Design patterns and systemic risks

Pollicino AIdvisory

1. Introduction

Two recent decisions, one in the United States and the other in the European Union, respectively, on addiction to social media and on generated images and deepfakes, indicate a decisive shift in how digital harms are conceptualised and how systemic risks with these technologies are governed.

In March 2026, a Los Angeles jury found Meta and Google (YouTube) liable for harm caused to a minor, linking that harm to the addictive design of their platforms, including infinite scroll, autoplay, and engagement-based recommendation systems. Crucially, the case did not turn on unlawful content, but on product architecture, allowing plaintiffs to circumvent the traditional liability shield under Section 230.

At the same time, in the EU, the Commission launched a new formal investigation against X under the Digital Services Act (DSA), concerning Grok, extending its ongoing investigation launched in 2023 into X's compliance. Moreover, for the first time, systemic risk is being operationalised in relation to generative AI integrated within platform environments, raising concerns not only about outputs but about how such systems function, scale, and interact with users.

This policy brief argues that *systemic risk*, understood as harm emerging from the design and large-scale operation of digital systems, provides the key to interpreting this transition. While the Digital Services Act operationalises systemic risk as a trigger for intervention on platform architecture, Art. 9 AI Act remains grounded in a system-centric and procedural model of risk management. The brief highlights this conceptual misalignment and proposes a systemic interpretation of the risk management system under Art. 9 to ensure effective governance of AI systems embedded in complex digital environments.

2. Systemic risk

In recent years, we all became more and more familiar with the notion of risk and with that of 'risk-based approach', starting from the GDPR (De Gregorio-Dunn, 2022). This recurrent topic in digital regulation is established in different nuances, along with different regulatory instruments, such as the DSA and the AI Act. Specifically, the notion of systemic risk, as it emerges in digital regulation, cannot

Pollicino AIdvisory
Via Visconti di Modrone 8
20122, Milano, Italy
info@pollicinoaidvisory.eu

be reduced to a generic reference to large-scale harm. Its meaning is more precise and carries specific regulatory consequences.
In its original formulation in financial law (European Central Bank, 2009), systemic risk refers to the possibility that a disruption, whether triggered exogenously or generated endogenously, affects not just individual actors but the functioning of the system as such, producing cascading failures, market dysfunctions, or regime shifts. What defines systemic risk is therefore not the gravity of a single event, but its capacity to propagate through interdependencies and to alter the equilibrium of the system. When transposed to the digital environment, this notion undergoes a crucial transformation.

First, systemic risk is no longer tied to institutional interdependence (as in financial markets), but to architectural and behavioural interdependence. Digital systems generate risk through the interaction between design choices, algorithmic processes, and user behaviour.

Second, propagation does not occur only across actors, but across layers of the digital ecosystem: from models to platforms, from interfaces to users, and across different deployment contexts. This is reflected in the AI Act's reference to risks that "propagate at scale across the value chain" (Art. 3, n. 65), AI Act).

Third, and most importantly, systemic risk in the digital domain is produced by design. Moreover, in the context of the DSA, four specific areas of systemic risk are considered, specifically for the VLOPs and VLOSEs (Kaesling and Wolf, 2025):

- the dissemination of illegal content through the services of the
- any actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights to human dignity enshrined in Art. 1 of the Charter, to respect for private and family life (Art. 7 of the Charter), to the protection of personal data (Art. 8 of the Charter), to freedom of expression and information, including the freedom and pluralism of the media, (Art. 11 of the Charter), to non-discrimination (Art. 21 of the Charter), to respect for the rights of the child (Art. 24 of the Charter) and to a high-level of consumer protection (Art. 38 of the Charter);
- any actual or foreseeable negative effects on civic discourse and electoral processes, and public security;
- any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors, and serious negative consequences to the person's physical and mental well-being.

Thus, it is not merely an externality or a failure, but often the by-product of optimisation logics, such as engagement maximisation, that are embedded in the system itself. This leads to a more precise definition: systemic risk in digital systems is the risk that arises from the design and operation of socio-technical

infrastructures, which, through scale and interaction, generates cumulative and propagating effects on fundamental rights and societal processes.
Under this lens, both the US Meta/Google case and the Commission's action on Grok can be read as instances where the law identifies harm not in isolated outputs, but in the systemic effects of design choices operating at scale.

3. From theory to practice

The tension between systemic risk and traditional risk management becomes particularly visible when comparing Article 34 DSA with Article 9 AI Act, respectively, on systemic risk and risk management system. At first sight, both provisions appear to rely on a similar architecture: they require the identification, assessment, and mitigation of risks. However, they operate on fundamentally different assumptions regarding the nature of risk and the object of regulation.

Article 34 DSA is built around a systemic conception of risk. The risks to be assessed are not limited to the functioning of a specific technical system, but extend to the overall operation of the platform, including its design, recommender systems, and interaction with users. The provision explicitly targets risks that affect fundamental rights, public discourse, and societal processes, and that emerge through scale, amplification, and behavioural dynamics. As a consequence, risk assessment under Article 34 is inherently open-ended and context-dependent. It requires platforms to consider how their services operate within a broader socio-technical environment and how design choices may generate cumulative effects over time. This is why, in practice, it enables and increasingly justifies intervention on platform architecture, as seen in recent Commission enforcement against X.

Article 9 AI Act, by contrast, reflects a contained and system-centric model of risk. The provision focuses on risks to safety, health, and fundamental rights associated with a given AI system and requires providers to implement a structured risk management process throughout its lifecycle. While comprehensive, this approach is not fully context dependent since it is, in principle, an analysis conducted by the provider, and not by the deployer, who will actually need to assess the risks related to the use of the system (Art. 27, FRIA, AI Act).

This difference is not merely technical, but conceptual: Art. 34 captures risk as produced through design and propagated through use; Art. 9 treats risk as contained within the system.

Hence, while the DSA is capable of addressing risks that emerge from design and deployment at scale, Article 9 risks remaining confined to a model of technical risk control, which might not be fully equipped to capture systemic effects, if not well structured. This becomes particularly problematic in contexts where AI systems are

embedded within platforms, and where their impact is inseparable from recommender systems, interface design, and user behaviour.

The recent US litigation on platforms' addiction reinforces this point from a different angle. By attributing liability to platform design, courts are effectively recognising that risk cannot be reduced to the internal properties of a system, but must be understood in terms of its systemic effects.

4. Lessons for the AI Act

If systemic risk is taken seriously, as it is under the DSA and increasingly in practice, then the risk management system under Article 9 must be reconstructed in light of a systemic understanding of risk.

This implies, at a minimum, that:

- risk identification cannot be limited to intended use, but must include deployment contexts and behavioural effects;
- mitigation cannot remain procedural, but must extend to design and interaction choices;
- responsibility cannot be confined to providers, but must reflect distributed roles across the value chain.

This latter one, in particular, seems to be also the approach with respect to other impact assessment: as a matter of fact, the recently (26 March 2026) approved position of the European Parliament on the Digital Omnibus on AI is proposing a cross-referencing method between the FRIA and the DPIA (Amendment §9b). It is desirable that the same approach will be discussed along with other impact assessment methodologies, with similar goals, such as Art. 9 AI Act and Art. 34 DSA. The current EU framework recognises systemic risk, but does not yet govern it consistently (King and Portante D'Alessandro, 2026). As this policy brief showcased, while the DSA targets risks at the level of system design, Art. 9 AI Act continues to address them as internal, manageable properties of individual systems.

Without such an interpretation, a gap emerges: systemic risk is recognised at the level of platforms and general-purpose AI, but not effectively governed within the core operational provision of the AI Act.