliva, Dennys Marcelo Antonialli and Alessandra Gomes, 'Fighting Hate Speech, Silencing Drag Queens? Artificial Intelligence in Content Moderation and Risks to LGBTQ Voices Online' (2021) 25 Sexuality & Culture 700; Brennan Suen, Carly Evans and Alex Paterson, 'Right-Leaning Facebook Pages Earned Nearly Two-Thirds of Interactions on Posts about Trans Issues' (*Media Matters for America*, 9 November 2021) <https://www.mediamatters.org/facebook/right-leaning-facebook-pages-earned-nearly-two-thirds-interactions-posts-about-trans> accessed 3 July 2024.

117 European Commission, 2023 (n 9) 30. See also Gretchen Peters, 'Time to Act on Harmful Deepfakes & Algorithms' (*Tech Policy Press*, 31 October 2024) <https://techpolicy.press/time-to-act-on-harmful-deepfakes-algorithms> accessed 20 November 2024.

118 For a lengthier discussion of this theoretical issue applied to platform regulation see Griffin, 'Rethinking Rights in Social Media Governance' (n 108) 46–55.

119 To see similar approximations to this conceptual question, see Sally Broughton Micova and Andrea Calef, 'Elements for Effective Systemic Risk Assessment under the DSA' (Centre on Regulation in Europe (CERRE) 2023) 11–13 <https://cerre.eu/wp-content/uploads/2023/07/CERRE-DSA-Systemic-Risk-Report.pdf> accessed 16 May 2024, discussing the systemic provenance and effects of digital platforms' potential harms and how they contributed to the use of the notion of 'systemic risk' in the DSA; and Griffin, 'Rethinking Rights in Social Media Governance' (n 108) 55, mentioning that the DSA (although with regard to its art. 14[4] and not art. 34) might serve to address cases of 'systemic injustice', stemming from 'system-level enforcement of platforms' content policies'; Pielemeier and Sullivan (n 40).

cases constitute evidence of systemic risk.[120] Beyond researchers, it is highly likely that different platforms, public authorities and civil society organisations will have different understandings of what an AI systemic risk is. And, as demonstrated in Section B., the legislative indications for the definition of this concept are scarce. It appears that, in EU AI systemic risk management processes, the definition of what is to be managed – systemic risks – will be iteratively constructed, on a case-by-case basis. This is consistent with the fact that AI risk regulation, as any form of risk regulation, is process-based: it is not concerned with setting substantive standards beforehand but, differently, is predicated on the fact that those substantive standards will be generated by the successive outcomes of risk management processes.[121] Consequently, and as tautological as it may seem, an AI systemic risk will be whatever is defined (and then managed) as an AI systemic risk in the DSA and AIA's risk management processes.

62 This lack of conceptual clarity might disappoint some. But instead of causing disappointment, the indeterminacy of the concept of 'AI systemic risk' should, I argue, prompt a shift in our analytical focus. Particularly, if the definition of 'AI systemic risk' is to be constructed as different types of AI systemic risks are progressively identified and managed, it is key to analyse *how* the corresponding risk management processes develop and, especially, *who* has more agency in influencing their outcomes and, therefore, in shaping the meaning of AI systemic risks. When presented with the set of conceptual questions listed above, we should, I argue, answer with another set of - preliminary - questions. These are more oriented towards methodological and practical issues, but answering them will necessarily lead us to bigger conceptual clarity on the meaning of AI systemic risks:[122]

- Who has more agency/power – private regulated actors, public supervisory authorities, civil society organisations, researchers, or other stakeholders – in shaping the concept of AI systemic risk as the DSA and AIA are implemented?
- What are the ideas of what AI systemic risks are that gain more currency in the early regulatory dialogue?
- Based on which information and evidence do different actors across the DSA institutional ecosystem conclude for the (in)existence of a systemic risk? Are all actors given the same possibility to access high quality and up-to-date evidence to assess AI systemic risks?[123]
- Which frameworks and methodologies are used by different actors to identify and measure systemic risks in concrete cases?
- What (political)[124] priorities are set by different actors regarding systemic risk management? In other words, on what specific types of systemic risk will these actors concentrate their resources for risk assessment and management?

63 In this sense, it is worth noting that both risk regulation and, more specifically, the notion of 'systemic risk' have 'baggage'. As Kaminski points out, risk regulation in general has a certain policy baggage: the typical tools, tactics, and troubles of risk regulation as implemented in other fields are transposed into AI regulation by the policymaking decision to frame and regulate AI harms as risks.[125] Among several elements of such policy baggage are the difficulty of risk regulation to capture and manage unquantifiable harms, as well as its typical technocratic and "techno-correctionist" nature, which means that "it largely tries to fix problems with existing technologies rather than considering whether it would be better to put regulatory energy elsewhere – including not to use a technology at all".[126] As such, when risk regulation is used to address technological problems that entail policy and political decisions, it can obfuscate the latter

120 Marsh (n 40) 5–12.

121 *Supra* footnote 45.

122 Here, I take a slightly different stance than Marsh (n 40) 1, who, when reporting on researchers perceptions on systemic risk assessment in the DSA, argued that the "more pressing problems" when researching systemic risks under the DSA are "practical rather than conceptual". In my view, more practical questions are indeed very important but, crucially, because they influence and inform one's answer to the conceptual questions regarding the definition and assessment of systemic risks under the DSA. Conceptual questions are, ultimately, still more pressing; but they are, to a large extent, pre-determined by practical and material considerations.

123 Early reports of DSA access to information suggest that researchers/civil society have significant difficulties in accessing information both from platforms and public authorities. See, e.g. ibid 14; Darius (n 87).

124 Josephine Adekola, *Power and Risk in Policymaking: Understanding Public Health Debates* (Springer International Publishing 2020) 13–19; Griffin, 'What Do We Talk about When We Talk about Risk?' (n 15).

125 Kaminski (n 19) 1389–1403.

126 ibid 1390.

and "shield them from democratic accountability".[127]

64 The concept of 'systemic risk' arguably also has a distinct baggage. This concept has most extensively been used to measure risks of widespread instability in the financial sector.[128] It is within this field that the literature on systemic risk is most developed. This has already led some to test the application of that systemic risk framework to the DSA context.[129] The adequacy of the transplant of financial systemic risk frameworks to the DSA can be questioned for many reasons. Those frameworks are, equally, predominantly quantitative and highly technical,[130] which may lead to the same troubles signalled by Kaminski regarding risk regulation in general. If these systemic risk frameworks are transplanted into the management of AI systemic risks in EU law, they may thus turn such management into a predominantly technical exercise that fails to fully engage with the social meaning of platforms' AI systems and, therefore, to address less quantifiable AI harms.[131]

65 Conversely, both the DSA and AIA call for AI systemic risks to be framed in sociotechnical terms. Indeed, both regulations mention that risk management processes must consider the impact of AI technology on public values, and political and societal processes.[132] Moreover, they stress the need for AI risks to be assessed and managed depending on the specific social contexts where platforms' AI systems operate and with which they interact.[133] This can only be achieved if AI systemic risk management is framed in sociotechnical terms. This ultimately means conceiving AI risks as stemming not just from AI systems as technological artifacts; but, instead, from the (dynamic) interactions between AI systems and society.[134] It requires, that we understand AI technologies and AI-generated content - as well as the digital platforms integrating or spreading them - as part of broader social systems, i.e., configurations where they shape and are shaped by existing social practices (including values, norms, institutions, relationships, multiple different actors, and other technologies).[135] With this lens, one cannot escape the fact that AI systems mediate several aspects of social life and, in so doing, catalyse social and cultural change.[136] Therefore, AI systemic risk management should not be reduced to technological considerations, framed in solely technical terms and measured quantitatively. On the contrary, it should also capture the social, political, cultural – and thus less quantifiable – meaning and impact of AI technologies.[137]

127 ibid 1397; see also Griffin, 'What Do We Talk about When We Talk about Risk?' (n 15).

128 See, e.g., Paweł Smaga, 'The Concept of Systemic Risk' (The London School of Economics and Political Science 2014) Systemic Risk Centre Special Paper, No 5; Robert Engle, Eric Jondeau and Michael Rockinger, 'Systemic Risk in Europe' (2015) 19 Review of Finance 145.

129 Broughton Micova and Calef (n 119) 9.

130 See, e.g., Engle, Jondeau and Rockinger (n 128) 148–156.

131 For a discussion of other limitations of transplanting financial systemic risk frameworks into EU AI systemic risk management (in this case regarding DSA systemic risk management), see 'Implementing Risk Assessments under the Digital Services Act, Discussion Summary of the Workshop "Implementing Risk Assessments under the Digital Services Act"' (Global Network Initiative, Digital Trust & Safety Partnership and Brainbox 2023) 5 <https://dtspartnership.org/wp-content/uploads/2023/06/Discussion-summary-%E2%80%93-GNI-and-DTSP-workshops-on-implementing-risk-assessments-under-the-DSA-June-2023.pdf#page=12> accessed 1 July 2024; Alice Palmieri, Konrad Kollnig and Aurelia Tamò-Larrieux, 'Systemic Risks of Dominant Online Platforms: A Scoping Review' (Social Science Research Network, 2024) 8–9 <https://papers.ssrn.com/abstract=5002743> accessed 12 December 2024.

132 E.g. recitals 6, 27, 61, 110, and art. 3(65) AIA; and art. 34(1)(c)(d) DSA.

133 E.g. recital 20 AIA ("AI literacy should equip providers, deployers (...) with the necessary notions to make informed decisions regarding AI systems. Those notions may vary with regard to the relevant context and can include understanding (...), in the case of affected persons (...) how decisions taken with the assistance of AI will have an impact on them"); or recital 90 DSA ("Providers of very large online platforms and of very large online search engines should ensure that their approach to risk assessment and mitigation is based on the best available information and scientific insights and that they test their assumptions with the groups most impacted by the risks and the measures they take.") and European Commission, 2023 (n 9) 13-15. See more in Section C.II. below.

