Constitutional Accountability in the Platform Age: A Three-Dimensional Framework for Algorithmic Governance

Nicola Lucchi[†]

Algorithmic governance increasingly shapes how information circulates, how norms are enforced, and how democratic decisions are made. Yet constitutional theory lacks the tools to conceptualize accountability in this new environment, where private digital platforms exercise public-like powers with limited oversight. This Article develops a new framework for digital constitutional accountability, structured around three dimensions: epistemic (who controls knowledge and visibility), normative (who sets and enforces behavioral standards), and systemic (which institutions ensure constitutional review and democratic legitimacy). Unlike prior models focused solely on transparency or ethics, this approach integrates comparative jurisprudence, regulatory theory, and institutional design. Through case studies and constitutional decisions from the EU, United States, and United Kingdom, the Article shows how platform power disrupts traditional mechanisms of accountability, and how courts, regulators, and lawmakers are beginning to respond. It concludes by proposing a reform agenda grounded in constitutional law, aimed at reasserting public oversight over privatized digital infrastructures.

† The author wishes to thank Paolo Veronesi, Cesare Mainardi, and Marco Bassini for their generous comments on earlier drafts of this Article. All remaining errors are the author's own. The author operationalized this framework as the "Three-Pillar Accountability Test" in Nicola Lucchi, Generative AI and Copyright: Training, Creation, Regulation (Eur. Parl., Pol'y Dep't for Just., Civ. Liberties & Institutional Affs., PE 774.095, July 2025), § 4.0, tbls. 6, 8 & 21.

Introduction

In a world where digital technologies such as artificial intelligence, big data, and social media increasingly shape political dynamics and democratic structures, understanding their impact on constitutional norms and governance has become essential. This Article examines key legal and institutional dimensions of how emerging technologies reshape democratic governance, with particular attention to their influence on public discourse and regulatory design.

The digital transition has progressively shifted the center of public power toward private actors, especially technology platforms that mediate access to information, regulate digital discourse, and shape political behavior. In response to this transformation, constitutional law requires a revised conceptual toolkit and new categories and frameworks capable of confronting the systemic power exercised by algorithmic infrastructures and data-driven systems. This Article proposes digital constitutional accountability as a first attempt to articulate such a framework: one that can reconnect emerging digital power structures with the normative foundations of constitutional democracy. Developed in dialogue with, and extending, classic accountability taxonomies,[1] this framework situates constitutional accountability within the specific conditions of platformized, algorithmic power. This need is not confined to a single jurisdiction. Across diverse legal systems – including the United States, the European Union, and the United Kingdom – constitutional law often lacks

1. *See*, *e.g.*, Mark Bovens, *Analysing and Assessing Accountability: A Conceptual Framework*, 13 EUR. L.J. 447 (2007); Pierre Rosanvallon, COUNTER-DEMOCRACY: POLITICS IN AN AGE OF DISTRUST (Arthur Goldhammer trans., 2008).

a conceptual vocabulary robust enough to capture the systemic, infrastructural nature of algorithmic authority. This Article addresses that analytical gap by offering a normative model capable of describing and confronting these new configurations of power. This intervention is closely related to the literature on "digital constitutionalism," but it departs from strands of that debate (and adjacent work on "digital sovereignty") that primarily either (i) map emerging digital rights catalogues and normative charters,[2] or (ii) frame the problem in terms of control-oriented claims over infrastructures and data flows.[3] Rather, it develops an operational accountability model that specifies rights-relevant duties, institutional fora, and remedial pathways across epistemic, normative, and systemic dimensions of digital power. Throughout, the Article uses constitutional authority as the core analytical term, understood as the State's final constitutional responsibility for rights-affecting public decisions. Constitutional authority is the responsibility claim; constitutional accountability is the framework that makes that responsibility administrable.

The methodological approach adopted in this Article is intentionally synthetic and concept-driven. It reframes classic constitutional categories in light of algorithmic governance, offering a normative-conceptual model designed to map shifting loci of power and legitimacy in technologically mediated environments. This conceptual lens does not depart from constitutional theory but builds on its foundational values applying them to new algorithmic contexts where legal doctrine remains underdeveloped.

This framework is developed along three key dimensions:

(1) Epistemic accountability, concerning how digital infrastructures shape access to knowledge and define visibility in the public sphere;
(2) Normative accountability, referring to the power to define and enforce rules of behavior and speech in digital spaces;
(3) Systemic accountability, focusing on the institutional mechanisms – courts, parliaments, and regulators – that can re-anchor digital power within the logic of constitutional democracy.

Adopting a comparative perspective grounded in constitutional and regulatory analysis, the Article focuses on how legal systems in Europe and the United States are responding to technological developments that affect democratic accountability. The choice to include the European Union, the United States, and the United Kingdom is not merely illustrative: each offers a distinct normative and institutional response to the challenges posed by algorithmic power and platform governance. The EU's approach, grounded in data protection and

2. *See*, *e.g.*, Dennis Redeker, Lex Gill & Urs Gasser, *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights*, 80 Int'l Commc'n Gazette 302 (2018) (surveying "Internet bills of rights" instruments); Edoardo Celeste, *Digital Constitutionalism: A New Systematic Theorisation*, 33 Int'l Rev. L., Computs. & Tech. 76 (2019) (systematizing digital constitutionalism scholarship).

3. Luciano Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, 33 Phil. & Tech. 369 (2020) (defining "digital sovereignty" as control over key digital dependencies); Stéphane Couture & Sophie Toupin, *What Does the Notion of "Sovereignty" Mean When Referring to the Digital?*, 21 New Media & Soc'y 2305 (2019) (tracing "sovereignty" as autonomy and control in digital debates); Gerda Falkner, et al., *Digital Sovereignty: Rhetoric and Reality*, 31 J. Eur. Pub. Pol'y 2099 (2024) (identifying infrastructure, code, and data as core layers of digital sovereignty).

regulatory interventionism, stands in marked contrast to the market-centered logic of the US, while the UK represents an instructive hybrid model, shaped by both EU regulatory legacy and a renewed emphasis on national discretion in the post-Brexit era.

Through these case studies, the Article seeks not only to trace diverging trajectories but to uncover how foundational principles such as transparency, participation, and constitutional accountability are being reinterpreted, or eroded, by the digital turn. Key examples include the Cambridge Analytica scandal, the strategic use of social media by populist movements in the U.S. and Italy, and the UK's use of predictive algorithms in political campaigns. These cases were selected for their relevance to core democratic principles – transparency and accountability – as well as their illustrative power in showcasing diverse regulatory responses to shared technological challenges. The selection reflects the diversity, and asymmetry, of regulatory responses to similar democratic threats, and is intended to foster a meaningful interdisciplinary dialogue.

Following an exploration of the foundational context in the Introduction this Article transitions, beginning with Section I, into four main analytical parts. Section I examines the evolving relationship between digital technologies and constitutional authority understood as the State's final constitutional responsibility for rights-affecting public decisions, culminating in the Article's original thesis in subsection I.A.: a tripartite framework of digital constitutional accountability that distinguishes between epistemic, normative, and systemic dimensions of digital power. Section II explores how technological innovation reshapes public debate and democratic participation, analyzing these developments through the lens of the proposed framework. Section III presents case studies that apply this analytical model to concrete contexts, tracing patterns of democratic erosion and institutional adaptation across diverse jurisdictions. Finally, Section IV addresses the regulatory challenges raised by digital technologies, drawing on the preceding analysis to propose strategies for effective and principled governance.

A. Digital Transformation and Democratic Governance

Digital transformation, particularly through AI and algorithmic technologies,[4] has begun to reshape key elements of democratic governance, with far-reaching impacts on information, communication, and authority structures.[5] At the heart of these changes lies the shaping of the digital information environment by AI-driven algorithms[6] embedded within digital platforms that mediate political communication. These systems curate political information in ways that determine its accessibility and diversity, producing patterns of selective

4. In this Article, "AI" is used as machine-based systems that infer outputs (e.g., predictions, recommendations, content, or decisions) from inputs. "Algorithmic technologies" is used as an umbrella term for automated decision or ranking systems, including rule-based systems.

5. *See* Domingo García-Marzá & Patrici Calvo, Algorithmic Democracy: A Critical Perspective Based on Deliberative Democracy 81 (Springer 2024); *see also* Nathalie A. Smuha, Algorithmic Rule By Law: How Algorithmic Regulation in the Public Sector Erodes the Rule of Law (Cambridge Univ. Press 2025).

6. *See* Andreas Jungherr, *Artificial Intelligence and Democracy: A Conceptual Framework*, 9 Social Media + Society, 1-14 (2023); Andreas Jungherr & Ralph Schroeder, *Artificial Intelligence and the Public Arena*, 33 Communic'n Theory 164–173 (2023).

exposure, heightened conflict, and potential manipulation that complicate individuals' ability to make well-informed decisions essential for self-governance and, [7] as developed in Section I.B and applied in II, undermine epistemic forms of constitutional accountability.

Furthermore, AI is reshaping the economic landscape of news production, where the emphasis on automated content over traditional journalistic practices strains news organizations.[8] Economic pressures foster business models that favor attention-grabbing content and, at times, disinformation, narrowing political coverage and limiting the spectrum of perspectives.[9] This shift widens informational gaps between those who can pay for high-quality news and those who depend on free, often AI-generated content, thereby deepening epistemic inequalities that constitutional law has not yet fully addressed.[10]

The influence of algorithms extends to free speech, where content moderation practices on digital platforms often filter information through opaque top-down mechanisms.[11] These algorithms sometimes misclassify legitimate expressions, particularly minority or dissenting voices, diminishing the diversity of viewpoints.[12] The absence of clear oversight in algorithmic moderation raises significant concerns about accountability and legal certainty, including uncertainty as to the applicable regulatory and liability regimes, underscoring the urgency of democratic oversight mechanisms and robust institutional counterweights.[13] These developments raise normative questions about who sets the applicable rules and systemic questions about which institutions supervise their

---

7. *See*, *e.g.*, Seth Flaxman et al., *Echo Chambers, and Online News Consumption*, 80 Public Opinion Quarterly, 298-320 (2016); R Kelly Garrett, *Echo Chambers Online? Politically Motivated Selective Exposure Among Internet News Users*, 14 J. Computer-Mediated Commc'n 265 (2009); Pablo Barberá, Social Media, Echo Chambers, and Political Polarization, in Social Media and Democracy 34-55 (Nathaniel Persily & Joshua A. Tucker eds., Cambridge Univ. Press 2020); García-Marzá & Calvo, *supra* note 5, at 85 (discussing on the role of digital platforms in facilitating polarizing message).

8. Felix M. Simon, *Artificial Intelligence in the News: How AI Retools, Rationalizes, and Reshapes Journalism and the Public Arena*, Tow Center for Digital Journalism (Feb. 6, 2024), https://towcenter.columbia.edu/sites/default/files/ content/Tow%20Report_Felix-Simon-AI-in-the-News.pdf. [https://perma.cc/7GQH-LPJ3]

9. *See* E. Bonadio et al., *Fake News and Copyright*, 11(4) Queen Mary J.of Intell. Prop. 444 (2021) (illustrating how fake news often operates as a clickbait-driven business model); Donato Vese, *Governing Fake News: The Regulation of Social Media and the Right to Freedom of Expression in the Era of Emergency*, 13 Eur. J. Risk Reg. 477 (2022).

10. *See* Stanislaw Piasecki et. al., *AI-generated Journalism: Do the Transparency Provisions in the AI Act Give News Readers What They Hope For?*, 13 Internet Pol'y. Rev. 1-28 (2024) (noting transparency deficits in AI-generated news).

11. *See* Andreas Jungherr & Ralph Schroeder, Digital Transformations of the Public Arena (Cambridge Univ. Press 2022) (showing how digital tech reshapes discourse via information access, issue framing, and increased polarization).

12. *See* Jungherr, *supra* note 6, at 5 (noting how opaque AI content classification risks suppressing legitimate political speech).

13. *See, e.g.*, Robert Gorwa et al., *Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance*, 7 Big Data & Soc'y 1–15 (2020); Barrie Sander, *Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of a Human Rights-Based Approach to Content Moderation*, 43 Fordham Int'l L.J. 939 (2020); Giovanni De Gregorio, *Democratising Online Content Moderation: A Constitutional Framework*, 36 Comput. Law & Sec. Rev. 1-17 (2020).

application, both of which are central to the framework of normative and systemic accountability articulated in Section II.B.

In parallel, AI's predictive and generative capabilities contribute to the manipulation of reality through targeted messaging that can influence opinions, behaviors, and potentially inundate digital spaces with misleading content.[14] This spread of disinformation can erode trust in information and diminish personal autonomy. From the perspective of epistemic accountability, this environment makes it harder for constitutional systems to secure a minimally reliable informational baseline for democratic deliberation. AI's rise has also shifted decision-making authority toward expert-driven models.[15] As predictive technologies gain prominence, they elevate the role of expert judgment over collective decision-making, potentially weakening democratic engagement by centralizing authority in fewer hands.[16] This technocratic shift not only redistributes normative authority over rule-setting but also raises systemic questions about how such expert power is checked and justified within constitutional structures.

Finally, AI's ascent has concentrated substantial power in tech giants, effectively transferring innovation and oversight responsibilities from public institutions to private entities.[17] This shift raises additional concerns about the erosion of democratic control, as these companies increasingly influence economic sectors, political decision-making, and information distribution.[18] The unchecked expansion of their influence emphasizes the need for robust regulatory frameworks and oversight to preserve democratic self-rule. These transformations illustrate how digital technologies unsettle the epistemic, normative, and systemic dimensions of constitutional accountability that the remainder of the Article seeks to conceptualize and address.

B. Populism and Digital Platforms

The evolution of digital technologies, including artificial intelligence (AI), big data, and social media, has also triggered a profound restructuring in the dynamics of executive and parliamentary powers, as well as in political practices.[19] In particular, contemporary populist movements in Europe, the United States, and elsewhere rely on these technologies in ways that may put pressure on, and

14. *See* Louis Rosenberg, *Generative AI as a Dangerous New Form of Media*, *in Proceedings of the International Multi-Conference on Society, Cybernetics and Informatics*, IMSCI (2023), https://www.iiis.org/CDs2023/CD2023Summer/papers/HA408FU.pdf [https://perma.cc/Y75D-VQF4]

15. *See*, *e.g.*, Melissa Schwartzberg, *Epistemic Democracy and Its Challenges*, 18 Ann. Rev. Pol. Sci. 187 (2015) (discussing the risks of over-relying on experts in decision-making).

16. *Id.; see also* Karen Lund Petersen & Vibeke Schou Tjalve, *Intelligence Expertise in the Age of Information Sharing: Public–Private 'Collection' and its Challenges to Democratic Control and Aaccountability*, 33 Intelligence and Nat'l Sec. 21–35 (2017) (discussing predictive tech's strain on democratic oversight).

17. *See* Paul Nemitz, *Constitutional Democracy and Technology in the Age of Artificial Intelligence*, 376 Phil. Trans. R. Soc. A 1, 2 (2018).

18. *See* Saura García, *Datafeudalism: The Domination of Modern Societies by Big Tech Companies*, 37 Philos. Technol. 90 (2024); García-Marzá & Calvo, *supra* note 5, at 234 (examining the Big Tech's role in controlling the public sphere.

19. *See* Giovanni Di Cosimo, La Partecipazione nell'era Digitale, *in* G. Di Cosimo, Processi Democratici e Tecnologie Digitali 231(Giappichelli, 2023).

in some instances prompt a rethinking of, classic categories of constitutional theory[20] and to recast the relationship between "the people" and institutional elites.[21] Populism, which manifests in various forms across different parts of the world, has used digital platforms to mobilize support, disseminate simple and often polarizing messages, and bypass traditional political and institutional intermediaries.[22] This has reshaped how political ideas are presented and received, posing new challenges to democratic governance and constitutional stability. At the same time, the multiplication of information channels does not necessarily disperse agenda-setting power, given the structural scarcity of attention and the role of platform curation in concentrating visibility. Such distorted uses can strain foundational principles of liberal democracies, including the separation of powers.[23] Populist leaders and movements have exploited digital platforms and social media to disseminate simplified and, at times misleading or false, information. Their aim is to polarize public opinion and erode trust in traditional democratic institutions. In doing so, they promote political agendas that favor a centralized and personalized vision of power, thereby justifying actions that often conflict with constitutional norms and fundamental rights.[24] This process contributes to the subversion of the traditional democratic order, replacing established checks and balances with agendas that prioritize the immediate will of the people as interpreted by these leaders, at the expense of constitutional safeguards.[25]

A central instrument in this dynamic is the strategic use of disinformation and so-called "fake news",[26] which functions as a low-cost, algorithmically amplified tool of digital propaganda.[27] Political actors exploit data analytics and

---

20. *See generally* Andrew Arato & Jean L. Cohen, Populism and Civil Society: The Challenge to Constitutional Democracy (Oxford Univ. Press 2022) (analyzing how communication technologies enable populist messaging that contests constitutional norms and reshapes civil society's role); Thomas Wellings & Lone Sørensen, *The Digital Performance of Populism, in* Handbook of Digital Politics 370 (Stephen Coleman & Lone Sørensen eds., 2023) (arguing that digital media is used to broaden reach and to reframe core democratic concepts, shaping perceptions of constitutional authority); Hans-Jörg Trenz, *Democracy in the Digital Public Sphere: Disruptive or Self-Corrective?*, 33 Commc'n Theory 143, 143–52 (2023) (exploring how online mobilization can facilitate populist reinterpretations of democratic principles).

