Review scientific paper DOI: 10.56461/iup_rlrc.2026.7.ch16

Fernanda FLORENTINO FERNANDEZ JANKOV*

PLATFORM GOVERNANCE AND THE DUTY TO ACT RESPONSIBLY WITHIN SYSTEMS-BASED REGULATION

The regulation of digital platforms is undergoing a significant transformation. Traditional regulatory models relied primarily on intermediary liability rules and reactive enforcement mechanisms, focusing on the removal of unlawful content after notification. More recent legislative frameworks, however, increasingly adopt systems-based approaches that require platforms to identify and manage systemic risks generated within their communication environments. This article offers a comparative analysis of three influential regulatory models: the United States' intermediary immunity regime, the European Union's Digital Services Act, and Canada's proposed Online Harms Act. While these frameworks differ significantly in structure and regulatory ambition, they collectively illustrate a broader shift in platform governance—from ex post liability toward proactive risk management and structured internal decision-making.

The article argues that this transformation reshapes the institutional role of digital platforms. Rather than functioning solely as intermediaries responding to unlawful content, platforms are increasingly required to interpret regulatory standards, assess systemic risks, and implement mitigation measures within their own governance systems. As a result, regulatory scrutiny increasingly focuses not only on individual moderation decisions but also on the adequacy of the internal structures through which platforms observe, assess, and mitigate risks. Understanding this emerging regulatory architecture is therefore essential for evaluating accountability and the protection of fundamental rights in the evolving governance of digital communication systems.

Keywords: platform governance, intermediary liability, Digital Services Act, algorithmic governance, risk-based regulation.

1. INTRODUCTION

The governance of harmful online content has undergone a significant transformation over the past decade. What began as a debate centred on intermediary liability and voluntary content moderation has gradually evolved into a broader reconsideration of the regulatory

* PhD, TEP (Trust and Estate Practitioner, STEP Switzerland), is a legal scholar affiliated with the Faculty of Law of the University of São Paulo (USP) and an attorney licensed to practice law in Brazil and Portugal, ORCID: https://orcid.org/0009-0007-9737-4293, email: *fernanda.jankov@usp.br*

responsibilities of digital platforms. Early regulatory approaches focused primarily on reactive mechanisms—such as notice-and-takedown procedures or the *post hoc* removal of unlawful content. Contemporary regulatory frameworks, however, increasingly impose proactive and systemic obligations on major online services, requiring them to anticipate and mitigate risks associated with the dissemination of harmful material.

In the United States, the regulatory landscape remains anchored in Section 230 of the Communications Decency Act (1996) and the strong constitutional protection afforded to speech under the First Amendment of the U.S. Constitution. This model preserves a relatively clear institutional distinction between public adjudication and private moderation. Platforms retain broad discretion to manage user-generated content through their own community standards, while courts remain the primary institutions responsible for applying and enforcing legal norms governing speech.

By contrast, the European Union has developed a more structured regulatory approach to digital platform governance. The Digital Services Act (2022) introduces layered due diligence obligations for online intermediaries, including systemic risk assessments and mitigation duties applicable to very large online platforms. Although public authorities retain supervisory powers through national Digital Services Coordinators (Digital Services Act, 2022. Arts. 49–51) and the European Commission (Digital Services Act, 2022. Arts. 56–60), the regulatory architecture increasingly requires platforms to internalise compliance and risk-management mechanisms within their organizational and technical infrastructures.

More recently, Canada's proposed Online Harms Act (Bill C-63), introduced in 2024 but not enacted prior to parliamentary dissolution, advanced a systems-based regulatory model centred on a statutory "duty to act responsibly"[1]. The proposed framework would have required regulated services to assess, mitigate, and prevent the circulation of harmful content through structured internal governance mechanisms extending beyond traditional notice-and-removal practices. Even in its unenacted form, the proposal illustrates an emerging legislative trend toward embedding public policy objectives directly within platform operations.