134 Merel Noorman and Tsjalling Swierstra, 'Democratizing AI from a Sociotechnical Perspective' [2023] Minds and Machines 4–5 <https://link.springer.com/10.1007/s11023-023-09651-z> accessed 8 February 2024; Brian J Chen and Jacob Metcalf, 'Explainer: A Sociotechnical Approach to AI Policy' (Data & Society 2024) 2–5 <https://datasociety.net/library/a-sociotechnical-approach-to-ai-policy/> accessed 3 October 2024; Brian Chen, 'Why AI Policy Needs a Sociotechnical Perspective' (*Tech Policy Press*, 29 May 2024) <https://techpolicy.press/why-ai-policy-needs-a-sociotechnical-perspective> accessed 29 May 2024.

135 Noorman and Swierstra (n 134) 4.

136 Julie E Cohen, 'Configuring the Networked Citizen' in Austin Sarat, Lawrence Douglas and Martha Merrill Umphrey (eds), *Imagining New Legalities: Privacy and Its Possibilities in the 21st Century* (Stanford, CA: Stanford University Press, 2012) 129–130.

137 A similar argument is made with relation to DSA systemic risk management in Meßmer and Degeling (n 40) 15.

66 All in all, the typically technocratic and quantitative nature of risk regulation and (predominant) financial understandings of systemic risk may, if applied to EU AI systemic risk management, leave outside of the DSA and AIA's frame several systemic forms of harm that these regulations want to address. It may render invisible more intangible forms of AI harm, obfuscate the political decisions necessarily made in risk management, and neglect the sociotechnical meaning of AI technologies. This would ultimately go against a second normative commitment of the EU's integrated AI risk management framework: that risk assessment and mitigation methodologies should be contextual.

II. Methodologically contextual systemic risk management

67 The DSA and AIA's sociotechnical framing has methodological implications. In particular, the methodologies used in both risk assessment and mitigation must be contextual. This means that any decision on whether and how to assess or mitigate a certain AI risk must consider the meaning and impact of AI technologies on the *social contexts* where those technologies are employed and where their effects are felt. As shown in Section B., both the DSA and AIA require that.[138]

68 The two regulations under analysis do not provide a full answer on how to contextualize risk management. However, drawing from several indications gathered in Section B., one can gain different insights from the DSA and AIA risk management frameworks which may be mutually translatable between them.

69 Firstly, risk assessment and mitigation must consider the societal or sociotechnical contexts where VLOP/SEs operate and, therefore, where the effects of their AI systems are felt.[139] References to 'societal context' should be conceived broadly, so that they encompass effects on society as a whole and broader collective goods,[140] particular situations of societal vulnerability,[141] cultural specificities such as regional and linguistic differences between impacted communities (art. 34(2) DSA and art. 13(1)(a)(i) DRA), as well as the political context of certain communities at given moments in time, such as in the case of a concrete election[142] or coordinated disinformation campaign.[143]

70 Such societal context should influence the choice of risk assessment and mitigation methodologies (art. 9(4)(a) DRA). It should also influence the specific contouring of selected methodologies, in terms of scope, processes of consultation of impacted individuals and groups, and data sampling. Regarding scope, the acute societal impact of platforms' AI systems on a particular issue or community might dictate that issue-specific (as opposed to general) risk management processes be carried out, e.g. for election periods[144] or for child harm online.[145] Still relating to scope, if the AI risks of platforms are not specific to an isolated VLOP/SE but are rather caused by many platforms, then risk assessments must be longitudinal and consider the compounded negative effects of platforms' AI systems on a given societal good.[146]

138 Recital 79, 90, and art. 34 (2) DSA; European Commission, 2023 (n 9) 10, 13, 15, 63; European Commission, 2024 (n 9) paras. 11-13. In the AIA, this is mainly noticeable regarding the identification and management of high-risk AI systems, see recital 64, 93, and arts. 3(12) and 9(5) AIA. As for systemic risk management in the AIA, although the regulation is somewhat silent regarding risk management methodologies, one can observe the emphasis on its sociotechnical framing and contextual methodologies by looking into the draft of the forthcoming code of practice on systemic risk management of GPAIs: Oliver and others (n 95) 4, 19, 30. A similar focus on context-based risk assessment and mitigation can be found in the AI risk assessment methodology being developed in the Council of Europe, with which the Commission seeks to align the AIA, see Luca Bertuzzi, 'EU Commission Seeks Alignment of AI Treaty's Risk Methodology with AI Act' (*MLex*, 8 November 2024) <https://shorturl.at/N4lWh>. Therein, Bertuzzi reports: "The European Commission wants to ensure that the methodology for risk and impact assessment for AI systems being developed in the Council of Europe is aligned with the EU's AI Act while remaining non-binding. (...) The methodology is based on four building blocks: a context-based risk assessment to collect and map the relevant information, a stakeholder engagement process to contextualize potential harm and risk mitigation measures (...)".

139 European Commission, 2023 (n 9) 15-16, 24-25; recitals 20, 24 and art. 9(4)(a) DRA; Oliver and others (n 95) 19.

140 It is useful here to look at the indicated impacted goods of the DSA and AIA risk management framework in art. 34(1)(c) and (d) DSA and art. 3(65) AIA.

141 Oliver and others (n 95) 19.

142 European Commission, 2024 (n 9), paras. 31, 36, and 43.

143 European Commission, 2023 (n 9), 24-25.

144 *Supra* footnotes 52 and 142.

145 'Call for Evidence for an Initiative: Digital Services Act - Guidelines to Enforce the Protection Online' (*European Commission*, 25 September 2024) 2 <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14352-Protection-of-minors-guidelines_en> accessed 25 September 2024; 'Commission Opens Proceedings against TikTok under the DSA' (n 80).

146 European Commission, 2023 (n 9), 8, 11, 13, 32, 46, 48, 63, 69; European Commission, 2024 (n 9), para. 16(h)(ii); Marsh (n 40) 11–12.

71 Furthermore, the assumptions that platforms, public authorities and auditors make regarding the existence, assessment, and how best to mitigate emerging AI risks must be tested with the groups (and, if applicable, their representative organisations) impacted by AI systems of platforms (recital 90, DSA; art. 13(1)(a)(v) DRA; recital 116 and art. 56(4) AIA[147]). This requires the consultation and involvement of impacted individuals and communities in risk management methodologies, something that the European Commission has already started doing.[148] Finally, and also to achieve an accurate portrayal of the population affected by AI risks, the samples of data to be used in risk assessments and in auditing risk mitigation measures should be representative and, in particular, appropriately depict the concerns of especially affected groups (with particular regard given to minor, vulnerable groups and minorities).[149]

72 The above are just a few non-exhaustive indications found in law and related policy recommendations regarding the selection and contouring of risk management methodologies. The two regulations do not prescribe a single adequate methodology for AI risk management; nor do they answer the question of how to ultimately calculate and assess the risks and impacts of platforms' AI systems. The latter remains an open question to be answered as iterative risk management procedures are developed by private regulated actors and scrutinised by public authorities.[150]

73 This section sought, however, to distil from these methodological indications a common, principle-level, emphasis placed by both the DSA and AIA on the need to socially contextualise AI risk management. Such methodological principle, as well as the sociotechnical frame of systemic risks depicted in Section C.I., are better accommodated by so-called 'social sciences approaches' or 'sociocultural theories' of risk.[151] These perspectives of risk[152] were developed in criticism of the limitations of dominant technical and probabilistic assessments of risk, which are carried out in abstraction from social contexts. Therefore, sociocultural theories of risk sustain that risk assessment and mitigation decisions should, at least in part, consider the *subjective* perceptions of individuals and groups regarding different sources of risk and their potential negative impacts.[153] In that sense, it is arguable that AI risk management methodologies, however they may be concretely tailored, should ensure that individuals and communities are able to articulate their perceptions of AI risks. This links to a third normative commitment of the integrated AI systemic risk management framework under analysis: that risk governance should be participated.

III. Participated systemic risk governance: in comes civil society

74 The DSA and AIA heavily rely on self-regulation by the providers and deployers of AI systems to assess and mitigate relevant emerging risks. As shown in Section B., digital platforms (as AI deployers) and AI providers are the primary decision-makers when it comes to assessing and mitigating emerging AI risks. This means they have the discretion to (i) determine what systemic risks are posed by AI systems in each concrete moment; (ii) which methodologies are used to identify and measure those risks; and (iii) whether and how identified AI risks are mitigated.

75 This discretion afforded to regulated tech companies entails a risk of their lack of accountability. Particularly, those companies may be able to entrench and privilege their own interests in how AI systemic risks are managed. This is supported by existing literature on previous experiences of empowering regulated tech companies to implement and concretise legislative requirements imposed on them.[154]

147 The AIA prescribes that codes of practice are drawn up with the input of, amongst others, "affected persons". One of the codes of practice to be drawn up in the context of the AIA is the one whereby procedures and measures for systemic risk assessment and management will be agreed upon by several AI providers and deployers.

148 See, e.g., European Commission, 'Call for Evidence for an Initiative: Digital Services Act - Guidelines to Enforce the Protection Online' (n 145) 4; European Commission, 'AI Act: Have Your Say on Trustworthy General-Purpose AI' (30 July 2024) <https://digital-strategy.ec.europa.eu/en/consultations/ai-act-have-your-say-trustworthy-general-purpose-ai> accessed 19 November 2024, mentioning 'rightsholders'.

149 Arts. 12 and 13(1)(a)(v) DRA.

150 On this note, the publication of systemic risk management reports and audits under the DSA is already underway, see Hohfeld (n 66). For an early commentary on published risk assessments, see Sally Broughton Micova, 'Evaluating Systemic Risk Management under the DSA' (*CERRE*, 6 December 2024) <https://cerre.eu/news/evaluating-systemic-risk-management-under-the-dsa/> accessed 6 December 2024.

151 Ortwin Renn, *Risk Governance: Coping with Uncertainty in a Complex World* (Earthscan 2008) 22–45; Haines (n 20) 184–185.