21. *See* Bart Bonikowski, *Three Lessons of Contemporary Populism in Europe and the United States*, 23 Brown Journal of World Affairs 9-24 (2016) (discussing populism's core characteristic of positioning "the people" against political elites both in EU and US).

22. *See* P. Veronesi, *"Farmaco e Veleno": Il Populismo tra Fisiologia e Patologia, in* GenIus 50-71 (2022).

23. *See* Final Report of the Select Committee to Investigate the January 6th Attack on the United States Capitol, H.R. Rep. No. 117-663 (2022) (describing social-media pressure tactics around the electoral-vote count).

24. *See* M. Monti, *Italian Populism and Fake News on the Internet: A New Political Weapon in the Public Discourse*, *in* G. Delledonne et al., Italian Populism and Constitutional Law: Strategies, Conflicts and Dilemmas 177 (Springer 2020); Veronesi, *supra* note 22. On the role of digital ecosystems in fostering polarization, *see also* García-Marzá & Calvo, *supra* note 5, at 85

25. G. Martinico, Filtering Populist Claims to Fight Populism: The Italian Case in a Comparative Perspective 15 (Cambridge Univ. Press 2022).

26. *See e.g.*, Susan Morgan, *Fake News, Disinformation, Manipulation and Online Tactics to Undermine Democracy*, 3 J. of Cyber Policy 3(1) 39–43 (2018).

27. *See* Katherine Ognyanova et al., *Misinformation in Action: Fake News Exposure is Linked to Lower Trust in Media, Higher Trust in Government When Your Side is in Power*, Harv. Kennedy Sch. Misinformation Rev.(2020), https://misinforeview.hks.harvard.edu/article/

micro-targeting to tailor emotionally charged messages to specific groups, reinforcing preexisting biases and deepening the patterns of polarization and echo chambers that Section II examines in greater detail.[28] From the standpoint of epistemic accountability, these techniques disrupt shared factual baselines and weaken the conditions for reasoned democratic deliberation.

However, it is also essential to recognize that populism is not merely a byproduct of technological change but reflects a broader breakdown of governance that includes both economic disenfranchisement and weakened information safeguards. The decline of traditional media's gatekeeping role and the rise of platform monopolies has fueled public resentment: resentment that populist leaders skillfully channel against both entrenched elites and marginalized groups. This concentration of communicative and economic power can enable highly concentrated platform ownership and corporate leadership to exert disproportionate influence over agenda-setting incentives and platform governance choices, with spillovers for civic discourse and democratic participation. This dynamic raises profound questions about the accountability of digital communication channels and the resilience of democratic debate in an era dominated by corporate interests. The recent growing nexus between populist figures and prominent platform owners and senior technology executives exemplifies a broader dynamic: as populist rhetoric taps into societal frustration, the conjunction of political strategy and platform governance can intensify visibility dynamics in ways that stress democratic resilience. These developments illustrate how populist uses of digital infrastructures simultaneously erode epistemic accountability (through distorted information flows), normative accountability (through the personalization and centralization of power), and systemic accountability (through weakened institutional checks), thereby motivating the constitutional framework advanced in Section I.B and the case studies analyzed in Section III.

These developments call for systemic constitutional responses: not only to regulate digital platforms, but to reassert public control over the normative and epistemic infrastructures through which democratic legitimacy is constructed.

C. Digital Political Communication: Balancing Privacy, Data Security, and Public Trust

The integration of communication technologies has also transformed the way governments and politicians interact with citizens, manage information, and make decisions.[29] The real-time analysis of large volumes of data allows policymakers to understand the needs and perceptions of the electorate more immediately.[30] However, this capability simultaneously challenges privacy, autonomy,

misinformation-in-action-fake-news-exposure-is-linked-to-lower-trust-in-media-higher-trust-in-government-when-your-side-is-in-power/ [https://perma.cc/J2ZN-C5DF]

28. *See* Spencer McKay and Chris Tenove, *Disinformation as a Threat to Deliberative Democracy*, 74 Pol. Rsch. Q. 703-717 (2021).

29. Di Cosimo, *supra* note 19, at 231.

30. *See e.g.*, Shannon C. McGregor, *"Taking the Temperature of the Room": How Political Campaigns Use Social Media to Understand and Represent Public Opinion*, 84 Pub. Opinion Q. 236-256 (2020) (discussing how campaigns use social media data to gauge public opinion quickly, providing a responsive approach to understanding electorate needs and perceptions);

and the legitimacy of democratic deliberation, raising pressing questions about how to protect citizens' rights while fostering innovation.[31] Moreover, social media have reshaped the landscape of political communication, facilitating a more direct and immediate interaction between politicians and the public.[32] This disintermediation has allowed political leaders to communicate without the filter of traditional media, presenting opportunities for greater transparency alongside risks related to the spread of unverified or manipulated information.

Recent election research illustrates how social media can polarize debate and concentrate exposure to low-quality political content among subsets of users.[33] Such developments reflect a deepening crisis of epistemic accountability in political communication, where algorithmic curation shapes democratic reasoning.[34]

Democratic control and public debate are thus influenced more and more by a flow of communication that can be as empowering as it is dangerous, depending on how it is managed.[35] Some political movements and leaders have exploited these dynamics to attack democratic institutions, manipulating constitutional narratives to their advantage. These strategies may weaken checks and balances through formally lawful means while eroding constitutional constraints.[36] Not all legislators – aware of the risks these dynamics pose to the integrity of the democratic process – have remained indifferent. Recently, the European Union adopted the Regulation on Political Advertising Transparency,[37] aimed at ensuring the clear identification of online political advertising and transparency regarding its sponsors.

Christopher S. Elmendorf and Abby K. Wood, *Elite Political Ignorance: Law, Data, and the Representation of (Mis)Perceived Electorates*, 52 UC Davis L. Rev. 571 (2019).

31. S. Calzolaio, *Dalla Protezione Dei Dati Personali all'ordinamento Dei Dati*, *in* G. Di Cosimo, Processi Democratici e Tecnologie Digitali 197 (Giappichelli, 2023).

32. E. Caterina, *La Comunicazione Elettorale Sui Social Media tra Autoregolazione e Profili di Diritto Costituzionale*, *in* G. Di Cosimo, Processi Democratici e Tecnologie Digitali 19 (Giappichelli, 2023).

33. *See e.g.*, Elisa Shearer et al., *Americans' Views of 2024 Election News*, Pew Research Center (Oct. 10, 2024) https://www.pewresearch.org/wp-content/uploads/sites/20/2024/10/PJ_2024.10.10_2024-election-news_report.pdf [https://perma.cc/2CY2-XB7Z] (noting that 73% of U.S. adults frequently encounter inaccurate election news, often via social media); Andrew M. Guess et al., *Exposure to Untrustworthy Websites in the 2016 US Election*, 4 Nature Human Behavior 472 (2020); Nir Grinberg et al., *Fake News on Twitter During the 2016 U.S. Presidential Election,* 363 Science 374 (2019) [https://perma.cc/2CY2-XB7Z]

34. *See e.g.*, Mike Ananny & Kate Crawford, *Seeing Without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability*, 20 New Media & Soc'y 973 (2018) (arguing transparency alone is insufficient for algorithmic accountability).

35. *See, e.g.*, B. Stark & D. Stegmann, *Are Algorithms a Threat to Democracy? The Rise of Intermediaries: A Challenge for Public Discourse*, AlgorithmWatch (2020), https://algorithmwatch.org/en/wp-content/uploads/2020/05/Governing-Platforms-communications-study-Stark-May-2020-AlgorithmWatch.pdf [[https://perma.cc/4CLN-YVX3]] (last accessed on Mar. 8, 2026); *see also* U. Klinger et al., Platforms, Power, and Politics: An Introduction to Political Communication in the Digital Age 50 (Cambridge, 2023) (arguing that democratic systems are damaged when the infrastructure of the public sphere can no longer "guarantee the formation of competing public opinions, i.e., qualitatively filtered opinions," and that the empowering and disruptive potential of platform-mediated communication flows depends on how such infrastructure is governed).

36. *See* Kim Lane Scheppele, *Autocratic Legalism*, 85 U. Chi. L. Rev. 545, 548-49 (2018) (defining "autocratic legalism").

37. Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising, OJ L 150, 15.3.2024 p. 1–44.

Commentators have nonetheless noted definitional and enforcement gaps, including risks of inconsistent application and weak cross-border effectiveness.[38] From the perspective of digital constitutional accountability, the EU's transparency regulation contributes to normative accountability by articulating public standards for online campaigning, and to epistemic accountability by mandating transparency around the sponsors of political messages. However, systemic accountability remains the weakest link: particularly due to insufficient cross-border enforcement, the absence of constitutional oversight mechanisms, and the lack of independent institutional scrutiny.

D. The Double-Edged Sword of Digital Democratization

Expanding on the preceding discussion, a further aspect concerns the widespread diffusion of communication technologies, which has lowered barriers to participation and contributed to more inclusive access to public discourse. However, this democratization of digital spaces is not without risks. It raises legal and normative challenges related to information integrity, the amplification of polarizing content, and the formation of algorithmically reinforced echo chambers. These dynamics increasingly test the limits of existing safeguards on media pluralism, freedom of expression, and informed democratic deliberation.[39] The challenge for governments and parliamentary systems in the 21st century is to navigate these turbulent waters by ensuring that adopting such technologies strengthens democratic principles rather than undermines them. Constitutional resilience in this context demands more than regulatory adaptation: it requires that core democratic principles – such as transparency, pluralism, and rights protection – be structurally embedded into digital infrastructures. This requires enforceable safeguards for pluralism, rights protection, and information integrity.[40] In particular, it requires legal safeguards against systemic disinformation and manipulative content practices, while promoting informational pluralism through enforceable standards for content moderation, algorithmic transparency, and access to diverse sources of information.[41] From a comparative law perspective, analyzing how new technologies reshape constitutional norms and influence political decisions is essential for understanding contemporary developments. Observing how different jurisdictions adopt, modify, and integrate these innovations

38. *See* V. M. R. Allegri, *La Propaganda Elettorale Online fra Regole Vecchie e Nuove*, *in* Il Diritto Della Regione 85-120, 90-1, 95 (Marsilio, 2024); *see also* Giovani De Gregorio & Catalina Goanta, *The Influencer Republic: Monetizing Political Speech on Social Media*, 23 Ger. L. J. 204, 204–206 (2022) (discussing how political speech can also be monetized by social media platforms through sponsorship and advertisement mechanisms).

39. *See* Raffaella Niro, *Piattaforme Digitali e libertà di espressione fra autoregolamentazione e co-regolamentazione: Note ricostruttive*, *in* Giovanni Di Cosimo, Processi Democratici e Tecnologie Digitali 245 (Giappichelli, 2023); García-Marzá & Calvo, *supra* note 5, at 41-42 (2024) (analyzing the algorithmic influence on political decision-making).

40. *See generally* Sheila Jasanoff, The Ethics of Invention: Technology and the Human Future 10 (2016) (arguing that technological progress must be carefully managed to protect democratic governance and human rights).

41. *See generally* Edoardo Celeste, Digital Constitutionalism: The Role of Internet Bills of Rights 175 (2022) (emphasizing the fundamental role of human dignity in digital rights frameworks).

allows us to see how constitutional principles evolve in response to shared global challenges. Each system, in turn, adapts successful approaches from others to suit its unique legal and cultural landscape.

E. Legal Perspectives on Technology's Influence

In academic discourse, many scholars have previously highlighted the normative power of technological infrastructures in shaping social and political behavior.[42] This insight has acquired renewed relevance in the context of AI-driven infrastructures, which increasingly influence the exercise of legal authority and democratic governance. The idea that the *intrinsic architecture of technology* is able to shape governance in a very powerful way serves as a reminder of the profound influence that technological systems hold over social and political life.[43] As these systems evolve, they begin to exert *de facto* regulatory functions: shaping behavior, rights, and institutional interactions without explicit legal mandates. This highlights the growing need to interrogate how technology shapes norms, rights, and democratic processes, a task that has become indispensable for any serious account of constitutional governance in the algorithmic age. A parallel strand of work, often grouped under the label of "algorithmic accountability," has examined how legal and technical design choices can make automated systems auditable and contestable, while at the same time challenging the assumption that transparency, especially disclosure of source code, is a sufficient foundation for accountability in complex socio-technical infrastructures.[44]

Other authors, such as Mireille Hildebrandt, have also explored the implications of artificial intelligence and automation on the principles of legality and fundamental rights.[45] In particular, Hildebrandt argues that AI systems may function as autonomous normative agents, challenging traditional conceptions of governance and sovereignty.[46] Her analysis highlights the need for oversight when regulatory functions are displaced to opaque systems.

In addition, the digitization of decision-making processes – as analyzed by Shoshana Zuboff – has introduced new dynamics of surveillance and control, particularly through the use of predictive algorithms and profiling techniques

---

42. *See, e.g.*, David R. Johnson & David G. Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367 (1996); *see* Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 Tex. L. Rev. 553 (1997); Lawrence Lessig, Code and Other Laws of Cyberspace (Basic Books 1999); Andrew Murray, The Regulation of Cyberspace: Control in the Online Environment (2007); Julie E. Cohen, Configuring the Networked Self: Law, Code, and the Play of Everyday Practice (2012); Giovanni Di Gregorio, *The Normative Power of Artificial Intelligence*, 30 Ind. J. of Global Legal Stud. 55 (2023).

43. *See, e.g.,* Langdon Winner, *Do Artifacts Have Politics?*, 109 Daedalus 122, 128 (1980) (observing that technological innovations, like legislation or political foundings, can set enduring frameworks of public order).

44. *See, e.g.,* Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. Pa L. Rev. 633, 657–60 (2017) (arguing transparency is neither necessary nor sufficient, and detailing technical tools to verify procedural regularity and legal fairness); Ananny & Crawford, *supra* note 34 (identifying ten limits of the transparency ideal and proposing a systemic model of algorithmic accountability).

45. *See* Mireille Hildebrandt, Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology (Cheltenham 2015).

46. *Id.*

based on big data. These technologies enable unprecedented monitoring of individual behavior, transforming personal data into predictive insights that allow organizations and institutions to anticipate and influence actions.[47] The shift toward predictive control challenges traditional boundaries of privacy and autonomy, as algorithmic surveillance and profiling increasingly shape both individual choices and societal norms. Zuboff's theory of surveillance capitalism frames the extraction and monetization of behavioral data not merely as an economic model, but as a transformation of governance. In her account, data-driven prediction operates as a new form of power: one that displaces public institutions by reallocating informational authority to private, transnational actors.[48] From a legal perspective, the asymmetries of knowledge and the opacity of algorithmic systems challenge democratic principles such as transparency, individual informational autonomy, and meaningful participation in public discourse. These dynamics undermine oversight and constitutional accountability. In this context, the economic and informational logic often referred to as "surveillance capitalism"[49] should be examined not only through the lens of data protection, but also as a structural transformation of public power, raising questions of legitimacy and democratic control in the digital environment.

These insights demand a constitutional response: one that ensures that innovation does not erode civil liberties. Scholars like Virginia Eubanks and Jack Balkin have called for greater scrutiny of automated systems in governance: Eubanks has examined how automated systems can perpetuate inequalities and biases,[50] while Balkin has discussed the importance of integrating digital technologies ethically into the political landscape.[51] In particular, Balkin has emphasized that technologies must promote transparency, accountability, and other democratic principles rather than compromise them.[52]

From this overview, it is evident that the doctrinal groundwork for addressing the challenges posed by technology has already been laid, offering a clear path for critical engagement. Technological advancements demand not only an updated interpretation of norms governing the relationship between technology and power structures but also a reaffirmation of foundational legal principles. The task for legislators, policymakers, and legal theorists is to harness this groundwork to guide the impact of emerging technologies within existing constitutional and governance frameworks. These technologies must be understood

47. *See* Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (Public Affairs 2019).

48. *Id.*

49. *Id.*

50. V. Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (Picador 2018).

51. *See* Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, in 51 UC Davis L. Rev. 1149, 1210 (2018).

52. *See* Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. Rev. 1 (2004) (examining the role of digital technologies in public discourse and democratic culture); Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 Minn. L. Rev. 1 (2008) (arguing that emerging technologies need to be regulated in ways that enhance transparency and accountability to prevent the erosion of democratic values).

not simply as instruments of innovation, but as structural forces with profound implications for democratic legitimacy, authority, and public accountability. This necessitates ongoing reflection and a careful, informed adaptation of regulatory frameworks to safeguard democratic values, civil liberties, and the accountability essential for a balanced technological future.

I. The Impact of Digital Technologies on Constitutional Authority in the Algorithmic State

The advancement of artificial intelligence and big data analytics introduces dilemmas for what this Article calls "constitutional authority".[53] Here, "constitutional authority" captures the State's ultimate responsibility for rights-affecting public decisions, even when decision-making is delegated to digital infrastructures or automated systems. These technologies, while offering powerful tools for analysis and policy implementation, also reconfigure where and how rights-affecting decisions are made, thereby intensifying concerns about transparency, accountability, and data governance, which are essential to preserving constitutional authority in a digitized environment.[54] This Article asks how public power can remain constitutionally grounded amid growing algorithmic mediation.