These developments reflect what Balkin (2018. p. 1149) has described as the rise of "algorithmic governance", in which digital infrastructures increasingly shape the conditions of public discourse. Regulation no longer operates solely as an external constraint imposed by the state upon private actors. Instead, contemporary legislative frameworks increasingly require platforms to integrate risk assessment, norm interpretation, and enforcement processes into their internal governance architectures.

From a broader theoretical perspective, this regulatory evolution can also be understood through the lens of sociological theories of risk governance. In Niklas Luhmann's social systems theory (Luhmann, 2005), modern societies increasingly attribute potential harms not merely to external dangers but to decisions embedded within institutional structures operating under conditions of complexity. Regulatory frameworks that require platforms to assess and mitigate systemic risks therefore reflect a wider transformation in the management of uncertainty: responsibility becomes progressively linked to the design and operation of decision-making infrastructures rather than solely to the *ex post* adjudication of unlawful acts.

This article examines whether such regulatory developments represent incremental refinements of intermediary liability regimes or a more substantive transformation in the

[1] Requiring operators of regulated services to implement measures to mitigate risks of exposure to harmful content.

allocation of regulatory functions. When platforms are required to identify risks, interpret statutory categories of harm, impose restrictions, and operate internal complaint mechanisms, they perform functions that bear structural similarities to processes traditionally associated with the implementation of legal norms. The purpose of this study is not to suggest a displacement of public authority, but rather to analyse how contemporary regulatory design reshapes the operational dynamics through which digital governance is exercised.

Through a comparative analysis of the United States, the European Union, and Canada, this paper explores how different jurisdictions conceptualise the relationship between freedom of expression, systemic accountability, and platform responsibility. By situating the Canadian proposal alongside established American and European regulatory models, the study seeks to clarify how systems-based frameworks reconfigure the practical implementation of public norms within digital constitutional democracies.

To frame this inquiry more precisely, this article advances the hypothesis that contemporary systems-based platform regulation represents more than a refinement of traditional intermediary liability regimes. Rather, it constitutes a structural reallocation of regulatory functions, whereby private platforms are increasingly required to internalise public governance responsibilities through risk assessment, mitigation duties, and institutionalised internal decision-making processes. The comparative analysis developed in this study examines how this transformation manifests differently across the United States, the European Union, and Canada.

At the same time, when regulatory frameworks require platforms to interpret statutory categories of harm, assess systemic risks, and implement mitigation measures within their internal systems, the quality of the decision-making processes through which those obligations are operationalised becomes a matter of normative significance. Questions concerning coherence, transparency, and accountability therefore emerge as central concerns. In this context, examining the governance structures through which platforms observe, evaluate, and respond to systemic risks becomes essential for understanding how contemporary regulatory models seek to balance platform responsibility, freedom of expression, and democratic oversight in the evolving architecture of digital governance.

2. MODELS OF PLATFORM GOVERNANCE IN CONTEMPORARY REGULATION

2.1. The American Model: Immunity, Editorial Discretion and Institutional Separation

The regulatory framework governing online platforms in the United States is built upon a combination of statutory intermediary immunity under Section 230 of the Communications Decency Act (CDA) and the strong constitutional protection of speech under the First Amendment. In institutional terms, this arrangement sustains a relatively clear separation between the public adjudication of legal norms by courts and the private moderation practices carried out by digital platforms.

Section 230(c)(1) provides that no provider or user of an interactive computer service shall be treated as the publisher or speaker of information provided by another content provider (Communications Decency Act, 1996, § 230(c)(1)). In the United States, where judicial precedent plays a central role in shaping the interpretation of statutory frameworks, courts have consistently construed this provision broadly, shielding platforms from liability arising from third-party content. The seminal decision in *Zeran v. America Online, Inc.* established that Section 230 bars claims that would treat an intermediary as the publisher of user-generated material (*Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997)). Subsequent case law has reinforced this expansive interpretation, extending immunity to a wide range of civil claims, including negligence and failure-to-remove allegations (see, e.g., *Blumenthal v. Drudge*, 992 F. Supp. 44 (D.D.C. 1998); *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119 (9th Cir. 2003); *Fair Housing Council of San Fernando Valley v. Roommates.com*, LLC, 521 F.3d 1157 (9th Cir. 2008) (en banc); *Jones v. Dirty World Entertainment Recordings LLC*, 755 F.3d 398 (6th Cir. 2014); *Force v. Facebook, Inc.*, 934 F.3d 53 (2d Cir. 2019)). The rationale underlying this interpretation has been the preservation of an open and innovative digital environment, free from excessive litigation burdens.