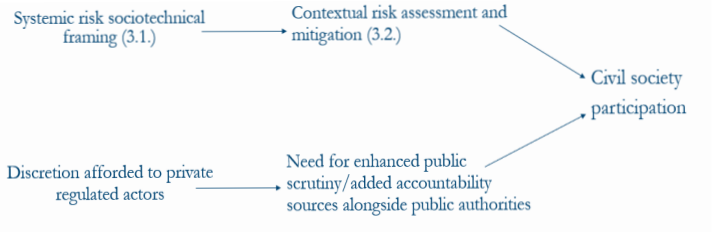
152 For an overview of the different social sciences approaches to assessing and managing risk, see Renn (n 151) 13–45.

153 ibid 40–42.

154 *Supra* footnotes 24 and 79; Kaminski and Malgieri (n 34) 128–129, 133–134, 140; Griffin, 'Rethinking Rights in Social Media Governance' (n 108) 43–51.

76 Applying these insights to the implementation of the EU's AI risk management framework, there is a distinct risk that regulated AI companies gain the dominant power to influence how the meaning of 'AI systemic risk' is shaped from the early stages of DSA and AIA implementation. Indeed, being very broad, the concept of AI systemic risk is open to different interpretations. Equally, systemic risk mitigation can also be done through different measures. As primary decision-makers in the EU's AI risk management provisions, may thus be able to decide how AI systemic risks are defined and mitigated *without* there being appropriate public accountability structures with adequate informational capacity.

77 In order to counter these accountability gaps favouring regulated tech companies, both the EU legislator and several scholars have highlighted the role that civil society actors can have in enhancing the public scrutiny over systemic risk management processes.[155] Civil society is here understood as encompassing not just civil society organisations, but also digital and non-digital NGOs, academic researchers, research institutes, investigative journalists, and fact-checkers.[156] There are two main stated rationales in the DSA and AIA for civil society involvement in risk management processes (Graph 1). First, if systemic risk should be framed in sociotechnical terms and its assessment and mitigation must be contextual, then civil society participation allows for the articulation of (at least some) competing visions of how AI systemic risks should be defined and mitigated. Such risk management decisions should be informed by the experiences and concerns of affected individuals and communities.[157] Second, civil society participation can enhance public scrutiny over platforms' AI risk management choices, thus complementing and feeding into the regulatory supervision of competent European and national public authorities.[158]



Graph 1: the rationales for civil society participation in the DSA and AIA

155 Recitals 40, 90, 92, 95-98, 137 DSA; and recitals 20, 27, 65, 74, 111, 116, 121, 139, 148, 150, 165 and arts. 56, 67, 95(2)(d) and (3) AIA. See also Martin Husovec, 'Will the DSA work?: On money and effort' (Verfassungsblog, 9 November 2022) <https://verfassungsblog.de/dsa-money-effort/> accessed 3 October 2023; Eder (n 24); European Commission, 2024 (n 9) paras. 12, 18, 31-36.

156 Marsh (n 40) 4; Suzanne Vergnolle, 'Putting Collective Intelligence to the Enforcement of the Digital Services Act: Report on Possible Collaborations between the European Commission and Civil Society Organisations' [2023] SSRN Electronic Journal 12 <https://www.ssrn.com/abstract=4435885> accessed 11 January 2024; Margot E Kaminski and Gianclaudio Malgieri, 'Impacted Stakeholder Participation in AI and Data Governance' (2024) 43–46 <https://papers.ssrn.com/abstract=4836460> accessed 18 September 2024. Although Vergnolle mentions industry groups as part of her operative definition of civil society organisations (which is perfectly conceivable since such groups are indeed called to participate in the implementation of the DSA and AIA, mainly by the Commission), I have left them out of this paper's definition of civil society, since they represent regulated actors, i.e., the tech industry companies on whom legislative requirements are imposed and whose compliance with such requirements public authorities and other civil society actors seek to scrutinise. To include industry representative groups in the definition of civil society in a paper directed at mapping how civil society participation can hold regulated companies to account would, for that reason, be illogical.

157 Recitals 90, 140 DSA; art. 13(1)(v) DRA; recitals 27, 93, 96 and arts. 56(4) AIA; Oliver and others (n 95) 15.

158 Recitals 40 and 90 DSA; Recital 1 DRA; Recital 20 AIA; Oliver and others (n 95) 23.

78 The enhancement of public scrutiny enabled by civil society participation can be understood in both quantitative and qualitative terms. Quantitatively, civil society will logically provide more instances of control, resources and data in addition to those of public authorities. Qualitatively, civil society participation may be a conduit for increasing the expertise needed to oversee regulated actors' compliance with their risk management obligations under EU law. In this sense, the DSA and AIA explicitly seek two types of expertise when it comes to AI risk management processes. First, there is a need for technical expertise on the technological capabilities of AI technologies and their impact.[159] In addition to technical expertise, the two regulations also look for first-hand or mediated lived knowledge of the impact of AI systems on those individuals and communities that are particularly affected by them.[160] Kaminski and Malgieri have designated this form of knowledge as 'lived expertise',[161] building on prior scholarly work that argued for the articulation of the lived experiences of affected individuals and communities in participatory schemes of AI governance.[162] The concept of lived expertise is not specific to AI governance. Indeed, prior work in areas such as criminal justice[163] or medical research[164] has analysed in those terms the idea of gathering and using the 'lived' lay knowledge of individuals - as experts on the effects of, e.g., certain laws, policies, institutional practices, social violence, mental health or physiological conditions – in processes of law-making, legal enforcement, institutional reform or highly technical research.[165] In addition, a recent turn in EU legal scholarship has called for the investigation of 'lived experiences' of individuals in order to better understand "the significance, challenges and opportunities" of the implementation of EU law.[166]

79 It must be acknowledged that 'expertise' in EU AI risk management may still be interpreted narrowly, so as to only include technical expertise. That much latitude is offered to the public authorities and regulated actors responsible for setting up participated procedures of AI risk management. Nevertheless, this paper argues that lived expertise is crucial for effectively achieving the normative commitments highlighted in sections C.I. and C.II., namely that systemic risk management processes be contextual and fully grasp the sociotechnical meaning of AI systems . For this to happen, civil society participation must also be about articulating the concerns and lived experiences of individuals and communities regarding the impact of AI systems. Their perceptions of AI systemic risks – even if not concretised in technical jargon – should influence, I argue, how regulators, researchers and platforms understand AI systemic risks and, in turn, shape how those risks are assessed and mitigated.

80 To sum up, both the DSA and AIA call for participated AI systemic risk management, as a way to contextualise those processes and inform public regulatory scrutiny with different forms of knowledge on the impact of AI systems. Although this possibility for civil society participation in risk management processes is explicitly endorsed in the DSA and AIA, the corresponding procedures are unclear. The next section uncovers and systematises them.

159 E.g., European Commission, 2024 (n 9), para. 18; recital 96 DSA; recitals 111, 151 and art. 68(2) AIA; Husovec (n 155).

160 E.g., art. 12(2)(f) and 13(1)(v) DRA; recital 20 and art. 56(4) AIA; Oliver and others (n 95) 15. In European Commission, 2024 (n 9) para. 35, we can notice an appeal to VLOP/SEs to engage with not just academics and civil society organisations but also with "representatives of various communities" in order to identify systemic risks that need mitigation in the context of electoral processes and civic discourse. One can imagine that the communities mentioned here will be those that suffer some negative effects that may then contribute to the identification of emerging systemic risks.

161 Kaminski and Malgieri (n 156) 55.

162 Ngozi Okidegbe, 'The Democratizing Potential of Algorithms?' (2022) 53 Connecticut Law Review 739, 762–765, 776. Okidegbe's work relates to the use of algorithmic technologies in pre-trial criminal procedures. In this context, she calls 'communal knowledge' to individuals' lived experience of the impact of algorithmic technologies used to determine whether they would be subject to pre-trial incarceration.

163 Benjamin Levin, 'Criminal Justice Expertise' (2022) 90 Fordham Law Review 2777. Kaminski and Malgieri take Levin's work as inspiration for their idea of 'lived expertise' being feature in AI governance.

164 Evelyne Baillergeau and Jan Willem Duyvendak, 'Experiential Knowledge as a Resource for Coping with Uncertainty: Evidence and Examples from the Netherlands' (2016) 18 Health, Risk & Society 407; Eva Marie Castro and others, 'Patients' Experiential Knowledge and Expertise in Health Care: A Hybrid Concept Analysis' (2019) 17 Social Theory & Health 307.

165 Baillergeau and Duyvendak (n 164) 408–410; Levin (n 163) 2821, 2828.

166 Floris de Witte, 'Here Be Dragons: Legal Geography and EU Law' (2022) 1 European Law Open 113, 116; Loïc Azoulai, 'Reconnecting EU Legal Studies to European Societies' [2024] Verfassungsblog <https://verfassungsblog.de/reconnecting-eu-legal-studies-to-european-societies/> accessed 27 March 2024.

D. The cracks in the law: mapping the loci of civil society participation in EU AI risk management

81 In the legal regime just described, there is no clear and systematised understanding of the modalities of civil society involvement in this regulatory framework. This section fills that gap, by mapping out all possible formal and informal avenues for civil society participation and involvement in EU AI risk governance. One key point is that civil society participation should not be understood here as only encompassing formal ways of public participation in the implementation of the law.[167] While it may include those mechanisms, to fully capture how civil society may attempt to influence platform AI risk regulation, this paper adds more informal avenues of civil society *involvement*. Indeed, legal mobilisation literature has pointed out that civil society actors may strategically opt to influence legal implementation and adjudication through informal means, i.e., those not explicitly recognised in the law as modes of public participation.[168]

82 All the possibilities for civil society participation in the EU's AI risk governance structure – so-called 'loci of participation' - have been mapped in Table 1. It should be added that many of the mapped loci are not designed to enable civil society to intervene *specifically* in the management of platforms' AI risks. Indeed, many DSA-related loci can be used for intervening in the management of risks stemming from other features of digital platforms beyond their AI systems. Similarly, many of the AIA-related loci may be used to influence the management of risks of non-platform-related AI systems.