A particularly revealing test case for the Article's account of constitutional authority in the platform-mediated public sphere is Estonia, often cited as a pioneer in e-government and internet voting.[55] The Estonian model exemplifies both the potential and the risks of delegating core state functions to digital infrastructures. While Estonia's digital electoral system has been praised for its accessibility and innovation, it also raises critical constitutional questions opacity, auditability, and democratic legitimacy in electoral processes. [56] From a constitutional perspective, the decisive issue is whether such systems preserve verifiability, public trust, and effective institutional control over voting integrity.[57] Nevertheless, internet voting has attracted sustained criticism from legal scholars, security experts, and political actors, with some jurisdictions - including the Netherlands and Great Britain - having abandoned or ruled out the option

53. *See* Alfredo D'Attorre, *Sovranità Costituzionale e Costituzionalismo dei Diritti dopo Maastricht* [*Constitutional Sovereignty and the Constitutionalism of Rights after Maastricht*], Politica del diritto 385 - 416 (2020); Paolo Bonetti, *Società del Rischio e sovranità costituzionale* [*Risk Society and Constitutional Sovereignty*], Il Mulino 803 (2006). This Article uses "constitutional authority" functionally, to denote the State's ultimate responsibility for rights-affecting decisions in digitally mediated environments.

54. *See* Celeste, *supra* note 41, at 27 (discussing the broader implications of transparency and accountability in digital contexts); García-Marzá & Calvo, *supra* note 5, at 234 (discussing the ethical imperatives of regulating and limiting Big Tech to safeguard democratic transparency).

55. *See* Sven Heiberg, *New Technologies for Democratic Elections*, *in* 132 BPM 2012 Int'l Workshops, Tallinn, Estonia, September 3, 2012, Revised Papers 630 (Marcello Rosa & Pnina Soffer eds., 2013); Ülle Madise & Tarvi Martens, *E-voting in Estonia 2005: The First Practice of Country-Wide Binding Internet Voting in the World, in* P-86 Electronic Voting 2006: Proceedings of the 2nd International Workshop 15 (Robert Krimmer ed., 2006).

56. *See* Isabella Wilkinson, *From Analogue to Digital: An Exploration of Digitizing Elections, Electoral Integrity and Voter Trust,* 18 Democracy & Soc'y 1 (2022).

57. *See* Directorate-General for Justice and Consumers (European Commission), Study on the Benefits and Drawbacks of Remote Voting (2018) [https://perma.cc/DBU8-YD7P].

altogether on the grounds that the electoral process must comply with basic democratic principles and stringent technical standards.[58] For example, it is essential to secure and verify each ballot's integrity and to maintain rigorous oversight over the governance, ownership, hosting, and control of data generated by internet voting systems.[59] Yet the complexity of algorithms and the difficulty of conducting thorough audits can threaten popular sovereignty itself, undermining citizens' ability to understand and trust the systems on which democratic participation depends.

Beyond electronic voting, the growing use of automated systems in core public functions – such as the allocation of public funds, the management of social services, and the development of policy – reflects a broader shift to algorithmic delegation, where key decisions are no longer made through traditional institutional channels but instead by opaque digital infrastructures.[60] This technological shift affects various domains, and challenges democratic oversight at its roots. If left unchecked, such systems may perpetuate opacity, exacerbate inequalities, and erode public trust in democratic institutions. The loss of transparency and traceability in algorithmic processes complicates traditional notions of legitimacy and procedural fairness, especially when citizens cannot understand or contest how decisions are made

Addressing these public challenges requires moving beyond conceptual frameworks[61] to actionable mechanisms. For example, independent algorithm audits in high-stakes public domains — such as voting, justice, and healthcare — could enhance technical transparency and institutional trust.[62] Similarly, embedding democratic values into the design of digital systems through ethical-by-design and privacy-by-design principles can help prevent automation from undermining fundamental rights.[63] These operational levers, in turn, connect to broader debates about how constitutional systems

58. *See* Claudio Novelli & Giulia Sandri, Digital Democracy in the Age of Artificial Intelligence 13-14 (July 22, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4901264 [https://perma.cc/PU39-E5CW].

59. *See id.*; Dimitris A Gritzalis, *Principles and Requirements for a Secure E-Voting System*, 21 Computers & Security 539 (2002).

60. *See* Celeste, *supra* note 41, at 11-14 (describing how humans live in a "virtual ecosystem" and human interactions are "translated into interactions of data").

61. *See, e.g.*, Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 Cal. L. Rev. 513, 513-15 (2015) (arguing that the cyberlaw conceptual toolkit and methods can inform responses to new transformative technologies, including robotics and AI); Karen Yeung, *Algorithmic Regulation: A Critical Interrogation*, 12 Reg. & Governance 505, 505-07 (2018) (defining "algorithmic regulation" and relaying legitimacy concerns raised by data-driven, automated governance); Danielle Keats Citron, *Technological Due Process*, 85 Wash. U. L. Rev. 1249, 1251–53 (2008) (showing how automated decision systems can threaten procedural fairness and require enforceable safeguards); Edoardo Celeste, *Digital Constitutionalism: Mapping the Constitutional Response to Digital Technology's Challenges* 1-4 (Humboldt Inst. for Internet & Soc'y, Discussion Paper No. 2018-02, 2018) (surveying and systematizing heterogeneous strands of "digital constitutionalism," including rights catalogues and normative charters).

62. *See* Narek Andreasyan et al., *Theoretical Framework of Digital Ethics Concerns for Public Services: Electronic Voting Use Case*, *in* 2024 Tenth International Conference on eDemocracy & eGovernment (ICEDEG) 8 (2024).

63. *See* Kjetil Rommetveit & Niels van Dijk, *Privacy Engineering and the Techno-Regulatory Imaginary*, 52 Soc. Stud. Sci. 853, 853-54 (2022).

can retain responsibility for the governance of data-dependent infrastructures. This constitutional-responsibility concern becomes acute in electoral contexts, where bigdata analytics and algorithmic profiling intensify informational asymmetries between citizens and the State. Big data analytics has revolutionized State decision-making through its ability to extract behavioral insights at scale,[64] enabling precise profiling, real-time monitoring, and targeted interventions — but at the cost of increased risks of discrimination, manipulation, and democratic exclusion.[65] Without robust safeguards, profiling can entrench voter bias, distort democratic deliberation,[66] and erode media pluralism.[67]

Across these domains, a comparative analysis between the United States and the European Union reveals diverging regulatory philosophies regarding artificial intelligence and data governance. The United States has historically adopted a more market-driven, innovation-led approach, characterized by fragmented sectoral regulation and limited federal oversight.[68] The European Union, by contrast, has moved toward a rights-based regulatory model, first exemplified by the General Data Protection Regulation (GDPR)[69] and, more recently, by the Artificial Intelligence Act,[70] which establishes a framework for imposing heightened requirements on high-risk AI applications.[71] The GDPR and the AI Act represent significant steps toward rights-based technology governance — but neither fully addresses the constitutional questions of democratic legitimacy and accountability that arise when automated systems make public decisions.[72]

---

64. *See* Jean-Michel Sahut et al., *The Impact of Big Data on Decision-Making, Processes and Organizational Change: An Essay of Synthesis*, 41 Can. J. Admin. Sci. 508, 509 (2024).

65. *See* Maddalena Favaretto et al., *Big Data and Discrimination: Perils, Promises and Solutions — A Systematic Review*, 6 J. Big Data 1, 6-15 (2019).

66. *See* Jacquelyn Burkell et al., *Voting Public: Leveraging Personal Information to Construct Voter Preference*, *in* Big Data, Political Campaigning and the Law 47, 51 (Normann Witzleb, et. al ed., Routledge 2020).

67. Resolution on Fundamental Rights Implications of Big Data: Privacy, Data Protection, Non-Discrimination, Security and Law-Enforcement, Eur. Parl. Doc. 2016/2225(INI), ¶ O (2017).

68. *See* Tatevik Davtyan, *The U.S. Approach to AI Regulation: Federal Laws, Policies, and Strategies Explained*, 16 J.L. Tech. & Internet 223 (2025).

69. Council Regulation 2016/679, Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2016 O.J. (L 119) 1.

70. Council Regulation 2024/1689, Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 1689) 1.

71. *See* Claudio Novelli et al., *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, 16 Eur. J. Risk Reg. 566, 571 (2025).

72. *See generally* Elaine Fahey, The Global Reach of EU Law (Routledge 2016) (analyzing how EU law produces extraterritorial effects); Anu Bradford, *The Brussels Effect,* 107 Nw. U. L. Rev. 1 (2015) (explaining how EU regulation can globalize standards through market mechanisms). *But see also* Marco Almada & Anca Radu, *The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy*, 25 Ger. L.J. 646 (2024) (arguing the AI Act's "Brussels Effect" may inadvertently undermine the EU's export of AI rules and values); Marco Almada & Nicolas Petit, *The EU AI Act: Between the Rock of Product Safety and the Hard Place of Fundamental Rights*, 62 Common Mkt. L. Rev. 85 (2025) (criticizing the AI Act's tension between product-safety logic and fundamental rights).

A. From Digital Sovereignty to Digital Justice: Rethinking Constitutional Reforms in the Age of Technology

Building on the framework introduced in the previous section, this section applies the concept of digital constitutional accountability to assess how democratic institutions respond, or fail to respond, to the growing power of digital infrastructures, particularly when non-state actors exercise such power.

The framework includes three interdependent dimensions: epistemic, normative, and systemic accountability. Here, constitutional accountability refers to enforceable obligations grounded in constitutional principles and addressed to actors who exercise structural power through algorithmic systems. Two conditions mark the scope of this obligation. First, the activity must affect rights in a legally contestable sense or operate as functionally public activity: for example, structuring access to civic discourse, allocating public benefits or burdens, or conditioning participation in democratic processes.[73] Where legal systems do not recognize robust horizontal effect, this threshold does not imply that fundamental rights bind private actors directly; rather it signals constitutional salience and the need for mediated accountability through statute, regulation, or constitutionally informed private-law duties. Second, the activity must use algorithmic systems that create sustained informational asymmetries or displace ordinary institutional checks. When both conditions apply, the claim of constitutional accountability operates in practice: legal systems must provide available determinable duties, cognizable forums, and effective remedies, even if the doctrinal vehicle differs across jurisdictions (for example, U.S. doctrine often relies on state action and forum-based categories).[74]

Read through this lens, the three dimensions ask for concrete things. Epistemic accountability requires advance notice of algorithmic use, intelligible reasons for decisive factors, retention of logs that permit independent verification, and proportionate disclosure under judicial control. In particular, this dimension resonates with proposals in the computer science and law literature that seek to engineer automated systems so that compliance with legal standards can be independently verified, for example through logging, cryptographic commitments and formal verification tools, rather than relying solely on ex post transparency.[75]

---

73. In U.S. constitutional doctrine, even rights-salient private governance will not ordinarily trigger First Amendment duties absent state action (including narrow public-function or attribution theories). *See* Manhattan Cmty. Access Corp. v. Halleck, 139 S. Ct. 1921 (2019) (private forum operator not subject to First Amendment absent those theories); Jackson v. Metro. Edison Co., 419 U.S. 345 (1974) (regulation and monopoly status alone insufficient); Blum v. Yaretsky, 457 U.S. 991 (1982) (no state action without state compulsion or significant encouragement). Under EU law, certain Charter rights may have horizontal effect. *See* Case C-414/16, Egenberger (Grand Chamber), ECLI:EU:C:2018:257 (Arts. 21(1) & 47); Joined Cases C-569/16 & C-570/16, Bauer/Willmeroth (Grand Chamber), ECLI:EU:C:2018:871 (Art. 31(2)).

74. *See, e.g.,* Marco Bassini, *Social Networks as New Public Forums? Enforcing the Rule of Law in the Digital Environment*, 1 Ital. Rev. Int'l & Compar. L. 311 (2022) (discussing the state-action barrier and the turn to "public forum" reasoning based on spatial characteristics); *see also* Biden v. Knight First Amend. Inst. at Columbia Univ., 141 S. Ct. 1220 (2021) (vacating as moot the Second Circuit's public-forum holding).

75. Kroll et al., *supra* note 44, at 662 (developing technical mechanisms such as cryptographic commitments, zero-knowledge proofs and verifiable logging as tools for legal accountability of automated decision systems).

Normative accountability imposes public, determinable rules; reason-giving and non-discrimination in enforcement; and internal appeal backed by external recourse, particularly where platforms perform public-function roles in the speech environment. Systemic accountability requires ex ante risk assessment, registration or prior authorization for high-impact systems, independent audit, and effective remedies for those affected. Because these obligations interact, serious failure on one axis presumptively undermines the others and courts and regulators should assess them holistically.

The adjustment of constitutions to integrate the protection of rights in the digital realm now occupies a central place in both academic and political-institutional debates.[76] Scholars have discussed how digital technologies prompt a reconsideration of traditional rights, with a particular focus on freedom of expression and privacy.[77] In particular, it has been argued that digital constitutionalism must extend beyond state-centered protections to address the quasi-public power exercised by large tech corporations, whose decisions increasingly shape civic space and democratic participation.[78] Yet the digital constitutionalism debate varies widely in scope and ambition, and it often stops at the level of rights-claims, principles, or institutional aspirations, without fully specifying how accountability should be triggered, through which procedures, and with what remedies when private infrastructures exercise functionally public power.[79] This Article's contribution translates the normative ambitions of digital constitutionalism into a structured accountability grammar, designed to be administrable by courts and regulators and adaptable across legal systems.

At the center of this debate, lies the notion of digital sovereignty, a concept that has gained traction in both legal and policy circles.[80] Yet, despite its widespread use, digital sovereignty often lacks a clear definition. Framed as control over infrastructures and data flows, digital sovereignty can obscure the core issue: how rights-affecting digital power, whether public or private, is constrained by constitutional responsibility, institutional checks, and democratic legitimacy. Digital constitutional accountability responds by shifting the focus from control claims to reviewable duties, institutional fora, and effective remedies. Without

76. *See* Celeste, *supra* note 41 (tracing how constitutional frameworks adapt to digital contexts while advocating for specific reforms).

77. *See* De Gregorio & Radu, *Digital Constitutionalism in the New Era of Internet Governance, in* 30 Int'l J.L & Info. Tech. 68, 87 (2022).

78. *Id.; see also* Giovanni De Gregorio, *The Rise of Digital Constitutionalism in the European Union*, 19 Int'l J.Const. L. 41 (2021) ((exploring EU digital constitutionalism and its impact on rights protection); Marco Bassini, *Fundamental Rights and Private Enforcement in the Digital Age*, 25 Eur. L.J. 182 (2019) (describing the shift toward privatized rights enforcement and warning that liability pressure incentivizes the removal of lawful content).

79. *See e.g.,* Marco Bassini, *Speech Without a Speaker: Constitutional Coverage for Generative AI Output?*, 21 Eur. Const. L. Rev. 375 (2025) (noting that "digital constitutionalism" targets private threats while upholding rights as protection against the state, and analyzing EU content moderation distinctions).

80. *See e.g.,* Stéphane Couture & Sophie Toupin, *What Does the Notion of "Sovereignty" Mean When Referring to the Digital?*, 21 New Media & Soc'y 2305–2322 (2019); Julia Pohle & Thorsten Thiel, *Digital Sovereignty*, 9 Internet Policy Rev. (2020; Floridi, *supra* note 3, at 369–378; Edoardo Celeste, *Digital Sovereignty in the EU: Challenges and Future Perspectives*, *in* Federico Fabbrini et al., Data Protection Beyond Borders (Oxford: Hart., 2021); Rocco Bellanova et al., *Digital/Sovereignty and European Security Integration: An Introduction*, 31 Eur. Sec. 337–355 (2022).

this normative grounding, claims of "digital sovereignty" risk becoming rhetorical devices that legitimize discretionary control, rather than a framework for protecting fundamental rights and democratic participation.[81]

The accountability lens clarifies how the rise of new digital actors disrupts existing constitutional categories, demanding targeted adaptations rather than wholesale reinvention. Several authors rightly emphasize the *quasi-public* nature of decisions made by tech corporations, decisions that increasingly shape the conditions of civic discourse and public reasoning, but without being subject to constitutional constraints.[82]

Moreover, a noticeable shift has emerged in Internet governance: increasing fragmentation, polarization, and hybridization are reshaping the architecture of freedom and power online.[83] These dynamics have been strategically leveraged by populist movements, which use digital platforms to disseminate polarizing narratives, delegitimize democratic institutions, and reframe constitutional values in ways that concentrate power.[84] Through digital manipulation of public discourse, these actors seek to present themselves as the sole authentic voice of the people, a moral claim to exclusive representation that the populism literature links to anti-pluralism and to plebiscitarian, majoritarian accounts of popular sovereignty that can erode liberal-democratic constitutional constraints.[85]

Navigating this complex landscape requires not only legal reforms, but also a renewed constitutional sensibility: one that takes seriously the structural changes in how power and participation are configured online. Scholars such as Oreste Pollicino have argued that digital constitutionalism must not limit itself to safeguarding existing rights in digital form; it must actively promote them and respond dynamically to the structural changes in how information is produced, accessed, and controlled.[86]

---

81. *See, e.g.*, Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism 6–7, 267–70 (Oxford Univ. Press 2019) (arguing that unaccountable legal and institutional categories can consolidate control and legitimate informational capitalism); Marketa Trimble, *The Future of Cybertravel: Legal Implications of the Evasion of Geolocation*, 22 Fordham Intell. Prop. Media & Ent. L.J. 567, 569–74 (2012) (discussing how sovereignty rhetoric justifies unaccountable, extraterritorial control over digital environments).