At the same time, Section 230(c)(2) allows platforms to engage in voluntary content moderation in good faith. This combination of immunity and discretionary moderation authority has shaped what is often described as a "market self-regulation" model.[2] Platforms retain broad autonomy to define community standards and to remove or restrict content according to private policies, while courts remain the primary institutions authorised to determine the legality of speech under constitutional and statutory standards.

Recent litigation has tested the contours of this arrangement. In *Moody v. NetChoice, LLC*, the United States Supreme Court addressed state-level attempts to regulate platform moderation practices (*Moody v. NetChoice, LLC*, 603 U.S. (2024)). Although the decision did not fundamentally alter Section 230 immunity, it underscored the constitutional sensitivity surrounding compelled hosting, editorial discretion, and the role of private platforms in structuring public discourse. As the Court observed, "the First Amendment protects the right of a private speaker to exercise editorial control over the speech it disseminates" (*Moody v. NetChoice*, LLC, 603 U.S. (2024) (slip op.)). The case illustrates the ongoing tension between legislative efforts to impose obligations on platforms and the constitutional commitment to freedom of expression.[3]

Scholarly analysis has increasingly described this environment as one of algorithmic governance—or, in Balkin's formulation, the emergence of an "algorithmic society" in which digital infrastructures shape the conditions of speech through design, ranking, and moderation practices (Balkin, 2018, pp. 1149–1210; Klonick, 2018, pp. 1598–1670). Nevertheless, under the American model, the authority to apply binding legal norms remains institutionally anchored in courts.[4] Platforms may structure speech environments and exercise significant practical

---

2 For influential analyses describing the emergence of private governance of online speech, see Balkin, 2018, pp. 1149–1210; Klonick, 2018, pp. 1598–1670.

3 The central role of judicial precedent in shaping the interpretation of statutory and constitutional norms is a defining feature of the American common law system. In the context of intermediary liability and platform governance, courts have played a particularly significant role in construing the scope of Section 230 and the constitutional protections applicable to private moderation practices. For scholars and practitioners trained in civil law traditions, the operative contours of the regulatory framework therefore emerge not only from statutory provisions but also from the cumulative development of case law.

4 In the United States, the interpretation and application of statutory and constitutional norms governing online speech have largely developed through judicial decisions. Courts have played a central role in defining the scope of intermediary immunity under Section 230 of the Communications Decency Act and

influence over the visibility and distribution of speech, but they are not formally charged with the proactive implementation of statutory duties to assess systemic risks or prevent harm prior to circulation. Their role remains framed primarily as an exercise of private editorial discretion rather than as a statutory obligation to operationalise public norms. This institutional configuration preserves a clearer conceptual boundary between adjudication by public authorities and moderation by private actors and stands in contrast to emerging European regulatory frameworks that increasingly assign platforms ex ante responsibilities for assessing and mitigating systemic risks associated with online communication.[5]

2.2. The European Union: Systemic Risk with Public Oversight

In contrast to the American model, the European Union has progressively developed a more structured regulatory approach to digital platform governance. Earlier frameworks, most notably the E-Commerce Directive (2000), relied primarily on conditional liability exemptions for intermediary service providers combined with notice-and-takedown mechanisms for the removal of unlawful content. This framework established the foundational "safe harbour" regime for hosting services while prohibiting general monitoring obligations (E-Commerce Directive, 2000). Recent legislative developments, however, reflect a shift toward systemic accountability.

The Digital Services Act (2022) represents the most comprehensive articulation of this model. Rather than merely clarifying intermediary liability, the DSA introduces a system of graduated due diligence obligations that vary according to the nature, size, and societal impact of digital services. In particular, Very Large Online Platforms (VLOPs)—defined as platforms reaching at least 45 million average monthly active recipients of the service in the European Union—are subject to enhanced responsibilities. These include systemic risk assessments, risk mitigation measures, independent audits, and extensive transparency obligations, reflecting the regulation's emphasis on the proactive governance of systemic risks associated with online communication (Digital Services Act, 2022. Arts. 33–37).