83 Furthermore, it is expected that this mapping exercise evolves over time, as new stakeholder participation and involvement initiatives surface in this field.

167 Deirdre Curtin, 'Transparency and Political Participation in EU Governance: A Role for Civil Society?' (1999) 3 Cultural Values 445; Deirdre Curtin and Joana Mendes, 'Transparence et participation: des principes démocratiques pour l'administration de l'union européenne' (2011) 137–138 Revue française d'administration publique 101; Joana Mendes, *Participation in EU Rule-Making: A Rights-Based Approach* (Oxford University Press 2011) <https://academic.oup.com/book/11861> accessed 21 November 2023.

168 Muir, Dawson and Claes (n 32); Conant and others (n 32).

Table 1: The loci of participation of the integrated EU AI risk management framework applicable to digital platforms

Locus of participation	Legal basis	Civil society actor(s)	Institutional type	Rationale	Expected sought or used expertise
Audits of platforms' risk assessment and mitigation action by vetted researchers (within the context of research supported by privileged access to information in accordance with DSA)	Recitals 96-98 and art. 40(4)(8) DSA; recital 1 DRA	DSA's vetted researchers, who must be affiliated to a research organisation devoted primarily to scientific research (art. 40(8)(11) DSA)	Informal	**Contestation:** conduct research based on privileged access to information that contributes to the assessment and contestation of platforms' risk assessment and mitigation choices. Research output will be made publicly available and put at the service of public authorities and the public at large.	Mostly technical expertise (see emphasis on scientific research), but maybe lived expertise, depending on the specific research project of the researcher in question
Supporting Digital Service Coordinators in data access processes pursuant to art. 40 DSA	Recital 23 and art. 14 Access to Data Delegated Regulation	Expert individuals or organisations with relevant expertise on specific elements of data access process[169]	Formal (organic)	**Enhanced public scrutiny:** support and facilitate the exercise by DSCs of their decisional function regarding the determination of whether and how much data should be shared by VLOP/SEs with vetted researchers pursuant to art. 40 DSA.	Technical expertise
Commission audits with the involvement of individual experts	Art. 69(3) and (5), and 72(2) DSA; Para. 53, DSA risk mitigation guidelines; recital 3 and art. 3(5)-(7) Implementing Regulation 2023/1021	Individual experts (can be vetted researchers) invited by the Commission to help support the platform audits it carries as part of its monitoring powers[170]	Formal (organic)	**Enhanced public scrutiny (and maybe explicit contestation):** support the performance of Commission-led audits to assess platforms' risk assessment and mitigation choices. If the Commission finds shortcomings and pursues corrective action, contestation will be involved.	Technical expertise

169 Some exemples given in recital 23 of the Access to Data Delegated Regulation are 'the determination of the access modalities, including appropriate interfaces, the formulation of the reasoned request [for data access] and any amendment requests [to the researcher's reasoned request] by the data provider'.

170 See in 'Commission Sends Preliminary Findings to X for Breach of DSA' (*European Commission*, 12 July 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3761>: "Based on an in-depth investigation that included, among others, the analysis of internal company documents, *interviews with_experts* [N.B. emphasis added by author], as well as cooperation with national Digital Services Coordinators (...)". Similarly, but mentioning "third parties" and not "experts", see 'Commission Opens Formal Proceedings against Temu under DSA' (n 81).

Submission of evidence to Commission and/or national regulators	Recital 141 and art. 51(1)(a), 67(1), 68(1), 72 DSA; art. 79(7), 90(3)(c) AIA (although not specifically, they signal the Commission's normal openness to receiving evidence from interested parties)	Individual experts and all interested/impacted stakeholders; civil society organisations	Informal	**Enhanced public scrutiny:** provide evidence to public supervisory authorities about emerging AI risks, their societal impact, and how platforms and other AI deployers and providers contribute to, assess and manage those risks.	Technical and/or lived expertise (type of expertise might be limited by the willingness of the Commission or the national regulator to receive certain types of evidence)
Participation in public consultations[171] and calls for evidence[172] for the development of guidelines or elaboration of risk assessments[173]	Recital 103 and art. 35(3), 39(3), 63(1)(e) DSA; DSA risk mitigation guidelines; Art. 96 AIA *juncto* arts. 3(2)(c) and 4(1)(b) AI Office Decision	Individual experts and all interested/impacted stakeholders; civil society organisations	Formal (procedural)	**Inclusiveness/legitimacy-building + enhanced public scrutiny:** Commission seeks to hear experts and impacted individuals and communities in the preparation of guidelines. This is aimed at combatting the opaqueness of guideline development and ensuring stakeholder representation; and have stakeholders provide additional information and give their opinions on what are relevant risks, what methodologies or metrics for risk assessment should be considered, and what risk mitigation best practices should be contained in the guidelines.	Lived[174] and technical expertise

171 See, e.g., European Commission, 2024 (n 9); European Commission, 'Multi-Stakeholder Consultation for Commission Guidelines on the Application of the Definition of an AI System and the Prohibited AI Practices Established in the AI Act' (13 November 2024) <https://digital-strategy.ec.europa.eu/en/news/commission-launches-consultation-ai-act-prohibitions-and-ai-system-definition>.

172 See, e.g., European Commission, 'Call for Evidence for an Initiative: Digital Services Act - Guidelines to Enforce the Protection Online' (n 145).

173 Vergnolle (n 156) 44.

174 European Commission, 'Call for Evidence for an Initiative: Digital Services Act - Guidelines to Enforce the Protection Online' (n 145) 3–4.

Collaborative development of codes of conduct and codes of practice[175]	Recitals 98, 103, 107 and art. 45(2) DSA; recital 27, 165 and arts. 56(3)(4) and 95(2)(d) and (3) AIA; arts. 3(2)(i) and 4(1)(b) AI Office Decision	Individual experts and all interested/impacted stakeholders; civil society organisations[176]	Formal (procedural)	**Inclusiveness/legitimacy-building:** hear experts and impacted individuals and communities and have them contribute to the drawing up of codes of conduct.	Lived and technical expertise
Other outreach initiatives directed at civil society and researchers (such as hackathons, stress tests or other crowdsourced events)[177]	No legal basis and unclear form, but that possibility has been mentioned by the Commission[178] in the context of the DSA and, theoretically, nothing excludes that it puts together these initiatives also in the context of the AIA	Individual researchers and civil society organisations	Formal (procedural)	**Inclusiveness/legitimacy-building + enhanced public scrutiny:** this will very much depend on the objective and format of every outreach initiative but, in general, it is assumed that this pursues Commission's double objective of obtaining, centralising and analysing additional data on a regulatory matter of interest. This also increases the representative credentials of the Commission's enforcement action.	Lived and technical expertise (depending on the specific outreach initiative)

175 E.g., European Commission, 'First Draft of the General-Purpose AI Code of Practice Published, Written by Independent Experts' (2024) <https://digital-strategy.ec.europa.eu/en/library/first-draft-general-purpose-ai-code-practice-published-written-independent-experts> accessed 19 November 2024.

176 In cases like that of the General-Purpose AI Code of Practice referenced in the footnote above, the involvement of stakeholders is done in accordance with a layered process, where there are multiple opportunities (with different levels for civil society access) to offer inputs to the development of a code of practice. In this case, some independent experts chosen by the Commission elaborated a first draft with contributions from general-purpose AI providers which then was submitted to an open multi-stakeholder consultation during two months. In parallel, 1000 stakeholders (civil society organisations, researchers, business groups, and others – there is no clarity regarding all types of represented actors) were selected by the Commission based on an open call for applications. The selected 1000 stakeholders will meet with the drafters of the code of practice in 3 iterative rounds, with the code being amended based on stakeholder input. For this, see European Commission, 'AI Act: Participate in the Drawing-up of the First General-Purpose AI Code of Practice' (30 July 2024) <https://digital-strategy.ec.europa.eu/en/news/ai-act-participate-drawing-first-general-purpose-ai-code-practice> accessed 19 November 2024; European Commission, 'Meet the Chairs Leading the Development of the First General-Purpose AI Code of Practice' (30 September 2024) <https://digital-strategy.ec.europa.eu/en/news/meet-chairs-leading-development-first-general-purpose-ai-code-practice>; 'The Kick-off Plenary for the General-Purpose AI Code of Practice Took Place Online' (30 September 2024) <https://digital-strategy.ec.europa.eu/en/news/kick-plenary-general-purpose-ai-code-practice-took-place-online> accessed 19 November 2024.

177 Vergnolle (n 156) 47; The European Board for Digital Services, 'Report on the European Elections: Digital Services Act and Code of Practice on Disinformation' (2024), p. 5 <https://digital-strategy.ec.europa.eu/en/library/european-board-digital-services-publishes-post-election-report-eu-elections>. For some examples of DSA and AIA-relevant outreach events to researchers, see European Commission, 'Info Webinar for Researchers: DSA Art 40 Delegated Act' (*EUSurvey*, 2024) <https://ec.europa.eu/eusurvey/runner/DataAccessInfoWebinar> accessed 18 November 2024; European Commission, 'Call for Evaluators: Participate in the European AI Office Workshop on General-Purpose AI Models and Systemic Risks' (25 November 2024) <https://digital-strategy.ec.europa.eu/en/news/call-evaluators-participate-european-ai-office-workshop-general-purpose-ai-models-and-systemic> accessed 12 December 2024.

178 European Commission, 'Call for Evidence for an Initiative: Digital Services Act - Guidelines to Enforce the Protection Online' (n 145) 3.