82. *See, e.g.,* Jack M. Balkin, *Information Fiduciaries and the First Amendment,* 49 UC Davis L. Rev. 1183-1234 (2016); Jack M. Balkin, *The Future of Free Expression in a Digital Age,* 36 Pepp. L. Rev. 427 (2009); Cohen, *supra* note 81; Nicolas P. Suzor, Lawless: The Secret Rules That Govern Our Digital Lives (2019); Tarleton Gillespie, Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media (Yale Univ. Press 2018).

83. *See, e.g.*, De Gregorio & Radu, *supra* note 78, at 69-70 (arguing that Internet governance is evolving towards these trends, which not only affect the technical infrastructure but also reshape the architecture of freedom and power in the digital environment).

84. *See* Martinico, *supra* note 25, at 22; Veronesi, *supra* note 22, at 65.

85. *See, e.g.*, Jan-Werner Müller, What Is Populism? 10–11 (Univ. of Pa. Press ed., 2016) (defining populism as anti-pluralist and exclusivist); Cas Mudde & Cristóbal Rovira Kaltwasser, Populism: A Very Short Introduction 6, 16–19, 38 (Oxford Univ. Press ed. 2017) (defining populism as "thin-centered" and in tension with liberal constraints).

86. *See* Oreste Pollicino, Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism? 200 (2021).

In this context, balancing freedom of expression, privacy, and public security has become a central constitutional challenge.[87] While digital technologies can enhance participation and transparency, they also can facilitate new forms of manipulation, surveillance, and power asymmetries. As Jack Balkin has noted, law must harness technology to promote democratic accountability, but only if it is accompanied by substantive limits and institutional safeguards that can resist its misuse.[88]

From a complementary perspective, digital constitutionalism requires a bifocal approach, where both opportunities and risks are equally considered.[89] If algorithm-driven systems are reshaping political communication and decision-making, conventional categories– such as legislative primacy, judicial review, or even popular sovereignty– require severe rethinking.[90] Rather than abandoning these categories, we must reinterpret them through the lenses of algorithmic governance and digital infrastructures.[91] Alongside these structural accountability concerns, digital justice is a complementary strand of digital constitutionalism. It goes beyond access or privacy rights and draws attention to structural inequalities in the digital sphere. This includes the ways in which algorithmic opacity and gatekeeping distribute opportunities and harms. Here, it informs the redistributive and inclusion-oriented stakes of the tripartite model, especially in designing systemic accountability mechanisms. It interrogates not only how rights are recognized in digital settings, but also for whom and under what socio-technical conditions. Proposed digital rights, such as meaningful data portability, platform neutrality, universal access, and algorithmic contestability,[92] must be tied to enforceable guarantees and not symbolic declarations. This Article uses the concept in this limited sense to identify exclusionary effects in existing digital arrangements and to justify corrective institutional design. For these reasons, advancing digital

87. *See* Joseph Cannataci, et al., *Balancing Privacy and Transparency and Redefining Their New Boundaries in the Internet Ecosystem*, *in* Privacy, Free Expression and Transparency: Redefining Their New Boundaries in the Digital Age 88-91 (2016).

88. *See* Balkin, *supra* note 52, at 6-9.

89. *See* Giovanni De Gregorio, Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society 273 (2022) (discussing the necessity of reframing constitutionalism to address the dual aspects of digital technologies, leveraging their potential while mitigating associated risks)

90. *See* Oreste Pollicino & Giovanni De Gregorio, *Constitutional Law in the Algorithmic Society*, *in* Constitutional Challenges in the Algorithmic Society 3-24 (H.-W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, G. De Gregorio eds., 2021).

91. *See* Ming-Sung Kuo, *Against Instantaneous Democracy*, 17 Int'l J. Const. L. 554, 561, 571 (2019).

92. Algorithmic contestability refers to mechanisms enabling affected individuals to challenge and seek redress for automated decisions. *See, e.g.*, Daniel N. Kluttz et al., *Shaping Our Tools: Contestability as a Means to Promote Responsible Algorithmic Decision Making in the Professions*, *in* After the Digital Tornado: Networks, Algorithms, Humanity 137, 137–52 (Kevin Werbach ed., 2020); Henrietta Lyons et al., Conceptualising Contestability: Perspectives on Contesting Algorithmic Decisions (2021); 5 Proceedings of the ACM on Human-Computer Interaction 1-25 (2021); Clément Henin & Daniel Le Métayer, *Beyond Explainability: Justifiability and Contestability of Algorithmic Decision Systems*, 37 AI & Soc'y. 1397–1410 (2022).

constitutionalism requires adaptive governance tools, such as sunset clauses, mandatory impact assessments, and independent oversight bodies with technical expertise. Without such adaptability, constitutional law may lose its normative traction in the digital environment. But if redefined with accountability at its core, it can remain a powerful instrument to preserve democratic legitimacy in an age of algorithmic power.

B. Reconceptualizing Constitutional Accountability: A Three-Dimensional Framework for the Algorithmic Age

In order to give analytical precision to the concept of digital constitutional accountability, this Article proposes a tripartite framework that identifies the key domains where constitutional oversight must evolve in response to emerging digital powers. Unlike traditional forms of accountability, which are often grounded in state-centric models, this framework addresses the hybrid, decentralized, and infrastructural nature of power in the digital environment.[93]

In order to formalize and systematize the framework already outlined, this subsection sets out a tripartite structure. Rather than classifying accountability mechanisms by actor or channel, it identifies three functional dimensions that reflect the distinct normative pressures emerging from algorithmic governance. This model distinguishes among the following three interdependent dimensions:[94]

> Epistemic Accountability: Who controls the visibility, accessibility, and prioritization of information in the digital public sphere? This dimension concerns algorithmic curation, recommendation systems, and ranking mechanisms that mediate access to knowledge while shaping the conditions for public discourse. It highlights the increasing epistemic authority exercised by platforms without transparency or public justification.
>
> Normative Accountability: Who decides what forms of expression are permissible, and based on which values, norms, or legal standards? This includes the rule-making and enforcement mechanisms of private platforms: content moderation policies, community guidelines, algorithmic filtering of speech, and the automation of norm enforcement. It raises fundamental concerns about legitimacy, pluralism, and due process in environments governed by non-state actors.
>
> Systemic Accountability: What legal and institutional structures ensure that digital infrastructures are embedded within broader constitutional architectures of rights protection, democratic legitimacy, and checks and balances? This dimension captures the role of courts, parliaments, regulators, and public oversight bodies in subjecting digital power to constitutional constraints and enabling institutional contestation.

This tripartite model of digital constitutional accountability departs from classical theories of democratic accountability, yet the model remains in implicit dialogue with these theories. Constitutional accountability traditionally implies

93. While various scholars have addressed epistemic, normative, or institutional concerns separately (e.g. SUZOR, *supra* note 82), this tripartite model integrates these strands into one constitutional framework.

94. While much has been written on digital legitimacy and accountability, existing frameworks often focus on sectoral or disciplinary logics. This model bridges normative theory and constitutional analysis.

the obligation of public authorities to justify their actions to institutions or bodies with the power to impose sanctions or corrective measures.[95] It is generally premised on a recognizable institutional structure and a clear allocation of responsibilities within the state. The originality of the proposed framework lies in extending this notion beyond public institutions, explicitly including private algorithmic infrastructures and platforms within constitutionally grounded accountability pathways, through jurisdiction-specific doctrinal routes (including direct or indirect horizontal effect, statutory duties, and mediated attribution frameworks) that translate constitutional values into enforceable obligations.[96] For instance, Mark Bovens' well-known tripartite distinction between vertical, horizontal, and diagonal accountability (respectively referring to electoral mechanisms, checks among institutional powers, and civil society oversight) assumes a relatively stable and recognizable institutional architecture.[97] By contrast, the framework advanced here does not classify channels of accountability. It instead identifies the functional dimensions of algorithmic power (epistemic, normative, and systemic) which often lack adequate mechanisms of control or legitimacy. In this sense, the model reframes the accountability question from who is held accountable todetermining which types of constitutional responsibility platforms and algorithmic systems should be held to account in the first place. Here, "constitutional responsibility" refers to the duty to ensure that rights-affecting decisions remain attributable and contestable within institutional pathways capable of supplying legal justification, procedural guarantees, and effective remedies, even when decision-making is mediated by private digital infrastructures.

Similarly, the framework diverges from Pierre Rosanvallon's account of counter-democracy. This separationhighlights the growing role of societal vigilance, monitoring, and distributed forms of legitimacy in democratic life.[98] While insightful, this perspective assumes that such distributed controls can still operate effectively. The present model suggests that in environments structured by opaque and privatized infrastructures of visibility and norm-setting, even these diffuse forms of accountability become ineffective. Neither institutional oversight nor civic vigilance can function properly without transparency, intelligibility, and enforceable standards. As such, this framework calls for a reconstruction of constitutional categories capable of addressing not only the absence

95. *See, e.g.*, Mark Bovens, *Analysing and Assessing Accountability: A Conceptual Framework*, 13 Eur. L.J. 447, 450-57 (2007)(distinguishing accountability as virtue vs mechanism and proposing information/debate/consequences); Richard Mulgan, "*Accountability*": *An Ever-Expanding Concept?*, 78 Pub. Admin. 555, 556–58 (2000) (defining accountability as answerability to those who can question and sanction).

96. *See, e.g.*, Stephen Gardbaum, *The "Horizontal Effect" of Constitutional Rights*, 102 Mich. L. Rev. 387, 390–95 (2003) (mapping direct and indirect models through which constitutional rights shape private relationships); Case C-414/16, Egenberger v. Evangelisches Werk für Diakonie und Entwicklung eV, EU:C:2018:257, §§ 76–79 (Apr. 17, 2018) (holding that Charter Arts. 21 and 47 are sufficient in themselves to be relied on "in disputes between" private parties and that national courts must disapply contrary national law).

97. *See* Bovens, *supra* note 95, at 458; Mark Bovens et al., The Oxford Handbook of Public Accountability 1, 3-6 (Mark Bovens et al. eds., 2014).

98. *See* Pierre Rosanvallon, Counter-Democracy: Politics in an Age of Distrust (Arthur Goldhammer trans., 2008) (arguing that new forms of democratic legitimacy emerge through practices of oversight, prevention, and judgment exercised by citizens outside electoral processes)

of traditional democratic controls, but also the invisibility and infrastructural nature of digital power itself.

This tripartite articulation has not been systematically integrated in this way within constitutional theory. Rather than offering a mere summary of existing categories, it develops an original constitutional framework designed to capture the distinctive modalities through which digital power operates. It constitutes a normative and analytical contribution to diagnose the distinct forms of power and legitimacy at stake in digital environments. In particular, this framework offers the advantage of articulating a systematic distinction that connects the production and accessibility of knowledge (epistemic level), private norm-setting and content governance (normative level), and the absence or weakness of institutional oversight (systemic level), within a unified and coherent constitutional structure designed to guide legal analysis. This integrated model addresses a gap in existing scholarship, where these dimensions are often examined in isolation or through sectoral lenses. Together, these three axes allow for a multi-level diagnosis of accountability failures in the digital sphere. In particular, they enable us to distinguish between a lack of transparency in algorithmic curation (epistemic), a failure of legitimacy in content regulation (normative), and the absence of judicial or democratic review (systemic). The case studies below apply the framework to identify where accountability breakdowns occur and which remedies are institutionally plausible.

More broadly, this tripartite model operationalizes digital constitutionalism in a context where traditional categories (e.g., public/private, state/market) are increasingly blurred. It moves beyond abstract principles and provides a functional grammar to assess power, responsibility, and legitimacy in the algorithmic age.

The proposed three-dimensional framework of digital constitutional accountability offers a more comprehensive and integrated response to the challenges of the algorithmic society than previous models. While earlier approaches often focused on single aspects – such as transparency,[99] ethical design,[100] or legal rulemaking[101] – this framework articulates how epistemic, normative, and systemic dimensions must operate cohesively to ensure constitutional accountability in digital environments. For instance, some recent literature develop technologically oriented models of algorithmic accountability centered on verifiable compliance with legal standards, while other literature reconstructs the transparency ideal and demonstrate its limits as a singular strategy for governing algorithmic systems.[102] In contrast, the framework advanced in this Article integrates transparency and technical verifiability within

99. *See* Zuboff, *supra* note 47, at 190-95 (on epistemic asymmetries and opacity); Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information 16 (Harvard University Press 2015) (on opacity and information asymmetry).

100. *See*, *e.g.*, Luciano Floridi et al., *AI 4 People's Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations,* 4People (2018), https://ai4people.org/PDF/AI4People_Ethical_Framework_For_A_Good_AI_Society.pdf [https://perma.cc/5DJ4-HDWL] (proposing an ethical AI framework of beneficence, non-maleficence, justice, and explicability that lacks formal enforcement mechanisms).

101. See *generally* Lessig, *supra* note 42 (arguing that "code is law" because software architecture regulates cyberspace).

102. *See e.g.* Kroll et al., *supra* note 44; Ananny & Crawford, *supra* note 34.

a broader constitutional structure that also specifies normative standards and systemic institutional checks.

The framework is especially suited to the algorithmic society,[103] where power is simultaneously epistemic (e.g., Who knows what? Who controls visibility and prioritization of knowledge?), normative (e.g., Who sets and enforces behavioral standards? Based on which values?), and systemic (e.g., How are oversight mechanisms and institutional counterbalances organized in a global and privatized infrastructure?). An adequate accountability regime must therefore respond to all three dimensions simultaneously, rather than sequentially or in isolation.

Partial responses, however well-intentioned, are prone to failure. As Shoshana Zuboff argues in The Age of Surveillance Capitalism,[104] transparency alone is insufficient when power asymmetries are so extreme that users lack any real understanding of, or leverage over, the mechanisms that govern their behavior. Likewise, in his work on AI ethics, Luciano Floridi emphasizes the importance of embedding normative principles such as fairness, beneficence, and explicability into the design of algorithmic systems; however, the framework shows that such principles also require enforceability and institutional support.[105] Even where such principles are widely endorsed, their practical impact depends on translation into determinate legal duties, measurable compliance criteria, and reviewable decision-making procedures. This is so that "fairness" or "explicability" can be assessed, contested, and remedied rather than remaining merely aspirational. Similarly, Julie Cohen critiques legal models that rely solely on user consent or formalistic transparency, arguing that they are easily circumvented or co-opted in the current data-driven economy.[106] Lawrence Lessig's seminal claim that "code is law" rightly emphasized the normative function of technical architectures, but offered limited tools for systemic institutional accountability beyond the regulatory choices of coders and platform designers.[107]

This framework is distinguishable because of its emphasis on structural interdependence. Epistemic accountability (e.g., transparency, intelligibility, auditability) enables legal contestation and institutional oversight; normative accountability (rules, rights, obligations) generates enforceable standards and legitimates the demand for transparency; systemic accountability (e.g., governance structures, institutional checks) ensures both transparency and

103. *See* Jack M. Balkin, *The Three Laws of Robotics in the Age of Big Data*, 78 Ohio St. L.J. 1217, 1219-1220 (2018) (coining "algorithmic society" to describe social ordering shaped by predictive analytics and machine learning and urging new constitutional oversight of private information intermediaries).

104. *See* Zuboff, *supra* note 47, at 16, 123 (arguing that surveillance capitalism creates knowledge/power asymmetries that transparency cannot remedy).

105. *See* Floridi et al., *supra* note 100, at 696–700.

106. *See* Cohen, *supra* note 81, at 14–18, 104–110 (critiquing liberal frameworks' reliance on consent and transparency, and showing their inadequacy for governing infrastructural, data-driven power)

107. *See* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 Harv. L. Rev. 501 (1999); Lessig, *supra* note 42, at 6-8 (arguing that "code is law" and the regulatory force of technical architecture).

norm-enforcement are continuously monitored, adapted, and legitimized.[108] These dimensions are not merely additive: they are mutually reinforcing. A deficiency in one undermines the efficacy of the others. Epistemic opacity reinforces normative evasion; without systemic oversight, both persist unchecked.

Therefore, this framework addresses a critical shortcoming in previous models: the lack of integration across these domains. Zuboff's emphasis on epistemic asymmetry, Cohen's call for rethinking legal categories, Floridi's ethical principles for AI, and Lessig's architectural regulation all point to essential facets of digital accountability. Yet, none of these, individually, offer a model for how these dimensions interact and reinforce each other in practice.

Moreover, this framework introduces a dynamic, iterative element by incorporating an accountability learning cycle. Epistemic accountability requires continuous monitoring and algorithmic audits. Normative accountability demands the updating of legal standards as technologies and risks evolve. Systemic accountability ensures that this process occurs inclusively, with proper checks and balances, and across both public and private spheres. In contrast to rigid, static, or one-dimensional approaches, this model supports the creation of a robust and adaptive accountability ecosystem, designed to remain administrable over time by calibrating the intensity of oversight to risk and scale, and by relying on periodic review rather than continuous scrutiny across the board.[109]

This three-dimensional framework offers a structured yet flexible lens through which to confront the evolving challenges of algorithmic power. By merging concerns around transparency, normative legitimacy, and institutional oversight, it articulates not merely a critique, but a constitutional structure suited to the algorithmic information environment. Rather than reinforcing the familiar dichotomy between state regulation and self-regulation, the model envisions a distributed architecture of responsibility, shared among designers, corporations, regulators, courts, and users alike. In a landscape shaped by invisible infrastructures and shifting boundaries of authority, sustaining democratic legitimacy will depend on this kind of multi-level and interdependent accountability.