In this regard, Articles 34 and 35 of the Digital Services Act establish a structured obligation requiring Very Large Online Platforms to identify and assess systemic risks related to the dissemination of illegal content, the protection of fundamental rights, civic discourse, and public security, and to implement reasonable, proportionate, and effective mitigation measures in response. These obligations move beyond the traditional reactive model of unlawful content removal. Instead, they require platforms to evaluate how the design and operation of their services—including recommender systems, algorithmic ranking mechanisms, and internal governance structures—may contribute to harmful societal outcomes (Digital Services Act, 2022. Arts. 34–35; see also Recital 79).

At the same time, the Digital Services Act (DSA) preserves a robust framework of public oversight. National Digital Services Coordinators and, in certain circumstances, the European

in determining the constitutional limits of speech regulation. See, e.g., *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997); *Moody v. NetChoice, LLC*, 603 U.S. (2024). The centrality of judicial precedent in shaping the operative content of legal norms reflects a defining methodological feature of the common law tradition.

5 For analyses describing the private governance of online speech in the United States and the contrasting emergence of systemic risk regulation in the European Union, see Balkin, 2018, pp. 1149–1210; Klonick, 2018, pp. 1598–1670. On the European approach introducing ex ante systemic risk obligations for very large online platforms, see Digital Services Act, 2022, Arts. 34–35.

Commission retain supervisory and enforcement authority over platform compliance (Digital Services Act, 2022, Arts. 66–74). Platforms designated as very large online platforms (VLOPs) must publish periodic transparency reports, provide access to platform data for vetted researchers, and comply with formal orders issued by competent authorities regarding illegal content or information requests (Digital Services Act, 2022, Arts. 9–10, 15 and 40). The regulation therefore embeds systemic risk management within platform operations while maintaining institutional control within public regulatory bodies.

This architecture reflects a calibrated regulatory design. Platforms are not granted autonomous authority to determine the meaning or application of legal norms independently of state institutions. Rather, they are required to implement structured compliance mechanisms under detailed legislative guidance and subject to external supervision. The DSA does not prescribe fixed timeframes for removal in the same manner as Germany's earlier Network Enforcement Act (NetzDG), nor does it impose a general monitoring obligation (Digital Services Act, 2022, Art. 8).[6] Instead, it emphasizes proportionality, procedural safeguards, and the protection of fundamental rights within the internal decision-making processes of platforms.

Nevertheless, the European framework signals an important evolution. By mandating systemic risk assessments and governance structures, the DSA requires platforms to internalise regulatory objectives within their operational architectures. VLOPs must identify and assess systemic risks arising from the functioning and use of their services and implement reasonable and proportionate mitigation measures addressing those risks (Digital Services Act, 2022, Arts. 34–35). Decisions concerning content prioritization, recommender systems, and enforcement practices therefore increasingly occur within private infrastructures, even where they remain subject to public oversight.

Compared to the United States, the European model narrows the gap between platform moderation and public regulatory objectives. However, it stops short of fully relocating the application of legal norms to private actors. The institutional centre of adjudication remains anchored in public authorities: enforcement powers, investigations, and sanctions remain within the competence of Digital Services Coordinators and, for VLOPs, the European Commission (Digital Services Act, 2022, Arts. 51–52). Platforms therefore operate within a clearly articulated supervisory framework rather than exercising independent regulatory authority.

In practical terms, these obligations may require very large online platforms to establish recurring internal risk-assessment processes, review how recommender systems and ranking mechanisms may contribute to the amplification of harmful content, document mitigation measures adopted in response, strengthen internal complaint and reporting channels, and maintain compliance structures capable of responding to regulatory audits or information requests. The practical significance of the DSA lies in integrating substantive obligations and institutionalised governance procedures into the operational structures of platforms.