Involvement in platform audits at the invitation of VLOPs and VLOSEs	Art. 37 DSA *juncto* arts. 12 and 13(1)(a)(v) DRA	Impacted individuals and communities, especially those deemed as most vulnerable	Regulatee-promoted	**Inclusiveness/legitimacy-building + Participatory design:** to test platforms' assumptions regarding the effectiveness of their risk management choices with impacted stakeholders.	Lived and technical expertise
Participation in Commission-led processes for updating delegated acts that update risk lists of the AIA	Recital 173 and Art. 112(11) AIA; arts. 3(2)(a) and 4(1)(b) AI Office Decision	Individual experts and all interested/impacted stakeholders; civil society organisations	Formal (procedural)	**Inclusiveness/legitimacy-building:** Commission hears experts and impacted individuals and communities in the preparation of updating the delegated acts that determine which AI systems present high-risk, unacceptable risk, and systemic risk; combat opaqueness of delegated act adoption.	Lived and technical expertise
Participation in hearings of EP that may inform potential objections to how the Commission has exercised its delegated power to update the risk lists of the AIA	Linked to arts. 6 and 7 AIA. No explicit basis in AIA, but linked to parliamentary practice of the European Parliament[179]	Individual experts and impacted stakeholders who are invited by the EP or the Council to be heard on a specific AI risk; civil society organisations	Formal (procedural)	**Enhanced public scrutiny:** provide information on the risks of specific AI systems whose risk status under the AIA was changed through a Commission delegated act. This additional information informs the scrutiny exercised by the Parliament over the Commission's decision to adopt such a delegated act.	Lived and/or technical expertise (depending on Parliament's request)
Involvement in red teaming exercises and other adversarial testing	Para. 27, d), DSA risk mitigation guidelines; recital 60q and art. 55(1)(a) AIA; Commission press release on election Stress Test[180]	Individual experts invited by VLOPs and VLOSEs as well as GPAI providers	Regulatee-promoted	**Enhanced public scrutiny:** have independent experts test genAI and other GPAIs for bias and other risk sources by seeking to game/exploit their design and other vulnerabilities.	Technical expertise
Ad hoc cooperation projects, expert consultations, and constructive dialogues between platforms and civil society	Paras. 18, 23, 31-36, DSA risk mitigation guidelines	Individual experts, research community and all relevant stakeholders	Regulatee-promoted	**Enhanced public scrutiny:** obtain extensive feedback and additional insights on risk management policies and actions.	Technical expertise

179 See, e.g., Amandine Crespy and Louisa Parks, 'The European Parliament and Civil Society' in Olivier Costa (ed), *The European Parliament in Times of EU Crisis: Dynamics and Transformations* (Springer International Publishing 2019); Laura Landorff, 'Who Gets a Seat at the Table? Civil Society Incumbents and Challengers in the European Parliament's Consultations' in Håkan Johansson and Anna Meeuwisse (eds), *Civil Society Elites: Exploring the Composition, Reproduction, Integration, and Contestation of Civil Society Actors at the Top* (Springer International Publishing 2024).

180 This is a very recent example of collaborative (i.e., Commission-promoted) testing of how VLOPs and VLOSEs mitigate specific risks according to the DSA. See 'Commission stress tests platforms' election readiness under the Digital Services Act' (*European Commission*, 24 April 2024), available at: <https://shorturl.at/cdmT8>. Another example of red teaming exercises potentially relevant for AIA enforcement can be found here: Will Douglas Heaven, 'How OpenAI Stress-Tests Its Large Language Models' (*MIT Technology Review*, 21 November 2024) <https://shorturl.at/dmqOp> accessed 10 January 2025.

Cooperation between platforms and independent fact-checking organisations[181]	Paras. 12-14, 16(c), 36, 51, DSA risk mitigation guidelines	Independent fact-checking organisations (e.g. the European Digital Media Observatory[182]) and journalists	Regulatee-promoted	**Enhanced public scrutiny:** capacity-building for adopting risk mitigation measures applied by platforms to manage systemic risks to electoral processes and civic discourse, namely by helping to flag false/deceptive AI-promoted and/or generated content.	Technical expertise
Issuance of qualified alerts of systemic risks of GPAIs	Arts. 51(1)(b), 68 and 90 AIA	Appointed/invited independent experts of scientific panel created by Commission in governance structure of AIA	Formal (organic)	**Enhanced public scrutiny (maybe through explicit contestation):** to provide a qualified alert[183] to the AI Office[184] flagging that a GPAI presents a systemic risk that needs to be managed at Union level (this will entail contestation if the GPAI provider has stated that the model does not present a systemic risk); based on this qualified alert, the Commission will designate the GPAI as presenting systemic risk, triggering a series of risk management obligations for the GPAI provider.	Technical expertise
Membership of scientific panel or advisory forum created in the governance framework of AIA	Recitals 148, 150 and 151 and arts. 67 and 68 AIA	Appointed/invited individual experts (for scientific panel); and also, for advisory forum, of civil society organisations and other interested/ impacted stakeholders with recognised expertise in the field of AI	Formal (organic)	**Enhanced public scrutiny:** to support the Commission (including its AI Office) and the AI Board in their implementation tasks under the AIA.	Mainly technical, but possibly also lived expertise for the advisory forum[185]

181 See, e.g., The European Board for Digital Services (n 177) 6.

182 ibid.

183 Relying on privileged access to information on GPAIs based on art. 91(3) AIA.

184 The AI Office is an internal division of the Commission entrusted with overseeing advancements in AI development, as well as the enforcement and monitoring of the AIA. See art. 55b AIA and AI Office Decision for more details.

185 This will ultimately depend on the interpretation by institutional actors of the concept of 'expertise' in art. 58a AIA.

Membership of DSA expert groups at European or national level[186]	Art. 64 DSA	Individual experts or members of civil society organisations with expertise in platform regulation (and related AI matters) which are invited to join expert groups set up by the Commission or by the DSA national regulators of each Member State (Digital Services Coordinators)	Formal (organic)	**Enhanced public scrutiny:** to support the Commission and Digital Services Coordinators in their supervision tasks under the DSA, including overseeing risk management processes.	Technical expertise
Invitation to attend meetings or to be consulted by the European Board for Digital Services (EBDS)	Art. 62(5) and (6) DSA	Individual experts or interested stakeholders who are invited to attend/ observe the meetings of EBDS, or that are consulted by it at its own initiative	Formal (organic)	**Enhanced public scrutiny:** to support the EBDS in its meetings and the fulfilment of its advisory and coordination tasks.	Technical expertise
Participation (and possible contestation) in processes of development of harmonised standards + implementing acts for Commission to adopt common specifications *in lieu* of harmonised standards	Recital 121 and art. 40(2) AIA; art. 3(2)(d) and 4(1)(b) AI Office Decision; art. 5 of Regulation 1025/2012	All interested/impacted stakeholders; civil society organisations; researchers	Formal (organic or procedural, depending on the modalities of stakeholder inclusion)	**Enhanced public scrutiny (maybe through explicit contestation) + Inclusiveness/legitimacy-building:** Standardisation organisations (for the development of technical standards) and Commission (for development of request for the production of standards or development of common specifications[187]) hears experts and other interested/ impacted stakeholders (including through advisory forum) in the preparation of European harmonised standards and other related documents; ensure inclusiveness/legitimacy of standardisation processes.[188]	Technical and lived expertise

186 This is a concrete proposal of civil society involvement made by Suzanne Vergnolle to concretise the mandate of the Commission and national regulators of creating the necessary expertise and capabilities to oversee DSA compliance. See Vergnolle (n 156) 23–43, 50–51.

187 Per art. 41 AIA, the Commission will adopt common specifications in case harmonised standards have not been, are deemed insufficiently protective of fundamental rights concerns, or otherwise do not comply with the corresponding Commission's request.

188 For general theory on civil society participation in technical standardization processes, see, inter alia, Annalisa Volpato and Mariolina Eliantonio, 'The Participation of Civil Society in ETSI from the Perspective of Throughput Legitimacy' (2024) Innovation: The European Journal of Social Science Research 1.

Participation in regulatory sandboxes	Arts. 53(16)(17) and 58(2)(f) AIA; arts. 3(2)(e) and 4(1)(b) AI Office Decision	Individual researchers and all interested/impacted stakeholders	Formal (organic or procedural, depending on the modalities of stakeholder inclusion)	**Technological participatory design:** involvement in the testing and, accordingly, in the design and/or structural adaptation of AI models/systems under development in the sandbox.	Technical expertise
Collaboration and dialogue between members of civil society, public authorities, and/or private regulated actors in conferences, workshops or other roundtable events[189]	None (but relevant for both DSA and AIA)	Individual researchers and members of civil society organisations/ NGOs (conceivably also journalists and fact-checkers, although less likely in academic settings)	Informal	**Enhanced public scrutiny:** members of public authorities seek additional information and insights over their area of regulation. Researchers and members of other civil society organisations seek to both gain new insights from their colleagues and members of public institutions about their research interests, but also to shape regulatory dialogue through the dissemination of their research findings.	Technical expertise (and, possibly, second-hand dissemination of lived expertise)
Innovation-fostering initiatives promoted by Commission and/or private sector[190]	None (but relevant for both DSA and AIA)	Research community	Informal	**Enhanced public scrutiny+ Technological participatory design:** have researchers contribute to regulatory dialogue with new ideas for how to design (i) technical solutions for the adaptation of AI models and systems to legal requirements; or (ii) ways for regulated actors to navigate compliance with legal requirements.	Technical expertise

189 Vergnolle (n 156) 18, 21; Marsh (n 40) 4. For concrete examples, see 'The DSA and Platform Regulation Conference 2024' (*DSA Observatory*, 11 December 2023) <https://dsa-observatory.eu/the-dsa-and-platform-regulation-conference-2024/> accessed 5 November 2024; Pielemeier and Sullivan (n 40); European Commission, 'Commission Gathers Good Practices to Combat Online Harm for Minors' (7 October 2024) <https://digital-strategy.ec.europa.eu/en/news/commission-gathers-good-practices-combat-online-harm-minors> accessed 18 December 2024; John Albert, 'DSA Risk Assessment Reports: A Guide to the First Rollout and What's next' (9 December 2024) <https://dsa-observatory.eu/2024/12/09/dsa-risk-assessment-reports-are-in-a-guide-to-the-first-rollout-and-whats-next/> accessed 13 December 2024.