The three dimensions are analytically distinct, yet deeply interdependent. Recognizing this duality is essential for avoiding fragmented interventions and for structuring coherent legal reforms. While each axis of accountability targets a specific facet of digital power, they function dialectically. Epistemic accountability is foundational; without access to reliable knowledge about algorithmic decision-making, neither normative oversight nor systemic redress can function effectively. Similarly, the absence of normative standards — such as transparency obligations or redress mechanisms — hampers the institutionalization of systemic checks, including judicial or parliamentary review. Conversely, a

---

108. *See* Case C-203/22, *CK v. Magistrat der Stadt Wien* (Dun & Bradstreet Austria GmbH intervening), EU:C:2025:117, ¶ ¶ 55–58 (linking "meaningful information" to effective contestation), ¶ ¶74–75 (requiring balancing, including trade secrets, to determine access).

109. The learning cycle relies on tiered triggers and supervisory prioritization, not permanent auditing, targeting heightened duties where algorithmic mediation creates sustained asymmetries. *Cf.* Commission Regulation 2022/2065, Digital Services Act, 2022 O.J. (L 277) 1, arts. 33(1), 34(1)– (2), 35(1), 37(1) (VLOPs/VLOSEs; risk assessments; mitigation; independent audits); Commission Regulation 2024/1698, AI Act, O.J. (L) 2024/1689 (July 12, 2024), recital 26, art. 72(1)–(3) (post-market monitoring for high-risk AI).

failure to establish robust systemic mechanisms, one capable of monitoring, enforcing, and adapting legal responses, leaves both epistemic and normative advances vulnerable to capture or obsolescence.

As such, the model is not merely additive, but also structurally integrated: a deficiency in one dimension undermines the efficacy and legitimacy of the others. Recognizing this mutual dependency reinforces the need for a constitutional response that is not only multidimensional in theory, but also integrated in institutional practice.

Building on this structural interdependence, the framework's analytical strength also depends on anchoring each dimension to the institutional actors and mechanisms capable of sustaining it in practice. Epistemic accountability calls for the involvement of algorithmic auditors, transparency bodies, and data protection authorities.[110] Normative accountability rests on the role of regulators, standard-setting institutions, and courts in adjudicating the legitimacy of platform governance. Systemic accountability, in turn, engages legislative oversight, constitutional review, and transnational mechanisms of institutional counterpower. Without this institutional mapping, the framework risks remaining a compelling normative schema without actionable relevance, too abstract to serve as a constitutional tool for managing digital power. To make the operational implications explicit, Table 1 (annexed) provides a baseline mapping of each accountability dimension to the main institutional actors, legal tools, and remedial pathways through which accountability can be triggered in practice.

This mapping is intentionally basic and jurisdiction-sensitive: legal systems differ on the doctrinal route through which these actors can be empowered, and on the permissible intensity of constraints on platform governance. The table therefore does not posit a single institutional design; rather, it clarifies the menu of forums, tools, and remedies through which each accountability deficit can be made administrable. The case studies discussed later in this Article draw on this map to show how different pathways become available, or foreclosed, depending on domestic constitutional constraints and regulatory architecture.

Grounded in a comparative and interdisciplinary analysis, this framework also responds to notable gaps in constitutional doctrine across jurisdictions. In the U.S., despite growing concern over platform governance, surveillance, and algorithmic discrimination, courts and scholars lack a cohesive conceptual structure to diagnose systemic digital power. European legal systems, in contrast, have been more proactive in developing regulatory instruments, but they still sometimes fail to integrate these interventions into a coherent constitutional logic. The tripartite model proposed here helps bridge these gaps by offering a structured and normatively grounded approach to articulating constitutional accountability in the algorithmic age.

110. *See, e.g.,* Commission Regulation 2022/2065, Digital Services Act, 2022 O.J. (L 277) 1, arts. 37 (independent annual audits for VLOPs/VLOSEs), 42 (enhanced transparency reporting for VLOPs/VLOSEs), 40 (access to data for supervision and compliance monitoring, including vettedresearcher mechanisms), & 49 (Digital Services Coordinators as national supervisory authorities); *see generally* Commission Regulation 2016/679, General Data Protection Regulation, 2022 O.J. (L 277) 1, art. 51 (independent supervisory authorities), 2016 O.J. (L 119) 1 (EU)

The next subsection clarifies the framework's limits and scope conditions; the case-study section (Section III) then operationalizes the model through concrete contexts, including platform content moderation, AI-driven political microtargeting, and institutional responses to disinformation, to illustrate how digital infrastructures disrupt traditional mechanisms of democratic participation.

1. 'Limits and Scope Conditions (Comparative Constraints)

The tripartite framework is a constitutional-accountability model for diagnosing and structuring responses to algorithmic power. It does not assume that private platforms are automatically bound by constitutional law in the same way as public authorities, nor does it treat constitutional litigation as the exclusive, or even primary, vehicle for disciplining platform governance. Instead, it identifies forms of private power that implicate constitutional values, namely epistemic control over visibility, private norm-setting and enforcement, and institutional displacement, and then asks which legal pathways can translate those values into enforceable duties within a given jurisdiction.

Accordingly, the framework operates at two levels. First, it is diagnostic: it specifies how algorithmic systems may undermine democratic legitimacy by distorting visibility (epistemic), privatizing rule-enforcement (normative), or bypassing public checks (systemic). Second, it is institutional: it maps the kinds of forums and remedies that can restore accountability, such as courts, regulators, parliaments, and independent audit bodies, while keeping open the jurisdiction-specific doctrinal route through which those forums are empowered.

This distinction matters because constitutional systems diverge on both the permissibility and the form of constraints on speech and on intermediary governance. In the United States, doctrines such as the state-action barrier[111] and the First Amendment[112] often narrow the scope for direct constitutional duties owed by private platforms. Accountability may therefore be mediated through statutory design, competition and consumer protection law, administrative oversight, or through private-law and statutory mechanisms that give effect to public-law values without formally treating the platform as a constitutional actor. In the European Union, by contrast, a rights-oriented regulatory tradition more readily supports ex ante legislative obligations for dominant intermediaries, backed by administrative enforcement and judicial review.[113] The framework is compatible with both approaches. It does not resolve contested doctrine, but clarifies which accountability deficits remain legally relevant in each system and where doctrinal resistance generates predictable blind spots.

Finally, the framework is not intended to provide a single test for when a platform becomes "public" or "private." It instead proposes scope triggers that

111. *See e.g.,* Manhattan Cmty. Access Corp. v. Halleck, 587 U.S. 802 (2019); Blum v. Yaretsky, 457 U.S. 991 (1982); Lugar v. Edmondson Oil Co., 457 U.S. 922 (1982).

112. *See generally* Miami Herald Publ'g Co. v. Tornillo, 418 U.S. 241 (1974).

113. *See e.g.,* Commission Regulation 2022/2065, Digital Services Act, 2022 O.J. (L 277) 1; Commission Regulation 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance) OJ L 265, 12.10.2022, p. 1–66.

should be assessed cumulatively and contextually, including functional indispensability for civic participation, gatekeeping power over visibility at scale, and high-impact effects on rights and democratic processes. Where these indicators converge, baseline safeguards become constitutionally salient, such as publicly accessible rules, reason-giving, non-discrimination standards, accessible review mechanisms, and independent oversight for high-impact measures. These safeguards may be implemented through constitutional adjudication, legislation, administrative enforcement, or hybrid public–private oversight structures.

With these scope conditions in view, the next subsection shows how each accountability dimension already appears, in fragmentary form, in constitutional and regulatory practice, and why integration remains incomplete.

C. From Framework to Reform: Towards a Constitutionally Grounded Agenda

The analytical framework presented above offers more than a theoretical lens: it seeks to inform a constitutionally grounded agenda for addressing the democratic implications of algorithmic governance. Each dimension of accountability – epistemic, normative, and systemic – identifies distinct institutional challenges and suggests targeted reform pathways. While the model remains broadly applicable across different jurisdictions and legal traditions, it precisely identifies the critical vulnerabilities in constitutional orders confronted with the governance of digital infrastructures and algorithmic decision-making.[114] The proposals that follow are framed to be reviewable: each specifies a duty, identifies a forum, and indicates an effective remedy. Because the dimensions are mutually reinforcing, partial compliance confined to a single axis should count as a presumptive failure where it frustrates contestation or oversight across the others.

Epistemic accountability demands legal mechanisms and institutions capable of ensuring transparency, intelligibility, and auditability of algorithmic processes. Practical interventions could include mandatory disclosure obligations for recommendation and content-ranking systems, public algorithm registries, and the establishment of independent algorithmic auditing authorities or dedicated transparency boards. Such interventions, whether embedded in data protection regimes, media regulations, or freedom of information laws, must be constitutionally anchored to effectively safeguard democratic legitimacy.

Normative accountability requires addressing the extensive delegation of rule-making and enforcement functions to private digital platforms. Legal systems must introduce clearly defined principles and procedural standards subjecting private platform moderation to public values such as legality, pluralism, due process, and non-discrimination. Potential reform strategies could include adapting administrative law doctrines to private actors, improving access to judicial or administrative remedies, and establishing hybrid public-private oversight bodies. Recent regulatory experiences in jurisdictions such as Germany

114. Here, "digital infrastructures" refers to socio-technical systems (platforms, recommender systems, and data pipelines).

(NetzDG – Network Enforcement Act),[115] Brazil (Marco Civil da Internet),[116] and the European Union (Digital Services Act)[117] highlight both the urgency and feasibility of statutory frameworks designed to regulate content moderation and address online harms.[118] These initiatives establish important procedural obligations – such as notice-and-action systems, transparency reporting, and complaint mechanisms – that begin to structure private platform governance in line with public law principles. However, their normative integration into constitutional architectures remains uneven, as many of these frameworks stop short of articulating clear constitutional mandates for legitimacy, pluralism, and due process. Further legal development is therefore needed to ensure that such regulatory models are not merely pragmatic tools, but vehicles for reinforcing democratic values within digital governance.

Systemic accountability addresses the broader constitutional infrastructure needed to manage hybrid and transnational digital power. Reconstructing institutional balances requires equipping parliaments, courts, and regulatory authorities with enhanced tools to scrutinize privatized norm-setting functions. Possible measures include parliamentary procedures for algorithm review, creation of constitutional or quasi-constitutional oversight bodies specifically dedicated to digital governance, and transnational frameworks facilitating institutional counterbalances to platform dominance. Each dimension of the proposed framework carries distinct normative implications: epistemic accountability calls for constitutional recognition of transparency rights, normative accountability demands clearer doctrinal criteria for private governance in digital spaces, and systemic accountability necessitates explicit constitutional mandates for institutions overseeing digital platforms. Such normative clarifications are crucial for grounding reforms in solid constitutional theory rather than mere regulatory pragmatism.

These dimensions are, above all, interdependent. Partial reforms focused solely on transparency or content moderation standards risk remaining ineffective without comprehensive institutional oversight. The three-dimensional accountability model thus provides a systemic blueprint, explicitly designed to guide integrated reforms rather than piecemeal interventions. However, implementing such a blueprint faces substantial obstacles, particularly in transnational contexts where jurisdictional mismatches and forum shopping undermine coordinated oversight. For example, algorithmic audit requirements may vary across jurisdictions, allowing dominant platforms to strategically locate governance functions in regulatory havens. To address this, constitutional reform proposals should explore bilateral algorithmic audit treaties, EU-level joint enforcement

115. Network Enforcement Act (Netzwerkdurchsetzungsgesetz, NetzDG) (2017), https://www.gesetze-im-internet.de/netzdg/ [https://perma.cc/F4EY-TGJN]

116. Lei No. 12.965, de 23 de Abril de 2014, Diário Oficial da União de 24.4.2014 (Braz.).

117. Digital Services Act, *supra* note 113.

118. The limits of expedited takedown models are illustrated by France's "Loi Avia," Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet, JORF n° 0156 du 25 juin 2020, texte n° 1 (Fr.): the Conseil constitutionnel struck down key provisions because the scheme incentivized over-removal and disproportionately restricted free expression. *See* Cons. const. decision No. 2020-801 DC, June 18, 2020 (Fr.); *see also* Brunessen Bertrand & Jean Sirinelli, Le Conseil constitutionnel et la liberté d'expression et de communication: la voie étroite de la lutte contre les discours de haine sur internet, 10 Dalloz IP/IT 577–83 (Oct. 2020).

task forces, or model laws enabling cross-border recognition of algorithmic impact assessments.

The model's practical applicability extends beyond purely constitutional domains. In a recent policy study authored for the European Parliament, this tripartite framework enabled the identification of specific accountability deficits in the context of generative AI and copyright. Despite its sector-specific focus, the model effectively highlighted key regulatory blind spots, such as the epistemic opacity surrounding AI training datasets, normative uncertainties regarding authorship and ownership, and systemic inadequacies in institutional oversight mechanisms.[119] This practical application of the framework revealed its ability to guide legal diagnosis across distinct regulatory layers. Rather than remaining a theoretical abstraction, the model served to illuminate how algorithmic governance reconfigures the foundational conditions for legal accountability, offering an integrated reading of informational asymmetries (epistemic), norm diffusion (normative), and institutional fragmentation (systemic) in a complex policy environment like the regulation of generative AI.[120]

This section does not claim to provide an exhaustive blueprint for reform. Instead, it illustrates how a functional, constitutionally anchored understanding of digital accountability can support legal systems – in any jurisdiction – in identifying normative priorities, addressing institutional deficits, and fostering innovative legal solutions. The goal is precisely to transcend abstract conceptualization and move towards an actionable, constitutionally coherent response to the complex and evolving challenges posed by algorithmic governance.

D. Grounding the Framework: Jurisprudential Insights into Digital Constitutional Accountability

The following decisions illustrate how each axis already surfaces, in fragmentary form, within contemporary constitutional jurisprudence. While the tripartite model of epistemic, normative, and systemic accountability is presented as a normative framework for conceptualising constitutional responsibility in the algorithmic age, its analytical coherence is reinforced by existing case law.[121] Courts across jurisdictions have begun to articulate constitutional responses to digital power, addressing issues from algorithmic opacity to private regulation of online speech, and institutional oversight of digital infrastructures. These developments provide jurisprudential grounding for the proposed accountability dimensions, suggesting that they reflect evolving constitutional commitments rather than merely theoretical constructs.

The epistemic dimension of constitutional protection – emphasising transparency, auditability, and intelligibility in algorithmic governance – has

119. *See* Nicola Lucchi, *Generative AI & Copyright: Training, Creation, Regulation,* EU Parliament (July 2025), https://www.europarl.europa.eu/RegData/etudes/STUD/2025/774095/IUST_STU(2025)774095_EN.pdf [https://perma.cc/G8VQ-7ZNM].

120. *Id.*

121. As used in this Article, "constitutional responsibility" is a functional term. It refers to responsibility for keeping rights-affecting decisions attributable and contestable through legally determinable duties, accessible institutional fora, and effective remedies, even when decision-making is mediated by private digital infrastructures. It captures the allocation of enforceable duties and remedies through jurisdiction-specific doctrinal routes.

found recognition in several constitutional decisions. In particular, these judicial developments mirror concerns expressed in the algorithmic accountability literature, which underscores both the need for intelligible explanations and the limits of transparency understood as mere disclosure of code or data.[122]

A landmark example is the German Federal Constitutional Court's judgment in Right to be Forgotten I (1 BvR 16/13, 2019).[123] Building on its doctrine of informational self-determination, the Court held that personal data processing which affects fundamental rights must be transparent and open to contestation. Applied to algorithmic or automated decision-making, this principle implies that such systems must be designed and operated in ways that allow those affected to understand and challenge their outcomes, thereby safeguarding individual autonomy and the democratic legitimacy of the constitutional order. Doctrinally, the decision is best read to require that processing which materially affects fundamental rights be transparent and contestable. Applied to algorithmic decision-making, affected persons must receive an intelligible account of the determinants of an outcome sufficient to enable meaningful challenge. Where public authorities rely on outputs supplied by private platforms or vendors, the ability to understand and contest must be contractually secured as a condition of lawful reliance; absent such guarantees, the decision lacks the minimum conditions of legality.

Similarly, in Decision n° 2018-765 DC (2018), the French Constitutional Council upheld provisions permitting certain individual administrative decisions to be based exclusively on an algorithm, but only under strict safeguards.[124] These include an obligation to disclose that the decision is algorithmically generated, to communicate the algorithm's main characteristics in an intelligible form upon request, to ensure the availability of judicial and administrative review, and to maintain human oversight to prevent the algorithm from autonomously modifying its own rules. The reference to "main characteristics" requires disclosure sufficient to make the decision intelligible and reviewable under judicial control. Failure to provide this minimum intelligibility renders the decision effectively unreviewable and warrants annulment or remittal with disclosure under judicial control. These guarantees embed transparency, intelligibility, and reviewability as constitutional requirements, reflecting the epistemic dimension of constitutional protection by ensuring that algorithmic governance remains understandable, accountable, and open to effective challenge. These judgments underscore that constitutional guarantees traditionally applied to human decision-making extend explicitly to algorithmic governance. In particular, both judgments affirm what can be described as the epistemic accountability dimension of constitutional protection, requiring that algorithmic decision-making processes

122. *See, e.g.,* Kroll et al., *supra* note 44 (criticizing source-code disclosure as neither necessary nor sufficient for accountability); Ananny & Crawford, *supra* note 34 (arguing that transparency must be situated within relational and infrastructural conditions of accountability).