The result is a hybrid configuration: private implementation of public obligations under structured regulatory control. This approach provides an intermediate reference point for evaluating more ambitious systems-based proposals, such as Canada's Online Harms Act. It illustrates how regulatory design can progressively embed compliance and risk-management

[6] On the contrasting German approach, see Network Enforcement Act (NetzDG) and its requirement that platforms assess reported content and remove or block illegal content within short timeframes. See also Max Planck Institute for the Study of Crime, Security and Law, *NetzDG and Human Rights*.

functions within platform operations while preserving institutional accountability through public oversight mechanisms, an issue examined in the following section.

2.3. Canada's Proposed Online Harms Act: Systems-Based Duty and Structured Internal Governance

Canada's proposed Online Harms Act (Bill C-63), introduced in 2024 but not enacted prior to parliamentary dissolution, represents one of the clearest attempts to articulate a systems-based approach to digital platform regulation. Even in its unenacted form, the proposal illustrates a regulatory design that moves beyond reactive content removal and toward proactive governance obligations embedded within platform infrastructures (Bill C-63, 2024).

At the centre of the proposed framework was a statutory "duty to act responsibly" (Bill C-63, 2024. p. 7). Rather than focusing solely on notice-and-removal mechanisms, the bill would have required regulated services to identify, assess, and mitigate the risk of exposure to harmful content on their platforms (Bill C-63, 2024, pp. 55–56). The regulatory emphasis therefore shifted from individual items of unlawful content to systemic risk management. Platforms would have been required to establish internal processes designed to prevent the amplification and circulation of categories of harmful material, including hate speech, incitement to violence, non-consensual intimate image distribution, and certain forms of large-scale disinformation (Bill C-63, 2024, Part 1, pp. 12–20).

In regulatory terms, systems-based risk management refers to an approach in which legal obligations are directed not only at individual instances of illegal content but also at the structural features of platform design and operation that shape the distribution and amplification of content online. Instead of adjudicating content item by item, platforms are required to assess systemic characteristics of their services—such as recommendation algorithms, amplification mechanisms, and moderation infrastructures—and to implement mitigation measures aimed at reducing the likelihood that harmful material will circulate at scale (Stephenson & Rinceanu, 2024, pp. 245–260).

This design reflects a structural evolution in regulatory technique. Instead of positioning platforms merely as intermediaries responding to complaints, the proposal required them to operationalise legislative objectives through structured governance mechanisms. Risk assessment, mitigation strategies, transparency obligations, and internal complaint procedures were conceived as integrated components of platform compliance architecture (Stephenson & Rinceanu, 2024, pp. 245–260).[7]

In operational terms, the proposed framework would likely have required regulated services to establish internal safety governance systems, develop recurring risk-assessment procedures, implement mitigation protocols for harmful content categories, maintain complaint and review mechanisms, and preserve documentary records demonstrating compliance with the statutory duty to act responsibly. Its significance lies in translating legislative objectives into ongoing internal governance responsibilities within platform infrastructures.

Importantly, the proposed Act did not eliminate public oversight. It envisaged the creation of a Digital Safety Commission of Canada with supervisory and enforcement authority, thereby maintaining an institutional role for public regulators (Bill C-63, 2024, Part 1, pp. 81–136). Nevertheless, the practical implementation of statutory standards would have occurred within platform systems themselves. Corporate compliance bodies and content

[7] For broader analysis of systems-based regulatory models, see also: Balkin, 2018, pp. 1149–1210.

moderation teams would have been tasked with interpreting statutory categories of harm, determining operational thresholds for intervention, and applying enforcement measures such as removal, restriction, or demotion of content.

In this respect, the Canadian proposal illustrates a more pronounced embedding of public regulatory objectives within private infrastructures than either the American or the European model. While the United States preserves a strong separation between public adjudication and private moderation, and the European Union combines systemic obligations with robust supervisory oversight, the Canadian framework more directly structured platforms as proactive risk managers operating under statutory mandate.