190 Vergnolle (n 156) 18; See, e.g., 'Call for Participation to the Innovation Challenge "AI Act Compass: Navigating Requirements for High-Risk AI Systems"' (*Legality Attentive Data Scientists (LeADS)*, 1 August 2024) <https://www.legalityattentivedatascientists.eu/2024/08/01/innovation-challenge-call-for-participation/> accessed 5 November 2024; 'EU Boosts European AI Developers' (*European Commission*, 10 September 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4621> accessed 9 October 2024.

Publication of policy reports,[191] academic articles/books,[192] press releases[193]	None (but relevant for both DSA and AIA)	Civil society organisations or individual researchers	Informal	**Enhanced public scrutiny + explicit contestation:** contributing to or influencing the regulatory dialogue on the implementation of the DSA/AIA by providing new evidence or perspectives regarding emerging AI risks and how those are being/ should be assessed and mitigated. These publications can be highly persuasive and be considered or taken up as evidence by both public authorities (Commission[194] or national regulators) or by platforms.	Lived and technical expertise (depending on publication's content)
Online activism and journalistic work	None (but relevant for both DSA and AIA)	Interested/impacted individuals, NGOs and journalists	Informal	**Explicit contestation (with possible enhancement of public scrutiny:** contributing to or influencing the regulatory dialogue on the implementation of the DSA/AIA by providing new evidence or perspectives regarding emerging AI risks and/or potential non-compliance with risk management obligations. Whereas journalistic work will have less of a contestatory tone, activism posts will often entail explicit contestation and thus articulate competing visions of overlooked AI risks and/or non-compliance with the law. These publications can be used by supervisory or parliamentary authorities, thus broadening their informational resources.[195]	Lived and technical expertise (often not formulated in technical terms, but rather highlighting the lived impact of AI technologies and social media algorithms)

191 Meßmer and Degeling (n 40); Broughton Micova and Calef (n 119).

192 E.g., Claudio Novelli and others, 'How to Evaluate the Risks of Artificial Intelligence: A Proportionality-Based, Risk Model for the AI Act' (2023) <https://papers.ssrn.com/abstract=4464783> accessed 9 November 2023.

193 E.g., 'European Digital Rights and Others, An EU Artificial Intelligence Act for Fundamental Rights: A Civil Society Statement' (30 November 2021) <https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf>; Article 19 and others, 'Civil Society Open Letter to Commissioner Breton' (17 October 2023) <https://www.article19.org/wp-content/uploads/2023/10/Civil-society-open-letter-to-Commissioner-Breton.pdf>; Access Now, ARTICLE 19, and Electronic Frontier Foundation (EFF), 'Commissioner Breton: Stop Politicising the Digital Services Act' (*Access Now*, 19 August 2024) <https://www.accessnow.org/press-release/commissioner-breton-stop-politicising-the-digital-services-act/>.

194 Francesco Duina, 'Is Academic Research Useful to EU Officials? The Logic of Institutional Openness in the Commission' (2022) 29 Journal of European Public Policy 1493.

195 See e.g. Samira Rafaela, 'Parliamentary Question, The Practice of Shadow-Banning Content on Social Media Platforms, E-003111/2023' (European Parliament 2023) <https://www.europarl.europa.eu/doceo/document/E-9-2023-003111_EN.html> where a member of the European Parliament made a question to the Commission based on, amongst others, investigative journalistic work; Sydney Bauer, 'Elon Musk Has Made Anti-Trans Hatred One of Twitter's Core Features' (*The Nation*, 23 June 2023) <https://www.thenation.com/article/society/elon-musk-transphobia-twitter/>.

Complaints to national authorities or Commission	Arts. 53 and 86 DSA; art. 85 AIA for administrative complaints. Specifically for the DSA there are other ways of presenting complaints and flagging illegal content moderation practices through out-of-court dispute settlement procedure (art. 21 DSA) or submitting notices to platforms by way of trusted flagger status (art. 22 DSA)	Interested/impacted individuals or civil society organisations/NGOs representing them	Informal (even though it involves the leveraging of formal procedures, this is not seen formally in the law as a mode of public participation)	**Explicit contestation + Defence function:** offering a competing vision of how private regulated actors have identified or mitigated a potential AI systemic risk. Complaints can be a powerful source of information for regulators,[196] and may escalate all the way up to judicial litigation leading to the establishment of substantive standards on a certain regulatory matter.[197]	Lived and technical expertise
Strategic challenge of Commission's transparency policy regarding its enforcement actions[198]	Recital 13 and art. 8(1) and (3) of Regulation 1049/2001(relevant for both DSA and AIA)	Interested/impacted individuals, NGOs, researchers, and journalists	Informal (even though it involves the leveraging of formal procedures, this is not seen formally in the law as a mode of public participation)	**Explicit contestation + defence function:** to challenge the Commission's information policies and seek bigger transparency regarding how they monitor compliance with DSA and AIA risk management obligations. This often takes place in the form of a challenge to the European Ombudsman of a Commission's individual decision to deny access to information to a certain individual.	Technical expertise

196 Vergnolle (n 156) 21, 45–46.

197 For an example of such escalation in a field of EU digital regulation, i.e., the General Data Protection Regulation, see *Schrems I*, Court of Justice of the European Union, C-362/14, Judgment of the Court (Grand Chamber) of 6 October 2015, ECLI:EU:C:2015:650, paras. 26-36; *Schrems II*, Court of Justice of the European Union, Judgment of the Court (Grand Chamber) of 16 July 2020, ECLI:EU:C:2020:559, paras. 50-68; James Jacoby, 'The Facebook Dilemma - Interview with Max Schrems, a Privacy Advocate' (*FRONTLINE*, 2018) https://www.pbs.org/wgbh/frontline/interview/max-schrems/; Giovanni De Gregorio, 'The Rise of Digital Constitutionalism in the European Union' (2021) 19 International Journal of Constitutional Law 41, 54–55.

198 Curtin (n 167) 460, suggesting that an assertive approach challenging EU institutions' information policies may be viewed through a participatory lens.

Engaging in and/or supporting strategic litigation	None (but relevant for both DSA and AIA)	Affected individuals, communities and/or legal persons; NGOs representing or supporting them[199]	Informal (even though it involves the leveraging of formal procedures, this is not seen formally in the law as a mode of public participation)	**Explicit contestation + defence function:** offering a competing vision of how a private regulated actor have identified or mitigated a potential AI systemic risk; and seeking to obtain from courts the establishment of substantive standards that protect the litigant's interests (and those of individuals in a similar position). Strategic litigation may be done at the national level and escalate all the way up to the CJEU.[200]	Lived and technical expertise

84 The mapped loci of participation come in many shapes and sizes. To begin with, they empower different civil society actors and provide a space, in varying degrees, for the articulation of different types of expertise (lived and/or technical), as was already discussed in Section C.III. Furthermore, institutionally speaking, they might be more[201] (i) formal, (ii) informal, or (iii) regulatee-promoted. They will be:

- formal, if they are explicitly mentioned in law as modes of public participation in the implementation of these regulations. Drawing from Mendes, formal participation may be organic, if participating actors are included in the institutional structures where participation takes place; or procedural, if participants remain outside institutional structures and are determined based on the

199 In Germany, the NGO Gesellschaft für Freiheitsrechte (Society for Civil Rights, GFF) is already supporting individual actors in DSA strategic litigation at the national level Jürgen Bering Vezzoso Simonetta, 'Meta's Fundamental Rights Blunder - And a Happy German Antitrust Fix' (*Tech Policy Press*, 6 August 2024) <https://techpolicy.press/metas-fundamental-digital-rights-blunder-and-a-german-antitrust-fix> accessed 14 January 2025.

200 Alberto Alemanno, 'Beyond EU Law Heroes: Unleashing Strategic Litigation as a Form of Participation in the Union's Democratic Life' (2025) <https://shorturl.at/nw891> accessed 8 November 2024.

201 This is a taxonomy offering a heuristic model to interpret the different institutional setups of loci of participation. As with any other taxonomy, it has limits as it reduces the observed complexity in this field. It is, however, important to note that the distinction between formal, informal, and regulatee-promoted loci of participation is one of degree: the institutional structures of different loci of participation might present more or less features of each type. Therefore, the institutional type of each locus of participation indicated in Table 1 is the predominant one in how each locus is structured. I adopt the same taxonomical approach as Simon Halliday, 'After Hegemony: The Varieties of Legal Consciousness Research' (2019) 28 Social & Legal Studies 859, 861. He states: "The sketch of these [categories] should be interpreted lightly. I am not suggesting, for example, that there is no overlap or dialogue between them. Rather, they are presented in the manner of Weberian ideal types - 'exaggerated or one-sided depictions that emphasise particular aspects of what is obviously a richer and more complicated reality' (...). The sketch is thus intended merely as an analytical device, (...)".

subject-matter of the procedure or process where they intervene.[202] Participation in public consultations or calls for evidence launched by the Commission are examples of procedural participation, whereas the invitation of experts to be part of the AIA advisory forum or DSA Commission audits of VLOP/SEs constitute examples of organic participation;

- informal, if they are not explicitly mentioned in law as loci of civil society participation but may nevertheless be used to attempt to influence AI risk management processes – for example, online activism or the publication of policy reports. Informal loci of participation may also entail the leveraging of other public procedures or legal provisions not primarily designed to enable civil society participation. Examples of this are the presentation of complaints by interested individuals or organisations to regulators about potential non-compliance with risk management provisions,[203] or the use of access to information provisions by researchers to conduct their own audits of how platforms have (or have not) identified and mitigated emerging systemic AI risks;[204]

- regulatee-promoted, if participation occurs within an institutional framework set up by private regulated actors, e.g., the participation of researchers in red teaming exercises organised by platforms or other AI providers and deployers; or the cooperation between VLOP/SEs and fact-checking organisations in the context of mitigating systemic risks of AI-generated or algorithmically-spread disinformation.