123. *See* Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], *Order of 6 November 2019*, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2019/11/rs20191106_1bvr001613en [https://perma.cc/ZXH3-FPL2] (last visited Apr. 17, 2026) (Nov. 27, 2019), (Ger.), http://www.bverfg.de/e/rs20191106_1bvr001613en.html.

124. *See* Conseil constitutionnel [CC] [Constitutional Court] decision No. 2018-765 DC, June 12, 2018, Nos. 65-72 (Fr.), https://www.conseil-constitutionnel.fr/en/decision/2018/2018765DC.htm. [https://perma.cc/Z5DE-KUVU]

remain knowable, contestable, and subject to effective legal oversight. At the administrative level, a notable example is also the Italian Council of State's decision no. 881/2020, which annulled the use of an opaque algorithm in the allocation of public teaching positions.[125] The Court underscored that algorithmic decision-making by public authorities must be intelligible, auditable, and subject to judicial scrutiny. It reasoned that algorithmic opacity violates the constitutional principles of transparency and equality by preventing individuals from understanding and challenging decisions that affect them. Moreover, this ruling reinforces the epistemic accountability dimension by affirming that legal validity in algorithmic governance hinges on visibility, auditability, and contestability. Generalizing the holding, intelligibility and auditability are conditions of legality wherever public functions are performed through algorithms. That condition entails: a clear legal basis; ex ante documentation of data sources, feature selection, and risk assessment; ex post access to code or logic for court-appointed experts under confidentiality; and a human fallback for exceptional cases. Courts should presume invalidity where an authority cannot demonstrate that the system permits effective review.

The normative accountability dimension focuses on legitimacy, due process, and pluralism within private digital regulation. As anticipated by the framework's limits and scope conditions set out above (§2.2.1), the point here is not that platforms are automatically constitutional actors, but that certain forms of platform power become constitutionally salient and therefore demand legally enforceable accountability through the pathways available in the jurisdiction. A key illustration of the normative accountability dimension can be found in *Packingham v. North Carolina* (582 U.S. 98, 2017).[126] In this decision, the U.S. Supreme Court struck down a state law that barred registered sex offenders from accessing social media platforms, holding that such a broad prohibition violated the First Amendment. Writing for the majority, Justice Kennedy emphasized that social media platforms had become the "modern public square," essential for political and civic discourse, as well as for accessing news, employment, and everyday communication.[127] The decision nonetheless underscores the constitutional stakes of platform-mediated access to public discourse, highlighting the urgency of ensuring legitimacy, procedural fairness, and pluralism in the governance of online speech. In light of this decision, when private platforms structure the conditions of public discourse, constitutional values mediate private law. Concretely applying the cumulative scope triggers described in §2.2.1 to this doctrinal setting, a practical threshold for treating platform decisions as public-function-like is met where several indicators converge: functional indispensability as a venue for civic participation; gatekeeping power over visibility at scale; de facto dominance in the relevant forum; state reliance on platform processes for public communication or enforcement; or delegated tasks with public-law effects. In such settings, certain baseline guarantees follow: publicly accessible rules, reason-giving,

125. Cons. di Stato, sez. VI, 13 Feb. 2020, n. 881 (It.) (Requiring transparency, contestability, and intelligibility for algorithmic allocation of teaching posts).

126. 137 S. Ct. 1730 (2017).

127. *Id.*at 1737.

non-discrimination, internal appeal backed by external recourse, and independent review for high-impact sanctions (e.g., account termination affecting public-interest speakers). Consistently with the limits clarified in §2.2.1, this line of argument does not convert platforms into state actors under U.S. doctrine. Rather, constitutional values mediate private law indirectly – through statutory interpretation, consumer protection and unfair practices law, and contract and tort – while direct First Amendment duties remain exceptional. In practice, such duties would be reviewable before communications and consumer authorities and the courts, with remedies including reinstatement, reasoned decisions, and penalties for systemic non-compliance. Similarly, the German Federal Constitutional Court's decision (1 BvR 1073/20, 2020) emphasized that courts must ensure a constitutionally informed balancing of fundamental rights, such as freedom of expression and personal dignity, even when disputes arise within privately governed digital spaces.[128] While dominant platforms like Facebook are not directly subject to the *Grundgesetz*, the Court made clear that constitutional values must shape the interpretation of private law when these platforms act as arbiters of public discourse. This reasoning reinforces the need for normative accountability, affirming that private actors exercising quasi-public regulatory functions must operate within a framework of legitimacy, proportionality, and procedural fairness.

Finally, the systemic accountability dimension concerns the institutional mechanisms necessary to embed digital power within established constitutional structures of rights protection and democratic oversight. The jurisprudence of the Court of Justice of the European Union (CJEU), particularly in Digital Rights Ireland (C-293/12 and C-594/12, 2014)[129] and La Quadrature du Net (Joined Cases C-511/18, C-512/18, and C-520/18, 2020),[130] illustrates this dimension with exceptional clarity. In both decisions, the Court invalidated indiscriminate data retention regimes, emphasizing that the large-scale processing of personal data by public authorities must be subject to strict proportionality review, independent oversight, and effective judicial remedies. These rulings affirm that systemic accountability requires more than transparency or normative standards alone: it depends on robust constitutional mechanisms capable of constraining concentrations of informational power, through both ex ante safeguards (such as prior judicial authorization) and ex post control (such as access to courts and effective remedies). The Court's insistence on legally foreseeable, limited, and targeted surveillance frameworks underlines the need for structural checks within the digital state architecture. Translated to high-impact algorithmic systems, this minimum implies prior authorization or registration with an independent authority, targeting and purpose limitation, ongoing supervision with renewal, and actionable rights (access, reasoned contestation, and, where appropriate, injunctive relief) against unlawful deployments.

---

128. *See* Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], Dec. 19, 2021, 1 BvR 1073/20 (Ger.), https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2021/12/rk20211219_1bvr107320.html [https://perma.cc/QLA9-5LZY]

129. Digital Rights Ireland Ltd and Seitlinger and Others, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

130. *See* Joined Cases C-511/18, C-512/18, and C-520/18, La Quadrature du Net v. Premier Minister, ECLI:EU:C:2020:6, ¶ 156 (Jan. 15, 2020)

Collectively, these judgments demonstrate judicial engagement with the proposed accountability dimensions, (epistemic, normative, and systemic), while simultaneously exposing their fragmented and isolated articulation across jurisdictions. What remains absent, and what this Article seeks to offer, is an integrated constitutional framework that explicitly combines these dimensions into a coherent model of digital constitutional accountability.

While individual court decisions affirm each dimension independently, the lack of doctrinal integration reveals jurisprudential gap. As further illustrated in the case studies (Section III), this siloed application of constitutional principles fails to adequately address the multifaceted accountability deficits of algorithmic governance. The proposed tripartite framework does not impose an abstract theory upon constitutional law. Rather, it responds to existing fragmentation by integrating visibility (epistemic), legitimacy (normative), and institutional oversight (systemic) into a unified, constitutionally grounded paradigm of accountability.

In this way, the model functions both diagnostically and normatively. It interprets isolated judicial interventions as normative fragments of a broader constitutional logic and offers a structured grammar for translating them into a jurisprudence of integrated accountability, capable of addressing the constitutional realignments prompted by the algorithmic turn, and of ensuring that digital governance remains anchored in democratic principles and fundamental rights.

II. Digital Communication and Democracy: The Implications of Technological Innovation on Public Debate and Participation

The evolution of communication technologies – particularly in data processing and network infrastructure – has significantly altered the dynamics of political communication. These developments have enabled new forms of civic engagement, while also intensifying concerns over information integrity, political polarization, and the algorithmic shaping of public discourse.[131] From the perspective of epistemic accountability, this shift challenges the visibility, traceability, and diversity of information sources in the digital sphere. Social media, microblogging platforms, and instant messaging applications, supported by powerful AI algorithms and vast databases, have facilitated direct interaction between politicians and the public, transforming completely the landscape of traditional political communication.[132]

Politicians and parties now use these tools not only to communicate but also to listen and gather real-time feedback. Disintermediation has allowed politicians to bypass traditional channels such as print and television, directly communicating with voters through posts, tweets, and videos.[133] This shift has led to

131. *See Polarisation and the Use of Technology in Political Campaigns and Communication*, Eur. Parl. Rsch. Serv. 1 (2019).

132. *See* S. Stieglitz, L. Dang-Xuan, *Social Media and Political Communication: A Social Media Analytics Framework*, *in* 3(4) Social Network Analysis and Mining, 1277, 1291 (2013), https://doi.org/10.1007/s13278-012-0079-3; García-Marzá & Calvo, *supra* note 5, at 41-42 (2024) (illustrating the disruptive effects of predictive algorithms on traditional democratic intermediaries).

133. *See, e.g.,* Scott A. Eldridge II et al., *Disintermediation in Social Networks: Conceptualizing Political Actors' Construction of Publics on Twitter*, 7 Media & Commc'n 271-285 (2019); *see*

a more personalized and seemingly transparent form of politics, where messages can be tailored and delivered to specific segments of the electorate with unprecedented precision.[134] In an era of simplified digital access, disintermediation has also enabled populist leaders and movements to communicate directly with the public, often bypassing the critical filters of traditional media.[135] This process has accelerated an apparent democratization of information: a shift that, in terms of normative accountability, challenges the integrity of public discourse by enabling content dissemination without institutional checks.[136] This openness has also created vulnerabilities to mass manipulation, facilitated by emotion-driven rhetoric and engagement-maximizing algorithms.[137]

An emblematic example of this evolution is the strategic use of social media data during recent election campaigns, where detailed user information was leveraged to influence perceptions and voting decisions.[138] These tools have the potential to improve the efficiency of political communication, but they also raise significant concerns regarding privacy, information manipulation, and the impact on democratic processes. Campaigns become highly targeted, relying on algorithms that analyze behaviors, preferences, and online interactions, leading to an extreme level of personalization that erodes epistemic accountability by shielding users from exposure to competing views.

This phenomenon—often referred to as "information bubbles" or "echo chambers"[139]—is a direct result of algorithmic personalization that undermines the pluralism necessary for democratic legitimacy.[140] Information bubbles reduce pluralism and intensify polarization, undermining shared conditions for democratic deliberation.[141] From a constitutional perspective, this fragmentation of the public sphere challenges the foundational assumption that democratic deliberation is premised on shared informational baselines. When algorithmic personalization systematically limits exposure to dissenting viewpoints, it not only amplifies polarization but weakens the communicative infrastructure upon

---

Sebastian Stier et al., *Election Campaigning on Social Media: Politicians, Audiences, and the Mediation of Political Communication on Facebook and Twitter*, 35 Pol. Comm. 50 (2018).

134. On the role of digital platforms in polarizing the public through targeted messaging, see García-Marzá & Calvo, *supra* note 5, at 85.

135. João Feres Júnior & Juliana Gagliardi, *Populism and the Media: Introduction to Part II*, *in* The Politics of Authenticity and Populist Discourses 75, 75–81 (Christoph Kohl et al. eds., Palgrave Macmillan 2021); Gianpietro Mazzoleni & Roberta Bracciale, *Socially Mediated Populism: The Communicative Strategies of Political Leaders on Facebook*, 4 Palgrave Commc'ns 50 1-10 (2018).

136. *See* Kuo, *supra* note 91, at 561.

137. *See* García-Marzá & Calvo, *supra* note 5, at 88.

138. *See* Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, Guardian (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. [https://perma.cc/2GSK-E5YZ]

139. *See* Emre Bozdag & Jeroen van den Hoven, *Breaking the Filter Bubble: Democracy and Design,* 17 Ethics & Info. Tech. 249, 265 (2015).

140. *See* William H. Dutton & Craig. T. Robertson, *Disentangling Polarisation and Civic Empowerment in the Digital Age: The Role of Filter Bubbles and Echo Chambers in the Rise of Populism*, *in* Howard Tumber & Silvio Waisbord, The Routledge Companion to Media Disinformation and Populism 420 (1st ed. 2021).

141. *See* Sebastian Stier et al., *Post Post-Broadcast Democracy? News Exposure in the Age of Online Intermediaries*, 116(2) Am. Pol. Sci. Rev., 768, 774 (2022),

which democratic legitimacy rests. Moreover, the fragmentation of political communication can easily be exploited by populism to consolidate power, manipulating voter perceptions through polarizing and divisive narratives.[142]

Traditional media has long played a role in shaping political campaigns, often through editorial alignment with parties or candidates. However, a key distinction lies in the regulatory frameworks that govern their operation. Traditional media is typically subject to transparency and pluralism standards—for instance, through broadcasting laws or audiovisual media regulations—which aim to safeguard electoral integrity and informed public discourse. By contrast, social media platforms operate in a regulatory grey zone where content dissemination is largely driven by algorithmic curation and commercial incentives, rather than public interest obligations. This shift raises new challenges for ensuring accountability and maintaining a healthy democratic information environment.[143] These challenges implicate both normative and systemic accountability: the normative legitimacy of digital political discourse, and the systemic capacity of institutions to respond to algorithmic opacity and market-driven logic.[144]

This dual deficit reveals a deeper dislocation between democratic ideals and the actual structure of the digital environment. Without enforceable standards of transparency and contestability, algorithmic infrastructures evolve outside constitutional frameworks, eroding the state's capacity to secure the conditions for fair political participation. Where regulatory oversight remains insufficient or fragmented, regulatory minimalism can become a form of structural abdication, leaving core democratic functions at the mercy of commercial infrastructures. In the European Union, this minimalist phase has been partially displaced by the Digital Services Act's due-diligence architecture and enhanced oversight for the largest platforms,[145] but these reforms do not convert platforms into traditional editors and do not eliminate engagement-driven amplification dynamics. Social media platforms therefore remain structurally distinct from traditional media: content visibility is still largely organized through algorithmic curation and commercial incentives, rather than public-interest obligations such as pluralism or balance.[146]

It is precisely this absence of informational pluralism that creates an environment where disinformation can proliferate unchecked, and users may unknowingly engage with content tailored to influence them on a personal level,

142. *See* Martinico, supra note 25, at 111.

143. *See e.g.*, Michele Polo, *Regulation for Pluralism in Media Markets*, *in* The Economic Regulation of Broadcasting Markets 106 (Paul Seabright & Jürgen von Hagen eds., Cambridge Univ. Press 2007); Toby Mendel & Eve Salomon, Freedom of Expression and Broadcasting Regulation (2011); Kari Karppinen, Rethinking Media Pluralism (2013).

144. *See* Curtea Constituțională a României [Romanian Const. Ct.], Decision No. 32 din Dec. 6, 2024, Monitorul Oficial al României, pt. I, nr. 1231 (Dec. 6, 2024) (annulling the 2024 presidential election due to alleged manipulation linked to nontransparent digital tools and funding).

145. *See* Regulation (EU) 2022/2065 (Digital Services Act) arts. 34(1)–(2) (systemic-risk assessment, including civic discourse/elections and recommender systems), arts 49, 56 (Digital Services Coordinators and coordinated supervision/enforcement).

146. *See* Mark Bunting, *From Editorial Obligation to Procedural Accountability: Policy Approaches to Online Content in the Era of Information Intermediaries*, 3 J. Cyber Pol'y 165 (2018) (arguing that platforms shape content markets through rules and algorithmic design, and that regulation should prioritize procedural accountability over publisher-style editorial obligations).

based on collected data and behavioral profiling. This erosion of public reasoning mechanisms severely compromises epistemic accountability, while also exposing institutional vulnerabilities that fall under systemic accountability. The anonymity trade-off is addressed below through tiered, context-sensitive verification mechanisms that preserve dissent while enabling accountability in high-risk electoral settings.

In the political realm, regulation must prioritize transparency and fairness to prevent abuses and ensure that new communication methods reinforce rather than undermine democratic processes. Efforts in regulatory contexts, such as the European Union's GDPR, and similar proposals globally, attempt to balance innovation with the protection of fundamental rights.[147] However, delegating content monitoring to social media platforms has shown significant limitations. Studies indicate that platforms struggle to contain disinformation and harmful content effectively, due to the vastness of online data, rapid information sharing, and economic incentives that often reward engagement over accuracy.[148] Furthermore, the lack of restrictions on anonymity allows disinformation to spread without accountability, posing a serious risk to informed public debate, as opaque, automated systems amplify content without due process or oversight, often beyond public scrutiny.[149] In the European Union, the establishment of the single market led to the incorporation of audiovisual and media policy, aiming to create a unified European market for audiovisual services while ensuring that cultural dimensions are respected across policies.[150] This approach began taking shape with the "Television Without Frontiers" Directive (89/552/EEC)[151] in response to the surge of cross-border broadcasting in the 1980s, setting minimum standards for content distribution across member states. This harmonization effort continues today, with ambitious initiatives such as the Digital Single Market, aiming to standardize digital services and protect citizens' rights.[152]

In contrast, the US regulatory approach has traditionally emphasized a free-market model, even in its media sector, prioritizing freedom of expression and limiting government intervention.[153] However, this laissez-faire premise has been increasingly unsettled in the platform era, as the consolidation of private

147. *See* Michael Gille et al., *Balancing Public Interest, Fundamental Rights, and Innovation: The EU's Governance Model for Non-High-Risk AI Systems*, 13 Internet Pol'y Rev. (2024), https://policyreview.info/articles/analysis/balancing-public-interest-fundamental-rights-and-innovation. [https://perma.cc/6CJT-DEWP]

148. *See* Eleonora Bonadio et al., *Fake News and Copyright* 11(4) Queen Mary J. of Intellec. Prop. 444 (2021), (demonstrating how the fake news phenomenon often underlines a real business model based on the use of intellectual property rights).