The significance of this model lies not in the transfer of formal adjudicative authority to private actors, but in the reconfiguration of where and how norm implementation occurs. Under a systems-based duty, the first instance of assessment—whether particular content falls within legislatively defined categories of harm and whether mitigation measures are required—would take place within platform governance systems before any intervention by courts or regulators. Public institutions would retain supervisory and review functions, yet the operational application of statutory standards would be embedded within private decision-making architectures.

Even though Bill C-63 was not enacted, its design signals an emerging regulatory trajectory. It reflects a growing willingness among legislators to require platforms to internalise harm prevention as a structural obligation rather than as a reactive response. This systems-based approach raises important analytical questions about accountability, procedural safeguards, and the balance between proactive governance and freedom of expression. These questions become particularly salient when comparing the Canadian proposal to the American emphasis on editorial discretion and the European model of supervised systemic compliance (Stephenson & Rinceanu, 2024, pp. 245–260, see also: Balkin, 2018, pp. 1149–1210). Understanding this regulatory shift requires examining the conceptual foundations of systems-based governance and the role of risk management in contemporary regulatory theory.

3. THE DUTY TO ACT RESPONSIBLY AND RISK GOVERNANCE IN PLATFORM REGULATION

3.1. Systems-Based Regulation and the Management of Harm

The emergence of systems-based regulatory frameworks reflects a broader transformation in how contemporary legal systems address complex technological risks. Rather than relying exclusively on *ex post* enforcement mechanisms, modern governance increasingly emphasizes anticipatory risk management, requiring regulated actors to identify, evaluate, and mitigate potential harms before they fully materialize (Black, 2005, pp. 510–546).

As the comparative analysis developed in the previous section has shown, the regulatory models examined here—particularly those of the European Union and the Canadian proposal—reflect an emerging shift toward systemic risk management in platform governance (Digital Services Act, 2022, Arts. 34–35; Bill C-63, 2024). These frameworks do not rely solely on the removal of unlawful content after its circulation. Instead, they impose obligations requiring platforms to evaluate systemic risks associated with the functioning of their infrastructures and to implement preventive governance mechanisms designed to mitigate such risks (Stephenson & Rinceanu, 2024, pp. 245–260).

This shift reflects a broader regulatory logic in which attention moves from isolated violations toward the structural conditions that enable harmful communication dynamics. In this model, regulatory intervention no longer focuses exclusively on the legality of individual pieces of content. Rather, it increasingly addresses the systemic environments in which digital communication occurs, and the institutional responsibilities associated with managing the risks generated by those environments.

Such developments can be more clearly understood through the analytical perspective offered by systems theory, particularly the work of Niklas Luhmann, who conceptualises risk as an intrinsic feature of decision-making in complex social systems (Luhmann, 2005). In Luhmann's framework, risk differs from danger: while danger refers to harm originating from external factors beyond the control of decision-makers, risk refers to harm that can be attributed to decisions taken within institutional structures (Luhmann, 2005). Modern institutions therefore operate under conditions of increasing complexity, where decisions must be taken despite limited knowledge about their potential consequences. When an institution selects one course of action among several possible alternatives, it simultaneously assumes responsibility for the risks generated by that decision (Luhmann, 2005).

Digital platforms operate within precisely such environments. Their infrastructures facilitate large-scale communication processes in which information circulates rapidly across interconnected networks and unpredictable patterns of interaction emerge (Balkin, 2018, pp. 1149–1210). Under these conditions, harmful outcomes cannot be fully prevented through traditional legal adjudication alone. Instead, regulatory frameworks increasingly require platforms to develop governance mechanisms capable of identifying patterns of risk and mitigating their potential effects (Digital Services Act, 2022, Arts. 34–35).

These developments suggest the gradual emergence of a regulatory model in which the management of digital harms increasingly occurs through proactive risk-management obligations embedded within platform infrastructures. Rather than relying solely on reactive enforcement after harm has occurred, systems-based regulation requires platforms to anticipate potential harms and adopt governance processes designed to mitigate foreseeable risks generated by their own communication environments (Stephenson & Rinceanu, 2024, pp. 245–260).