85 At the same time, the mapped loci of participation pursue different underlying rationales. This is of great importance since, as explained by Kaminski and Malgieri, the theoretical explanations behind civil society participation "lead to calls for different kinds of interventions by civil society".[205] By that same token, the underlying rationale pursued, in theory, by a certain locus of participation will necessarily shape what civil society may achieve therein. Drawing from the work of Kaminski and Malgieri – who have sought to disentangle different theoretical explanations for stakeholder participation in AI governance[206] – and from other legal and political science literature on how third parties intervene in complex regulatory arrangements, I have developed a taxonomy of five rationales for civil society participation in the EU's AI risk governance framework[207]: (i) inclusiveness and legitimacy-building; (ii) technological participatory design; (iii) enhanced public scrutiny; (iv) explicit contestation; and (v) defence function. The following paragraphs describe each rationale in detail.

86 Firstly, when participation aims to promote inclusiveness and legitimacy-building, that means ensuring the representation of all relevant stakeholders in procedures of legal implementation. This rationale derives from theories of democratic representation.[208] From the perspective of the represented persons, participation is seen as a tool to make legal implementation processes less opaque, actively involve civil society actoirs, and thus reconcile the bureaucratic domination of public authorities over those processes with democratic values.[209] In this sense, participation does not mainly concern the substantive results of legal implementation processes (contrarily to the rationales below), but rather how inclusive and open those *processes* are.[210] However, democratic rationales of participation also allow for claims regarding the legitimacy and goodness of law-making and legal implementation. In particular, participation in the democratic sense may be used for legitimacy-building purposes, inasmuch as the involvement of civil society allows institutions to claim their own legitimacy, as well as the legitimacy and goodness of the output of the procedures where civil society actors were involved.[211]

202 For further elaboration on this distinction, which is beyond the scope of this paper, see Mendes (n 167) 30–31.

203 See, e.g., 'Commission Sends Request for Information to LinkedIn on Potentially Targeted Advertising Based on Sensitive Data under Digital Services Act' (14 March 2024) <https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-linkedin-potentially-targeted-advertising-based-sensitive-data> accessed 25 September 2024. Here, the Comission states that "This enforcement action is based on a complaint submitted to the Commission by civil society organisations".

204 See Section B.I.3.(c).

205 Kaminski and Malgieri (n 156) 22.

206 ibid 22–42.

207 The same considerations made in footnote 201 apply to this taxonomy as well. Furthermore, this taxonomy constitutes a tentative exercise that is expected to evolve with an empirical inquiry of the purposes of civil society participation in the DSA and AIA's risk management frameworks.

208 Curtin (n 167) 455–457; Kaminski and Malgieri (n 156) 22–25.

209 Curtin (n 167) 445–446, 461; Gloria Golmohammadi, 'Realizing the Principle of Participatory Democracy in the EU: The Role of Law-Making Consultation' (Stockholm University 2023) 88–89 <http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-220289> accessed 21 November 2023.

210 See, to this effect, Kaminski and Malgieri (n 156) 22–24.

211 Mendes (n 167) 91, 94, 126, 129; Danai Petropoulou Ionescu, 'Habemus Legitimacy? The European Commission Opens Public Consultation for a Guidance Document' (2021) 12 European Journal of Risk Regulation 861.

87 The second identified rationale is technological participatory design. In this case, civil society participation is part of a distinct methodological approach to computational design.[212] It does not aim to ensure stakeholder representation (contrary to the inclusiveness and legitimacy-building rationale), nor to assess and potentially contest choices that regulatees have already made. Differently, it aims to integrate stakeholder interests into technological design. Importantly, it does not seek to address and represent all civil society perspectives, but only those that may be integrated into technological design in a resource-efficient way.[213]

88 Thirdly, civil society participation may serve to enhance public scrutiny over regulated actors, thus adding to public regulatory capacity. Civil society actors may do so in two, distinct ways: they may facilitate the exercise of public authorities' functions; or, alternatively, act as surrogate regulators. Starting with the former case, civil society participation may be a source of new factual and/or technical information for administrative authorities, thereby facilitating the exercise of their supervisory and decisional functions on any given regulatory area.[214] In addition, civil society actors may also act as surrogate regulators, providing an added level of scrutiny over both (i) regulated actors about how they comply with the law and (ii) public authorities for how they enforce it. This function of civil society participation is highlighted by theories of tripartism. According to them, public accountability is not ensured through a top-down relationship between States and regulated actors but, instead, in a tripartite scheme where civil society participates in regulatory enforcement next to the State and regulated actors.[215] In general, enhanced public scrutiny may take a lot of forms, such as collaboration and dialogue with public authorities and regulated actors, research (potentially disseminated), and assessment.[216]

89 Fourthly, civil society participation may serve a defence function. In this sense, the intervention of persons in administrative procedures is aimed at allowing them to defend their subjective rights or legally relevant interests potentially affected by administrative decisions. In this way, participation enables administrative authorities to account for the interests of persons potentially affected by administrative action, serving as an ex-ante complement to judicial review.[217]

90 Finally, as a fifth rationale for civil society participation, civil society actors may intend to *explicitly* contest how a specific piece of law is being implemented and, relatedly, challenge and politicise the dominant regulatory arrangements of each given time, often portrayed as a form of technical or apolitical consensus between divergent interests.[218] Contestation is here defined as the use of a locus of participation by civil society actors to articulate competing visions[219] of (i) what are AI systemic risks, (ii) what concrete risks emerge over time; and (iii) alternatives ways of assessing and mitigating those risks. In this sense, contestation is not just concerned with articulating the systemic impacts of platforms' AI systems. It also contains an ambition to change the risk management choices made by private actors and overseen by public authorities. In this sense, contestation may have several (potentially simultaneous) objects. This is to say, that it may seek to challenge (i) concrete compliance decisions made by public authorities or private regulated actors through administrative or judicial means;[220] (ii) general institutional policies that impact regulatory enforcement by public authorities or compliance by private actors;[221] or even the regulatory agenda, meaning the regulatory issues that gain the attention of the members of the public and government officials, thereby becoming priorities in the policy and enforcement debate.[222]

212 Kaminski and Malgieri (n 156) 32–34; Ned Cooper and Alexandra Zafiroglu, 'From Fitting Participation to Forging Relationships: The Art of Participatory ML', *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Association for Computing Machinery 2024) <https://dl.acm.org/doi/10.1145/3613904.3642775> accessed 30 January 2025.

213 Kaminski and Malgieri (n 156) 32–34.

214 Curtin (n 167) 459; Mendes (n 167) 32.

215 Ian Ayres and John Braithwaite, 'Tripartism: Regulatory Capture and Empowerment' (1991) 16 Law & Social Inquiry 435, 439, 441–445; Darren Sinclair and Neil Gunningham, 'Smart Regulation' [2017] Regulatory theory: Foundations and applications 133, 133.

216 Sinclair and Gunningham (n 215) 135–138.

217 Mendes (n 167) 33.

218 Curtin (n 167) 467; Chantal Mouffe, *The Democratic Paradox* (Verso 2000); Eugen Octav Popa, Vincent Blok and Renate Wesselink, 'An Agonistic Approach to Technological Conflict' (2021) 34 Philosophy & Technology 717; Daniel E Walters, 'The Administrative Agon: A Democratic Theory for a Conflictual Regulatory State' (2022) 132 Yale Law Journal 1, especially 48-57.

219 Competing visions are here defined as those counter-hegemonic approaches to how a particular regulatory arrangement is shaped at any given time. See Paulina Tambakaki, 'The Tasks of Agonism and Agonism to the Task: Introducing "Chantal Mouffe: Agonism and the Politics of Passion"' (2014) 20 Parallax 1, 7–10.

220 See, in Table 1, the possibility to lodge administrative complaints with national supervisory authorities or the Commission, as well as strategic litigation.

221 Curtin (n 167) 460; Walters (n 218) 56.

222 Contestation by civil society in this last case is aimed at 'agenda-setting', see Thomas A Birkland, 'Agenda Setting in Public Policy' in Frank Fischer and Gerald Miller (eds), *Handbook of public policy analysis: theory, politics, and methods*

91 A few final remarks are needed to fully explain how contestation as a rationale for civil society participation may be present in the DSA and AIA. Specifically, I argue that contestation-driven civil society participation may prove particularly crucial in the context of AI systemic risk management. If, as seen in Sections 2. and C.I., the definition and mitigation of AI systemic risks are open to different interpretations, and if regulated actors will concretise them in time, then their determinations of what AI systemic risks are and how they should be managed are contingent. And, if they are contingent, they are also open to contestation and concomitant change.[223] In this sense, contingency and contestation of regulatory arrangements are intimately tied: in Mouffe's words, a definitive and depoliticized rational consensus around a certain regulatory arrangement cannot exist. Instead, consensus will always exist as a temporary result of a provisional hegemony that stabilises power and social relations in a particular way. This is done necessarily to the exclusion of some, who may choose to contest such temporary regulatory arrangements in order to change them.[224]

92 Applying this to the DSA and AIA, if the two regulations explicitly count on civil society actors to enhance public scrutiny in this field and help contextualise risk assessment and mitigation, then contestation of risk management choices is a possibility for them. Therefore, the different loci of participation mapped in Table 1 may be theoretically framed as spaces of contestation,[225] albeit in varying degrees. Some loci are specifically geared towards *explicit* contestation by civil society, in that they allow or intend individuals and organisations to explicitly articulate their concerns about (and alternative proposals for) AI systemic risk management. Those loci are the ones identified in Table 1 as predominantly pursuing a contestatory rationale. This is the case of, for example, adversarial audits of VLOP/SEs' risk management reports based on vetted researcher access to information under the DSA: contestation is expected in this locus of participation and, therefore, it is practised explicitly.