149. *See* Danielle K. Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1, 33 (2014).

150. *See generally* Seamus Simpson et al., European Media Policy for the Twenty-First Century: Assessing the Past, Setting Agendas for the Future (2016); Heritiana Ranaivoson et al., European Audiovisual Policy in Transition (1st ed. 2023).

151. *See* Council Directive 89/552/EEC of Oct. 3, 1989 on the Coordination of Certain Provisions Laid Down by Law, Regulation or Administrative Action in Member States Concerning the Pursuit of Television Broadcasting Activities, 1989 O.J. (L 298) 23.

152. *See* Eur. Counc., Council of the Eur. Union, *Digital Single Market for Europe* (last updated Sept. 21, 2020), https://www.consilium.europa.eu/en/policies/digital-single-market/ [https://perma.cc/4SGA-GQSG].

153. *See e.g.,* Christopher S. Yoo, *The Rise and Demise of the Technology-Specific Approach to the First Amendment*, 91 Geo. L.J. 245 (2003).

control over the online speech environment has generated renewed pressure for regulatory intervention and constitutional re-framing of how First Amendment values operate in platform governance.[154] Historically, this orientation fostered a media landscape with minimal constraints on corporate influence, where freedom of speech outweighs calls for extensive data protection or media pluralism standards. In particular, the First Amendment underpins a general reluctance in the U.S. to impose strict regulations on media, especially when it comes to content.[155] Historically, courts and regulators adopted a technology-specific approach, treating various media differently based on their unique characteristics: such as broadcast media being subject to stricter regulations due to its pervasive nature and spectrum scarcity.[156] This market-oriented approach, coupled with minimal regulation, highlights the philosophical differences between the EU's fundamental rights protection-focused framework and the US's market-driven paradigm. These contrasting regulatory models underscore a broader global debate on balancing innovation and rights protection, with the EU leading on harmonization for transparency and accountability, while the US continues to champion market freedom and individual autonomy. The divergence between EU and US approaches to digital regulation reflects not only different policy choices but diverging conceptions of constitutional accountability. Where the EU increasingly relies on a regulatory model of fundamental rights enforcement, the US framework reveals structural resistance to systemic oversight. This normative asymmetry creates fragmented constitutional geographies, where the effectiveness of democratic protections depends on the jurisdictional context, raising concerns about the uneven realization of constitutional guarantees in the digital sphere. This divergence has also produced structural gaps in systemic accountability across jurisdictions. As a consequence, some scholars have identified a form of digital imperialism, whereby U.S.-based tech platforms leverage domestic legal principles, particularly the First Amendment, as a tool to resist foreign regulation and assert extraterritorial influence over global governance norms.[157]

As international discourse evolves, it is therefore essential to move beyond abstract appeals to ethics and accountability and advance a coherent, enforceable regulatory framework capable of resisting asymmetric power dynamics in digital governance.[158] This includes addressing the extraterritorial reach of dominant platforms that invoke domestic legal protections as shields against foreign regulatory authority. Such dynamics highlight the erosion of democratic oversight

154. *See* Evelyn Douek & Genevieve Lakier, *Lochner.com?,* 138 Harv. L. Rev. 100, 102–04 (2024) (on platform power and the shift toward litigation and regulation).

155. *See* Yoo, *supra* note 153, at 251-252.

156. *Id.* at 252-253.

157. *See* Yasmin Curzi de Mendonça & Camille Grenier, *Digital Imperialism: How US Social Media Firms Are Using American Law to Challenge Global Tech Regulation*, Conversation (Mar. 21, 2025), at https://theconversation.com/digital-imperialism-how-us-social-media-firms-are-using-american-law-to-challenge-global-tech-regulation-224366. [https://perma.cc/8LSS-K8R7]

158. *See e.g.,* Eyal Benvenisti, *Upholding Democracy Amid the Challenges of New Technology: What Role for the Law of Global Governance?*, 29 Eur. J. Int'l L. 9-82 (2018) (arguing transparency and ethics in international frameworks are vital for trust and global democratic resilience); Göran Hermerén, *Accountability, Democracy, and Ethics Committees*, 1 L., Innov. & Tech. 153-170 (2009) (arguing that institutional trust requires integrity and accountability as the basis for tech ethics)

beyond borders, an issue that must be addressed through systemic accountability tools at the supranational level. The urgency of this task is underscored by persistently low levels of voter participation across numerous democracies, reflecting not only growing disillusionment with political institutions, but also a broader perception of regulatory impotence in the face of transnational digital influence.[159] Rebuilding democratic trust will thus require frameworks that embed transparency and fairness into technological design while simultaneously reaffirming State's capacity to uphold constitutional principles within the digital domain.

As the preceding analysis suggests, the erosion of democratic structures in the platform-mediated public sphere cannot be fully grasped without unpacking the layered failures of epistemic clarity, normative legitimacy, and systemic responsiveness. The case studies that follow trace these failures across different contexts, illustrating how digital constitutional accountability can serve as both diagnostic and normative tool.

III. From Social Media to Predictive Algorithms: Case Studies on Technology's Role in Shaping Democracy

As discussed, digital platforms have reconfigured political communication through disintermediation and data-driven personalization, enabling politicians to engage directly with the electorate while bypassing institutional and media filters.[160]

While these techniques can enhance message efficiency and engagement, they also raise significant concerns regarding transparency, informational asymmetries, and the manipulation of political will.[161] Regulatory frameworks, particularly within the European Union, have attempted to mitigate these risks by introducing rules on political advertising, data protection, and algorithmic accountability. Yet, enforcement remains uneven, and accountability gaps persist across both public and private actors. The four cases that follow are not presented as an empirical sample, but as interpretive, illustrative probes that make the framework operational. Together, they capture a range of failures: the private regulation of public discourse (Trump's deplatforming), Italian algorithmic populism,[162] the abuse of personal data (Cambridge Analytica), and the use of predictive analytics in electoral campaigns (UK case). Each case reveals distinct yet interconnected facets of democratic erosion in contemporary digital environments, and helps locate those failures across the epistemic, normative, and systemic dimensions of the proposed accountability framework.

---

159. *See, e.g.,* Aki Koivula, et al., *The Voice of Distrust? The Relationship Between Political Trust, Online Political Participation and Voting*, 11 J. Trust Res. 59-74 (2021); Shwadhin Sharma, *Can't Change My Political Disaffection! The Role of Political Disaffection, Trust, and Resistance to Change in Internet Voting,* 22 Digit. Pol'y, Regul. & Governance, 71-91 (2020) (associating digital election distrust with institutional disaffection).

160. On the dangers of disintermediation through predictive algorithms, see, e.g., García-Marzá & Calvo, *supra* note 5, at 41.

161. *See* David W. Nickerson & Todd Rogers, *Political Campaigns and Big Data*, 28J. Econ. Persp. 2 51, 57-58 (2014).

162. *See generally* Marco Bassini, *Rise of Populism and the Five Star Movement Model: An Italian Case Study*, 11 Ital. J. Pub. L. 303 (2019).

A. Digital Propaganda and Political Polarization: The Case of Trump's Social Media Strategy

The deplatforming of former U.S. President Donald Trump in January 2021[163] offers a paradigmatic example of a combined normative, systemic, and epistemic accountability gap.[164] Twitter, a private company, unilaterally decided to restrict the speech of a sitting head of state based on internal policies and opaque standards, with limited external constraint or structured public scrutiny.[165] This was a decision of major democratic and symbolic significance. The case reveals how normative authority—deciding the limits of acceptable political speech—has shifted to private digital actors. This shift underscores a central challenge of digital constitutionalism: Who sets the rules of political discourse online, under what authority, and subject to what oversight?[166]

Trump's use of Twitter fundamentally redefined the relationship between political power and digital communication.[167] Digital communication became an instrument of direct political mobilization and unmediated narrative control, circumventing conventional media filters and reshaping the public agenda in real time. Scholars such as Ott and Dickinson have described this as a "politics of white rage," where Twitter became both the amplifier and the medium of populist, polarizing, and often misleading messaging.[168] These "tweet politics,"[169] based on short and emotionally charged messages, contributed to the rapid diffusion and amplification of divisive content, exploiting algorithmic virality to bypass democratic deliberation.[170] More generally, the case illustrates a systemic vulnerability: constitutionally relevant speech-governance decisions

---

163. *See* Andrew Ross Sorkin et al., *The Deplatforming of President Trump*, N.Y. Times (Jan. 8, 2021), https://www.nytimes.com/2021/01/08/business/dealbook/trump-facebook-twitter-deplatforming.html [https://perma.cc/4HMN-X96X]

164. *See* Knight First Amendment Inst. at Columbia Univ. v. Trump, 302 F. Supp. 3d 541 (S.D.N.Y. 2018) (holding that blocking users from @realDonaldTrump constituted viewpoint discrimination within a designated public forum), aff'd, 928 F.3d 226, 230 (2d Cir. 2019) ("the First Amendment does not permit a public official . . . to exclude persons from an otherwise-open online dialogue because they expressed views with which the official disagrees"), vacated as moot, Biden v. Knight First Amendment Inst. at Columbia Univ., 141 S. Ct. 1220 (2021).

165. *See* M. R. A. Muhammad & N. Nirwandy, *A Study on Donald Trump Twitter Remark: A Case Study on the Attack of Capitol Hill*, 14(2) J. of Media & and Info. Warfare, 75, 104 (2021); A. Prabhu et al., *Capitol (Pat) Riots: A Comparative Study of Twitter and Parler*, ArXiv (2021), https://arxiv.org/abs/2101.06914 [https://perma.cc/F8VD-NXCC]

166. *See e.g.,* William H. Dutton et al., Freedom of Connection – Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet (UNESCO 2011).

167. *See* Brian L. Ott, *The Age of Twitter: Donald J. Trump and the Politics of Debasement,* 34 Critical Stud. Media Commc'n, 59 (2016).

168. *See* Brian L. Ott, G. Dickinson, The Twitter Presidency: Donald J. Trump and the Politics of White Rage (2019).

169. *See* Ramona Kreis, *The "Tweet Politics" of President Trump*, 16 J. Lang.& Pol., 607, 618 (2017).

170. *See* David Randall & Jessica Toonkel, *Trump's Low Advertising Spending Weighs on U.S. Broadcasters*, Reuters (Mar. 1, 2016), https://www.reuters.com/article/us-usa-election-mediaspend/trumps-low-advertising-spending-weighs-on-u-s-broadcasters-idUSMTZSAPEC31DC1REH [https://perma.cc/J5BY-6FG4] (examining Trump's minimal advertising expenses following his strategic use of Twitter in his presidential campaign).

increasingly occur within private infrastructures that sit uneasily within traditional public-law controls.

From a constitutional perspective, this dynamic illustrates how private digital actors now perform functions traditionally reserved for state institutions, setting rules for speech, allocating visibility, and controlling the flow of political information. Yet, unlike state actors, they operate without structural checks and balances, without appeal, and without institutionalized channels of public contestation.[171] This hybrid public-private power generates a systemic void that evades both traditional legal and corporate accountability frameworks.[172] Read through the tripartite framework, the accountability failures can be made operational: (epistemic) limited visibility into amplification and enforcement logics, (normative) internally defined standards for high-stakes political speech decisions, and remedy. At the normative level, the case raises foundational questions: Who decides what speech is permissible in digital public spaces, by which criteria, and with what procedural guarantees? At the epistemic level, opaque moderation and amplification systems shaped not just visibility but also perceptions of legitimacy and relevance, producing a curated political reality optimized for engagement rather than democratic deliberation. The controversy also captures a core dilemma of digital constitutionalism: how to balance freedom of expression and democratic security when neither key decisions nor enforcement standards are reliably anchored in public-law forms of justification and review.[173] The case also exemplifies the datafication of political discourse: emotionally charged, micro-targeted content optimized to provoke and polarize. Platforms driven by engagement logic amplify outrage and division, prioritizing emotional salience over informational value. This constitutes a structural failure of epistemic accountability, as users are subjected to manipulated, non-transparent informational environments that distort public reasoning.[174] In practical terms, the case points to policy pathways consistent with the tripartite framework: mandatory transparency and auditability of enforcement and amplification (epistemic), legally grounded standards and procedural safeguards for high-stakes content

171. *See* Kreis, *supra* note 169, at 618.

172. *See* Biden v. Knight First Amend. Inst. at Columbia Univ., 141 S. Ct. 1220 (2021) (Thomas, J., concurring) (questioning public-forum analogies given private platform control and pointing to common-carrier/public-accommodation approaches).

173. *See e.g.,* J. R. Bambauer et al., *Platforms: The First Amendment Misfits,* 97(3) Ind. L.J. 1047, 1069 (2022).

174. *See e.g.,* Vera Eidelman & Kate Ruane, *The Problem with Censoring Political Speech Online - Including Trump's*, ACLU (June 15, 2021), https://www.aclu.org/news/free-speech/the-problem-with-censoring-political-speech-online-including-trumps [https://perma.cc/59U8-JT6G]; *see* Glenn Reynolds, *When Digital Platforms Become Censors*, Wall St. J. (Aug. 18, 2018), https://www.wsj.com/articles/when-digital-platforms-become-censors-1534514122?gaa_at=eafs&gaa_n=AWEtsqcJ_q_XZxlur2c6XTk8t_xcKcv8tokXaSD6H71k7zB5FzkOIE2WBlEOZn_lffg%3D&gaa_ts=69adcb40&gaa_sig=3B0C2DZjRaHthHN3oJQ-kcp7Sa-y1AoNGqVi0hJgzPFSP1VS3SZKjdcXloP-wC2QEctyhoFpjb6NnnEOH6l6hA%3D%3D [https://perma.cc/59U8-JT6G]; *see* Kristen Cuetos, *The Search to Find a Legal Remedy for Regulating Censorship on Social Media*, 2022 B.C. Intell. Prop. & Tech. F. 1, 2; *see* Michael Cusumano et al., *Pushing Social Media Platforms to Self-Regulate*, Regul. Rev.(Jan. 3, 2022), https://www.theregreview.org/2022/01/03/cusumano-yoffie-gawer-pushing-social-media-self-regulate [https://perma.cc/NXF4-9W9T]; Marie-Andrée Weiss, *Regulating Freedom of Speech on Social Media: Comparing the EU and the US Approach*, Stanford-Vienna Trans. Tech. L. Forum (Working Paper No. 73), https://law.stanford.edu/wp-content/uploads/2021/02/weiss_wp73.pdf.

governance (normative), and independent oversight with escalation powers and effective remedies (systemic).

B. Algorithmic Populism in Italy: Between Participation and Manipulation

The so-called "La Bestia" (The Beast), the digital communication system employed by the Italian political party, Lega, presents a parallel case to that of President Trump in the United States.[175] Under Matteo Salvini's leadership, the Lega transformed social media into a powerful political tool, employing micro-targeting strategies and personalized messaging similar to those used by Trump. As in the U.S., the party bypassed traditional media, directly shaping public narratives.[176] Unlike Trump's broader messaging, La Bestia focused on a narrow set of high-salience issues, reinforcing echo chambers in which emotionally charged content, algorithmic amplification, and the absence of independent oversight converged, producing a paradigmatic failure of epistemic accountability. Users were primarily exposed to ideologically aligned content, reducing exposure to dissenting perspectives and contributing to increased polarization. [177] This environment was curated through opaque systems with limited transparency and weak possibilities of audit or contestation, revealing combined epistemic and systemic failures. From a normative perspective, the lack of binding standards for online political messaging enabled ethically questionable tactics—such as emotional manipulation, fear-based appeals, and misleading claims—to proliferate without legal consequence. Systemically, no independent authority was tasked with overseeing the digital strategies of political actors, allowing political infrastructure to evolve outside constitutional oversight. This case illustrates how algorithmic filtering and behavioral targeting do not merely distribute political messages—they actively construct divergent political realities tailored to reinforce ideological loyalty.

The result is an asymmetrical information flow that amplifies loyalist discourse while undermining pluralism.[178] This strategic manipulation of public discourse not only consolidated political support but also circumvented traditional mechanisms of democratic scrutiny.[179] These dynamics embody a full-spectrum accountability breakdown, where neither the platforms nor the political actors are held to standards of epistemic transparency, normative integrity, or systemic control.[180]

---

175. *See* Margherita Barbieri, La Bestia di Salvini. Manuale della Comunicazione Leghista, Edizioni del Girasole (Ravenna 2019); Roberto D'Alimonte, *How the Populists Won in Italy*, 30 J. Democracy 114 (2019); Franco Zappettini & Marzia Maccaferri, *Euroscepticism Between Populism and Technocracy: The Case of Italian Lega and Movimento 5 Stelle*, 17 J. Contemp. Eur. Rsch. 239-257 (2021).

176. *Id.*

177. *See* Stark & Stegmann, *supra* note 35.

178. *See* Barbieri, *supra* note 175, at 26.

179. *See generally* Petros Iosifidis & Nicholas Nicoli, Digital Democracy, Social Media and Disinformation (2020).

180. *See e.g.,* Phillip N. Howard & Samantha Bradshaw, *The Global Organization of Social Media Disinformation Campaigns*, 71(1.5) J. Int'l Aff. 23-32 (2018).