From this perspective, contemporary platform regulation seeks not to eliminate all harmful outcomes—an impossible objective in complex communication systems—but to ensure that platforms assume institutional responsibility for managing the risks generated by their infrastructures. Proactive risk management therefore becomes a central component of modern regulatory approaches to digital platforms, shifting regulatory attention from the adjudication of individual pieces of content toward the governance of the infrastructures through which digital communication occurs (Luhmann, 2005).

3.2. Decision-Making Structures in Platform Governance

The regulatory shift toward systemic risk management also entails a transformation in the institutional role of digital platforms. When platforms are required to identify risks, interpret regulatory obligations, and implement mitigation measures affecting the circulation of information, they necessarily engage in forms of structured decision-making within their governance systems (Stephenson & Rinceanu, 2024, pp. 245–260).

Although these decision-making processes remain formally situated within private organizational infrastructures, they increasingly involve the interpretation of regulatory standards, the evaluation of potentially harmful communication dynamics, and the adoption of measures that may affect the visibility, distribution, or removal of content. In this respect, platform governance increasingly operates at the intersection of private organizational management and the implementation of public regulatory objectives (Balkin, 2018, pp. 1149–1210). In this sense, platforms operate within regulatory environments in which the implementation of legal norms is partially mediated through internal governance mechanisms.

Within these frameworks, platforms increasingly function as institutional actors responsible for the management of systemic communication risks. Their governance architectures may include internal review procedures, risk-assessment protocols, algorithmic moderation systems, and complaint or appeal mechanisms through which enforcement decisions can be examined and potentially revised (Digital Services Act, 2022, Arts. 14, 16–17, 20, 34–35). From the perspective of systems theory, such governance mechanisms can be understood as organizational decision structures through which institutions process uncertainty and attribute responsibility for the risks generated by their own operations (Luhmann, 2005).

The emergence of these structures reflects the broader regulatory strategy discussed throughout this article. Rather than relying exclusively on external enforcement by courts or administrative authorities, contemporary regulatory frameworks increasingly require platforms themselves to develop institutional capacities for risk observation, evaluation, and mitigation within their own infrastructures (Bill C-63, 2024).

This development does not imply that platforms replace public authorities or assume the role of judicial institutions. However, it does indicate that regulatory design increasingly situates certain forms of decision-making within platform governance systems themselves. These processes therefore constitute a form of institutionally structured decision-making embedded within digital infrastructures, through which regulatory objectives are operationalised in practice (Luhmann, 2005). These internal governance processes therefore contribute to the practical redistribution of decision-making authority in digital communication environments, even where formal jurisdiction remains located within public institutions (Digital Services Act, 2022, Arts. 14, 16–17, 20, 34–35). As digital communication environments continue to evolve, these internal governance processes are likely to play an increasingly significant role in shaping how regulatory norms are implemented in practice.

For this reason, examining how platforms organize and exercise these decision-making functions becomes an important element in understanding contemporary models of digital governance. At the same time, the increasing reliance on internal governance mechanisms raises questions regarding the forms of oversight that may apply to these decisions. Where platforms interpret regulatory obligations and adopt mitigation measures under statutory frameworks, courts may be called upon to review whether these processes satisfy the legal standards established by regulation and whether the "duty to act responsibly" in the management of systemic risks has been fulfilled (Digital Services Act, 2022, Arts. 45–51).

4. CONCLUSION

The comparative analysis of the United States, the European Union, and Canada reveals a significant transformation in the regulatory architecture governing digital platforms. While the

American model continues to emphasize intermediary immunity and the protection of editorial discretion, and the European framework embeds systemic obligations within a robust supervisory structure, more recent systems-based proposals such as Canada's Online Harms Act reflect a growing legislative commitment to proactive risk management and structured internal governance.

This transformation does not amount to a formal transfer of adjudicative authority to private actors. Courts and regulatory bodies remain central to the institutional framework of digital governance, and public oversight continues to provide the foundation for regulatory legitimacy. Yet the operational site at which public norms are implemented increasingly lies within platform infrastructures themselves. Platforms are required not only to remove unlawful content when notified, but also to identify systemic risks, interpret legislative standards, and implement mitigation measures through internal governance processes embedded within their own decision-making systems.