93 Regulatory scrutiny through explicit contestation by civil society is, however, not the predominant rationale of all mapped loci of participation. In fact, it is not certain for numerous loci whether there will be a possibility for explicit contestation, as can be seen in Table 1. But in all loci, there is, I argue, space for implied contestation to occur.[226] This would be the case if civil society intervenes in a locus of participation not primarily designed to allow for explicit contestation but, nonetheless, the specific form of such an intervention either (i) implicitly builds upon a competing vision of risk management or (ii) engages in contestation despite the main rationale and expected form of participation of that locus. In simpler words, contestation is implied if it is not expected in a locus of participation but nonetheless practiced. This would be the case if, for example, during the collaborative development of an AIA code of conduct, intervening researchers or civil society organisations use their presence to propose alternatives to risk assessment or mitigation solutions advocated by regulated actors or the Commission. There would equally be implied contestation if, in an AI regulatory sandbox or innovation-fostering initiative set up by the Commission, intervening civil society would propose solutions of AI and/or platform design that build upon underrepresented gained knowledge of the concerns, perspectives, and lived experiences of individuals and communities regarding platforms' AI systems.

E. Conclusion: AI systemic risk will be what we want it to

94 Exegesis of legal texts through the canons learned in the continental legal tradition can only take us so far. It is increasingly common in legislation to see certain key concepts being so broadly defined that they may encompass many different, often conflicting meanings. Choosing one of those meanings from a set of possibilities is a value-laden choice. One can opt to use legal interpretation techniques to settle on one meaning for a certain broad legal concept, and then fictionalise that that was that concept's innate meaning all along. That is the way of legal practice and how, after all, most legal researchers in Europe learned to reason in law school. An alternative option would be to accept that certain vague legal concepts do not have such an innate meaning and, on the contrary, will be shaped by regulatory practice and dialogue. I must confess (as unorthodox as this candidness might be) that, when I started researching how EU law regulates digital platforms' AI systems, I still very much had in mind the traditional way of continental legal thought. However, after understanding that the EU opted for a risk-based regulatory approach and while seeking to answer the main research question guiding this paper - how do the DSA and AIA foresee creating an effective risk regulatory regime applicable to the AI

(1st edition, Routledge 2017) 63–65.

223 Mouffe (n 218) 97–98, 100, 104; Crawford (n 3) 82–83.

224 Mouffe (n 218) 104, 113, 126. In p. 126, Mouffe posits that contestation could be achieved through the promotion of civil society associations.

225 To clarify, this theoretical framing constitutes the formulation of a hypothesis regarding the nature of civil society interventions in EU AI risk management which, necessarily, begs empirical questioning.

226 The same remarks of the above footnote apply here.

systems of digital platforms? – I have quite clearly encountered the limits of that continental approach. And all due to the concept of 'AI systemic risk'.

95 As shown in Section B., the EU's risk regulation of platforms' AI systems revolves around the concept of systemic risk, primarily through the DSA systemic risk management scheme, which is complemented by numerous relevant AIA provisions. Despite several indications of the two regulations, AI systemic risks are not fully defined in the law. As is typical of risk-based approaches, that conceptual determination will be iteratively achieved by the concrete compounded outcomes of successive concrete risk management processes. Simply put, what is considered an AI systemic risk in each instance of AI risk management will eventually flesh out the meaning of this concept. Similarly, the strategies most commonly adopted to manage identified risks will be considered best practices of AI systemic risk mitigation. Most importantly, these will all be contingent choices, which may change.

96 Acknowledging the contingency of AI systemic risk definition and mitigation should inform both the regulatory implementation and research agenda of this EU's AI risk management framework. Specifically, there are three concrete implications of this acknowledgement which may turn into possible trajectories of future regulatory and scholarly dialogue.

97 First, significant conceptual focus should be put on the *who* - and not just the *what* - of AI systemic risk management. There is, of course, space for attempts to conceptualise the meaning of AI systemic risks and find adequate indicators and measures for such determination. But, in light of all the above, there must be significant empirical inquiry into how the meaning of 'AI systemic risk' is constructed in EU law. Namely, this means empirically questioning which actors have more agency in the field of AI systemic risk management, who influences systemic risk management choices the most, and whose ideas of what are AI systemic risks gain more currency in the developing regulatory dialogue.[227] This is especially true for the early stages of implementation of the DSA and AIA, where the meaning of this concept is still particularly undefined and is thus more malleable. In this sense, both enforcers and researchers should pay special attention to (i) the risk management methodologies used by different actors; (ii) the priorities and interests of those setting the regulatory agenda and thus focusing on certain types of systemic risks as opposed to others;[228] (iii) and the frames and models used to represent and capture the impact of platforms' AI systems in early regulatory dialogue.

98 Second, if systemic risk management is process-based, one should turn to the law for guidance on how those processes *should* go. By distilling from the law its normative aspirations for risk management processes, one gains not only an important benchmark for their internal assessment and critique but also a transparent enunciation of legal ambitions that can then be critiqued from external, non-legal viewpoints. That is what Section C. sought to accomplish. It identified three common normative aspirations cutting across the DSA and AIA risk management provisions.[229] The DSA and AIA frame the risks of platform-related AI systems as 'systemic'. They do so in socio-technical terms, by requiring that risk assessment and mitigation not be focused just on the technical traits of those AI systems as technological artifacts that cause isolated instances of harm; but rather on the more structural and collective impact that AI systems may have in their interactions with societal systems (C.I.). Consequently, risk management should be concretised through methodologies that socially contextualise the risks of platforms' AI systems and thus take risk perceptions by individuals and communities as a measure for their identification and subsequent management (C.II.). Institutionally speaking this requires that risk governance be participated and, specifically, the DSA and the AIA count with civil society involvement as a conduit for contextualising risk management and enhancing the scrutiny over platforms' risk management choices (C.III.). This also entails that if the perspectives of civil society on risk assessment and mitigation do not align with those of private regulated actors and platforms, civil society actors should have space to contest how AI systemic risks are assessed and mitigated in light of their technical and lived expertise.

99 Third and finally, if AI systemic risk management is to be contested and participated, then a fruitful focus of research and regulatory action is to map and consolidate an understanding of how such contestation and participation in AI systemic risk governance may occur. Section D. aimed to take a first step in this direction by looking at the law and mapping all existing and very different possibilities for civil society participation and involvement in the EU's AI risk management framework. Then, it more specifically identified and disaggregated the

227 This empirical objective is framed in Bordeusian terms, see Yves Dezalay and Mikael Rask Madsen, 'The Force of Law and Lawyers: Pierre Bourdieu and the Reflexive Sociology of Law' (2012) 8 Annual review of law and social science 433.

228 Similarly see Griffin, 'What Do We Talk about When We Talk about Risk?' (n 15).

229 These are by no means the only ones, and future research could uncover more.

rationales of the identified loci of participation. Crucially, however, this was a theoretical exercise based on a reading of the existing law and civil society practice. It is, therefore, a 'best-case scenario' mapping of all the possible cracks in the law that different civil society actors can exploit to influence the legal implementation of platforms' AI risk management. Only a very optimistic person would expect all these loci to allow, in practice, for meaningful civil society interventions. Whether these can, in fact, become meaningful depends much more on practice. And there are many reasons why civil society participation could go wrong. Civil society actors could just be performatively involved in risk management processes, thereby legitimising private actors' risk management choices without having much ability to influence these outcomes.[230] Furthermore, different civil society actors have starkly disparate material and technical resources, available information, and access to participation fora, which may lead to a limitation of the types of concerns and proposals raised through civil society participation.[231] Finally, there is a possibility that the lived experiences of impacted individuals and communities are either not sufficiently represented by participating organisations or considered by private and public actors responsible for AI systemic risk management.[232]

100 All these open questions will eventually dictate how the meaning of AI systemic risks will be shaped in EU law. Above all, they beg a broad empirical research agenda, one that involves scholars of different perspectives in the task of scrutinising how AI systemic risks are identified and managed in EU law. Such a research agenda should both evolve and inform policymaking and regulatory implementation in this field. Scholarly and regulatory dialogue should be mindful of this: the EU legislator gave the concept of AI systemic risk enough latitude for it to be many things. Its definition and corresponding management are not purely technical matters; rather, they require legal, political and even ethical[233] choices to be made. These choices should not be the exclusive purview of those with more informational capacity and technological understanding of AI systems. In that sense, AI systemic risks can be what we, as a society, want to. Whether we will be given the space to articulate our concerns, perspectives and experiences and thereby shape risk management will dictate, to a large extent, the future of platform and AI regulation in EU law.

230 Michele Gilman, 'Beyond Window Dressing: Public Participation for Marginalized Communities in the Datafied Society' (2022) 91 Fordham Law Review 503, 529–532; Kaminski and Malgieri (n 156) 39, 50.

231 Griffin, 'Rethinking Rights in Social Media Governance' (n 108) 71–73; Marsh (n 40) 13–14; Karolina Iwánska and others, 'Towards an AI Act That Serves People and Society: Strategic Actions for Civil Society and Funders on the Enforcement of the EU AI Act' (European Center for Not-for-Profit Law 2024) 51–53 <https://europeanaifund.org/wp-content/uploads/2024/09/240827_FINAL_AI_ACT_Enforcement.pdf> accessed 25 September 2024. General reports on effective civil society participation highlighted the need to ensure independent public funding and adequate staff training of civil society organisations, see e.g. Vanja Skoric, 'Standards and Good Practices for Public Funding of Civil Society Organisations' (European Center for Not-for-Profit Law Stichting 2020) 14–15, 60–63 <https://ecnl.org/sites/default/files/2020-09/TUSEV%20Public%20Funding%20Report_Final.pdf?utm_source=chatgpt.com> accessed 29 January 2025.

232 Gilman (n 230) 529; Kaminski and Malgieri (n 156) 16.

233 Mittelstadt and others (n 3); 'Ethics Guidelines for Trustworthy AI' (Independent High-Level Expert Group On Artificial Intelligence - European Commission 2018) 9–13.