Recognizing the functional resemblance between such processes and traditional forms of norm application does not collapse the distinction between public and private authority. Rather, it clarifies how contemporary regulatory design reshapes the practical dynamics of governance in digital constitutional democracies. As systems-based obligations become more prominent, the focus of regulatory oversight gradually shifts from isolated enforcement decisions toward the adequacy of the institutional structures through which platforms observe, assess, and mitigate systemic risks within their communication environments.

From this perspective, accountability increasingly depends on the standards used to evaluate whether platforms have fulfilled their statutory duty to act responsibly. Regulatory and judicial scrutiny is therefore likely to focus less on individual moderation outcomes and more on whether platforms have implemented coherent risk-assessment processes, developed appropriate mitigation strategies, and maintained governance architectures capable of identifying and responding to emerging harms. In systems-theoretical terms, risk arises not simply from uncertainty but from decisions taken within institutional structures operating under conditions of complexity. Where platforms are required to manage systemic risks generated by their own infrastructures, the responsibility attached to those decisions becomes a central concern of regulatory design.

Future regulatory debates will therefore turn on how best to preserve accountability and fundamental rights while embedding proactive responsibilities within private communication infrastructures. The challenge is not merely to allocate liability after harm has occurred, but to articulate legal and institutional standards capable of guiding and evaluating the structured discretion exercised by platforms under statutory mandates of systemic risk management. In this sense, the evolution of digital governance illustrates a broader transformation in regulatory thought: the task of law increasingly lies not only in adjudicating individual violations but also in shaping the institutional conditions through which complex communication systems generate, observe, and respond to risk. Sustained comparative analysis will remain essential to understanding how constitutional principles, regulatory institutions, and private infrastructures interact in the ongoing development of governance in the algorithmic society.

LIST OF REFERENCES

Books and Articles

Balkin, J.M. 2018. Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation. *UC Davis Law Review*, 51, pp. 1149–1210.

Black, J. 2005. The Emergence of Risk-Based Regulation and the New Public Risk Management. *Public Law*, Autumn 2005, pp. 510–546.
Klonick, K. 2018. The New Governors: The People, Rules, and Processes Governing Online Speech. *Harvard Law Review*, 131(6), pp. 1598–1670.
Luhmann, N. 2005. *Risk: A Sociological Theory.* With a new introduction by N. Stehr and G. Bechmann. London/New York: Routledge.
Stephenson, R. & Rinceanu, J. 2024. Differential Diagnosis in Online Regulation: Reframing Canada's "Systems-Based" Approach. *eucrim – The European Criminal Law Associations Forum*, 3, pp. 245–260. https://doi.org/10.30709/eucrim-2024-007

Reports and Online Sources

Rinceanu, J. n.d. *NetzDG and Human Rights*. Max Planck Institute for the Study of Crime, Security and Law. Available at: https://csl.mpg.de/en/projects/netzdg-and-human-rights (24. 4. 2026).
Rinceanu, J. & Stephenson, R. n.d. *Rethinking Digital Media Regulation*. Max Planck Institute for the Study of Crime, Security and Law. Available at: https://csl.mpg.de/en/projects/rethinking-digital-media-regulation (24. 4. 2026).

Legislation

Canada. 2024. *Bill C-63: An Act to enact the Online Harms Act, to amend the Criminal Code, the Canadian Human Rights Act and related Acts*, 1st Sess., 44th Parl. (first reading 26 February 2024).
European Union. 2022. *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act).*
Germany. 2017. *Network Enforcement Act (NetzDG).*
United States. 1996. *Communications Decency Act, 47 U.S.C. § 230.*

Cases

Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998).
Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003).
Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008) (en banc).
Force v. Facebook, Inc., 934 F.3d 53 (2d Cir. 2019).
Jones v. Dirty World Entertainment Recordings LLC, 755 F.3d 398 (6th Cir. 2014).
Moody v. NetChoice, LLC (2024) Supreme Court of the United States.
NetChoice, LLC v. Moody (2022) 34 F.4th 1196 (11th Cir.).
Zeran v. America Online, Inc. (1997) 129 F.3d 327 (4th Cir.).