Another significant Italian case illustrating the use of digital technology in politics is the Five Star Movement.[181] Founded in 2009 by comedian Beppe Grillo and strategist Gianroberto Casaleggio,[182] the Movement introduced an innovative model of digital participation through the online platform Rousseau, allowing members to vote on legislation, select candidates, and participate in internal consultations.[183] At first glance, this digital experiment embodied the ideal of participatory democracy, facilitating engagement beyond traditional party hierarchies.[184] However, critical analysis reveals that this inclusionary potential was offset by failures of normative accountability, particularly in the design and governance of the platform.

In particular, Rousseau was plagued by allegations of internal manipulation and the absence of clear oversight.[185] The platform's security flaws and vulnerability to data breaches triggered sanctions from the Italian Data Protection Authority.[186] Over time, participation declined dramatically, revealing a disjunction between the rhetoric of digital empowerment and its practical execution.[187] This reflects a failure of normative accountability: Rousseau lacked codified, democratically legitimized rules to ensure procedural fairness, data protection, and meaningful deliberation. Furthermore, systemic accountability collapsed due to institutional passivity; despite repeated data breaches and legal violations, no structural reforms were implemented to safeguard participatory integrity. These phenomena exemplify the dangers of substituting procedural legitimacy with technological mystique: opaque decision parameters (epistemic), weakly institutionalized participation rules (normative), and limited ex ante oversight of platform architecture and data use (systemic). In the absence of safeguards, Rousseau evolved into a centralized system of control masquerading as participatory democracy, where key decisions could be orchestrated by unelected actors, shielded from institutional scrutiny.[188]

---

181. *See* Maria Elisabetta Lanzone, *The "Post-Modern Populism" in Italy: The Case of the Five Star Movement*, *in* B. Wejnert, The Many Faces of Populism: Current Perspectives 53–78 (Emerald Group 2014).

182. *See* Eric Turner, *The Grillini in Italy: New Horizons for Internet-Based Mobilization and Participation*, 12 Soc. Mov. Stud. 214-220 (2013); Martinico, *supra* note 25, at 63-98; Zappettini & Maccaferri, *supra* note 175, at 128; Fabio Bordignon & Luigi Ceccarini, *The Five-Star Movement: A Hybrid Actor in the Net of State Institutions*, 20 J. Mod. Italian Studies 454–473 (2015).

183. *See* Camille Bedock & Bartolomeo Cappellina, *Beyond Digital Populism: Civic Culture and Visions of Political Participation Among Five Star Movement Activists*, 54 Italian Pol. Sci. Rev. 70-83 (2024); L. Mosca, *From the Streets to the Net? The Political Use of the Internet by Social Movements*, 1 Int'l J. E-Pol., 1-21 (2010).

184. *See* Marco Bassini, *Rise of Populism and the Five Star Movement Model: An Italian Case Study*, *in* Italian Populism and Constitutional Law: Strategies, Conflicts and Dilemmas 199, 207 (Giacomo Delledonne et al. eds., 2020).

185. *See* Lorenzo Mosca, *Democratic Vision and Online Participatory Spaces in the Italian Movimento 5 Stelle*, 55 Acta Pol. 1-18 (2020); *see also* Marcho Tarchi, Italia Populista. Dal Qualunquismo a Beppe Grillo (2015).

186. *See* Gabriele Giacomini, *To Be or Not to Be 'Rousseauian'. The Rise and Fall of 'Digital Utopianism' in the Five Star Movement*, 14 J. of eDemocracy & Open Govt. 149, 159 (2022); Mosca, *supra* note 183.

187. Giacomini, *supra* note 186, at 159, 162.

188. *See* Cecilia Biancalana, *The Spectrum of Italian Populist Parties in the 2024 European Elections: A Shift to the Right*, 2024 EP Elections under the Shadow of Rising Populism 235, 235-39 (Gilles Ivaldi & Emilia Zankina eds., European Center for Populism Studies (ECPS)(2024).

Together, the cases of La Bestia and Rousseau illustrate how algorithmic populism distorts knowledge, erodes legal safeguards, and escapes institutional control. This highlights the urgent need for a constitutional framework that restores oversight of digital political infrastructures. Concrete remedies include mandatory algorithmic audits (epistemic), binding standards for digital political communication based on democratic principles (normative), and the establishment of independent electoral oversight bodies equipped to scrutinize the use of technology in political campaigns (systemic).

C. Digital Propaganda and Data Manipulation: The Cambridge Analytica Case

The Cambridge Analytica scandal stands as a defining case illustrating the complex intersections of data technology, political influence, and democratic integrity.[189] It exemplifies a compound failure of epistemic, normative, and systemic accountability, combining weak institutional leverage over cross-border data practices (systemic), the absence of enforceable boundaries for political profiling and targeting (normative), and opaque, unchallengeable voter profiling and message delivery (epistemic). In 2016, the data analytics firm accessed and utilized personal data from millions of Facebook users, without explicit consent, to construct detailed psychographic voter profiles.[190] These profiles enabled a highly personalized political messaging strategy during the U.S. presidential election, using advanced data mining and micro-targeting techniques to shape public opinion on a large scale.[191] This case exposed critical gaps in existing regulatory frameworks, particularly concerning privacy and data protection. It demonstrated the potential for digital platforms to be exploited by private entities, highlighting an urgent need for more robust, cohesive data protection policies. As discussed in the Introduction, subpart A, this also highlights divergence between the United States' fragmented approach to data privacy and the EU's unified GDPR model, reflecting deeper differences in constitutional orientation and regulatory capacity. However, even a robust framework like the GDPR, while essential, does not resolve the systemic concentration of informational power and enforcement asymmetries revealed by this case. From a systemic accountability perspective, the scandal underscores how electoral commissions and data authorities lacked both practical cross-border enforcement leverage and algorithmic literacy to counteract transnational manipulation, even though the GDPR's technology-neutral toolbox can reach certain forms of profiling and behavioural

189. *See* Cadwalladr & Graham-Harrison, *supra* note 138. For a broader discussion of Cambridge Analytica and the subsequent scandal and investigation, see also, Joanne Hinds et al., "*It Wouldn't Happen to Me": Privacy Concerns and Perspectives Following the Cambridge Analytica Scandal*, 143 Int'l J. Hum.-Comput. Stues 102498, 1-2 (2020).

190. *See* Jim Isaak & J. Hanna Mina, *User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection*, 51 Computer 56, 56 (2018).

191. *See* Vian Bakir, *Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting*, 5 Frontiers Commc'n, at 2-4 (2020); Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N. Y. Times (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html; [https://perma.cc/VWJ4-KDPZ] Jonathan Heawood, *Pseudo-Public Political Speech: Democratic Implications of the Cambridge Analytica Scandal*, 23 Info. Polity 429, 429-31 (2018).

monitoring when they fall within data-protection law.[192] Applying the tripartite model reveals that while epistemic and normative remedies have since been partially addressed through the GDPR and political advertising rules, systemic safeguards remain elusive. The case calls for the institutional embedding of algorithmic oversight at the constitutional level, particularly through inter-agency cooperation mechanisms and supranational governance instruments. Beyond regulatory concerns, the Cambridge Analytica case also reveals profound ethical dilemmas associated with the use of personal data for political purposes. Techniques employed by the firm exemplify what has been termed "surveillance capitalism," where data is not only mined for economic benefit but also strategically wielded to shape individuals' beliefs and behaviors.[193] These practices raise profound questions not only about individual privacy, but also about epistemic accountability, that is, the ability of citizens to access reliable information and form political opinions free from covert manipulation. When predictive algorithms micro-target users based on psychological traits, they do not merely invade privacy: they reshape the epistemic environment in which democratic deliberation occurs.

The manipulation of voter sentiment seen here highlights the broader risk posed by digital tools that, without ethical safeguards and constitutional oversight, can distort political outcomes and undermine democratic principles.[194] This case catalyzed transnational reflection on the need to regulate political micro-targeting and reaffirm democratic boundaries. Safeguarding digital democracy demands more than compliance;[195] it requires accountability tools that retain democratic control over how political preferences are shaped.[196] Specifically, this entails: i) Epistemic remedies: mandatory algorithmic transparency measures; ex ante and ex post audits of micro-targeting campaigns; public registers of political ads with targeting criteria. ii) Normative remedies: binding ethical standards for the political use of personal data, with clear thresholds of legitimacy and mandatory consent protocols; restrictions on psychographic profiling in electoral contexts. iii) Systemic remedies: establishment of independent electoral oversight bodies with authority over transnational platforms; enhanced powers for data protection authorities to investigate and sanction political manipulation

192. *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1, recital 15. (stating that data protection "should be technologically neutral" and "should not depend on the techniques used"); Janis Wong &Tristan Henderson, *The Right to Data Portability in Practice: Exploring the Implications of the Technologically Neutral GDPR*, 9 Int'l Data Privacy L. 173 (2019) (discussing the GDPR as a technologically neutral framework intended to remain durable as technologies change).

193. *See* Zuboff, *supra* note 47.

194. *See* Jacquelyn Burkell & Priscilla M. Regan, *Voter Preferences, Voter Manipulation, Voter Analytics: Policy Options for Less Surveillance and More Autonomy*, 8 Internet Pol. Rev. 4 (2019).

195. *See e.g.,* Boldyreva Elena L. et al., *Cambridge Analytica: Ethics and Online Manipulation with Decision-Making Process*, 51 Eur. Proc. Soc. & Behav. Sci. 91–102 (2018); Syafira Fitri Auliya et al., AI Versus AI For Democracy: Exploring the Potential of Adversarial Machine Learning to Enhance Privacy and Deliberative Decision-Making in Elections 1-13 (Springer 2024).

196. *See* Eric Rosenbach & Katherine Mansted, *Can Democracy Survive in the Information Age?*, Belfer Ctr. For Sci. And Int'l Aff. (Oct. 2018), https://www.belfercenter.org/publication/can-democracy-survive-information-age. [https://perma.cc/24HQ-YZP9]

practices; and clear public-law constraints on non-consensual behavioral targeting in electoral contexts.

D. Digital Propaganda and Predictive Analysis: The UK Case

Another critical case that highlights the democratic challenges posed by emerging technologies is the use of predictive algorithms in political campaigning in the United Kingdom. These tools are designed to analyze voter behavior, segment audiences, and forecast electoral trends based on behavioral and psychographic data. Predictive algorithms operate as informational filters, subtly shaping which political messages individuals receive, how frequently, and in what emotional register. This manipulation compromises voters' autonomy: decisions are increasingly formed within opaque systems of behavioral influence, rather than through transparent deliberation. These dynamics reveal a clear failure of epistemic accountability, as individuals lack visibility into the data-driven mechanisms that structure their political reasoning. [197]

At the same time, the UK case exposes a deeper failure of systemic accountability. The current regulatory framework – combining statutory provisions, common law principles, and post-Brexit data protection norms – struggles to provide effective mechanisms for scrutinizing how predictive models influence electoral behavior.[198] Judicial oversight, traditionally a cornerstone of constitutional control, becomes difficult when decision-making is delegated to opaque, algorithmic processes.[199] This opacity limits legal review and undermines public trust.[200] The delegation of communicative power to algorithmic infrastructures, often governed by private incentives, undermines the democratic principle that legitimacy must be grounded in accountable public reasoning.

This case illustrates how predictive analytics are not merely technical instruments of communication, but structural agents of political transformation.[201] When electoral competition becomes a contest of data extraction rather than a confrontation of ideas, democratic deliberation is displaced by behavioral engineering.[202] Such systems take on quasi-constitutional roles, restructuring how legitimacy is produced.[203]

While the UK GDPR retains many protections introduced under EU law, the post-Brexit flexibility opens the door to regulatory divergence and uncertainty.[204] Existing data protection principles remain generalist and do not provide clear

197. *See* P. Rita et al., *Social Media Discourse and Voting Decisions Influence: Sentiment Analysis in Tweets During an Electoral Period*, 13 Soc. Network Anal. Min. 1-16 (2023).

198. *See* Bethany Shiner, Big Data, Small Law: How Gaps in Regulation are Affecting Political Campaigning Methods and The Need for Fundamental Reform, 362 (2019).

199. *Id.; see also* García-Marzá & Calvo, *supra* note 5, at 44.

200. *See* Rita et al., *supra* note 197, at 9.

201. *Id.* at 6; Eubanks, *supra* note 50; J. Bartlett, The People Vs Tech: How the Internet is Killing Democracy (and How We Save It) (2018).

202. *See* Cathy O'Neil, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy (Crown Publishing Group 2016).

203. *See e.g.,* Stephanie Hankey et al., *Data and Democracy in the Digital Age*, Const. Soc'y (2018), https://consoc.org.uk/wp-content/uploads/2018/07/Stephanie-Hankey-Julianne-Kerr-Morrison-Ravi-Naik-Data-and-Democracy-in-the-Digital-Age.pdf [https://perma.cc/9544-Q95Y]

204. *See* Data Protection Act 2018, c. 12 (UK); Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, SI 2020/1586, regs. 2-3 (incorporating the GDPR at UK law as the "UK GDPR.").

standards for political uses of AI.[205] This regulatory ambiguity highlights a normative accountability deficit: without binding, democratically legitimated standards for algorithmic campaigning, predictive systems operate in a legal void, beyond the reach of electoral ethics or institutional scrutiny. This facilitates the emergence of algorithmic governance, a delegated, opaque decision-making process that bypasses traditional procedures and institutions. Democratic legitimacy, in such contexts, rests on untraceable inferences rather than public deliberation. Additionally, epistemic accountability is compromised by the inherent opacity of predictive analytics, making it difficult for voters to assess how algorithmically curated content influences their political autonomy.

Comparatively, jurisdictions such as Germany and France have begun to address these challenges through targeted legal frameworks, such as mandatory algorithmic impact assessments and AI-specific political safeguards.[206] These examples show that a more robust and democratically responsive approach is possible and urgently needed. Drawing on such models, the UK could benefit from developing tailored constitutional and regulatory mechanisms to govern the political use of predictive algorithms. A coherent response should include: i) Epistemic remedies: Mandatory transparency registers for political ads; public disclosure of targeting criteria and content provenance; algorithmic explainability standards applicable to electoral contexts; external audits of campaign influence strategies. ii) Normative remedies: A binding electoral code of conduct for algorithmic campaigning; explicit limits on psychographic micro-targeting and behavioral manipulation; legal requirements for voter consent when data are used to infer political orientation. iii) Systemic remedies: Establishment of an Independent Electoral Algorithmic Authority empowered to monitor, investigate, and sanction misuse; ex ante review of predictive models used in campaigns; clear constitutional provisions delineating which political functions may not be outsourced to algorithmic systems. The UK case shows that predictive analytics must be treated as rights-affecting governance infrastructure, requiring doctrinal and institutional pathways that extend classic constitutional principles – including informed consent and proportionality – to the digital architecture of political campaigning. Without structural intervention, democracy risks capture by opaque, algorithmic logics. The next section thus turns to possible strategies for fostering responsible digital governance, in line with the proposed framework of digital constitutional accountability.

---

205. *See* Karen McCullagh, *Post-Brexit Data Protection in the UK – Leaving the EU but Not EU Data Protection Law Behind*, *in* Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics 35, 35–58 (Gloria González Fuster et al. eds., Edward Elgar Publ'g 2022).

206. *See*, *e.g.*, *Commission Nationale de l'Informatique et des Libertés, Elections : quelles influence de l'IA sur notre vote?* (2024), https://linc.cnil.fr/sites/linc/files/2024-09/dossier-ia-elections_v1.pdf [https://perma.cc/6W23-YD8N]; Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI), *Opinion of the Data Ethics Commission* (2019), https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Datenschutz/Data-Ethics-Commission_Opinion.pdf [https://perma.cc/4LXY-865L]

IV. A Framework for Responsible Digital Governance

The integration of new technologies within democratic systems has sparked a complex debate among executive and legislative bodies, which now face the dual challenge of fostering innovation while safeguarding democratic values.[207] As these infrastructures reshape democratic architectures, governments must adopt regulatory frameworks that do not merely balance innovation and rights, but that embed constitutional safeguards within the design and deployment of digital systems.

Consistently with the limits and scope conditions illustrated in §2.2.1, a forward-looking approach to digital governance must move beyond abstract principles and adopt concrete, enforceable measures. Legislatures should require independent, periodic audits of digital platforms and their algorithms.[208] Companies should be obligated to disclose details about content moderation policies, algorithmic decision-making criteria, and political advertising methods. These duties should be enforced through periodic audits, public registers of political content, and scrutiny by independent authorities with technical and constitutional expertise. These proposals align with models of algorithmic accountability that combine technical mechanisms for verifiable compliance with institutionalized oversight, while at the same time responding to critiques of transparency that warn against treating disclosure as a substitute for structural control over algorithmic infrastructures.[209] Establishing a dedicated regulatory agency with the authority to conduct these audits and impose corrective measures would serve as a critical check on the considerable power wielded by technology firms, which function as "information fiduciaries."[210] Audits should

---

207. *See e.g.,* Thomas s. Kuhn, *The Structure of Scientific Revolutions*, in 2 Int'l Encyclopedia of Unified Science (2d ed., Univ. of Chicago Press 1970) (showing how tech breakthroughs force shifts in scientific and regulatory norms). For a more recent perspective on the issue, see Michael Gille et al., *Balancing Public Interest, Fundamental Rights, and Innovation: The EU's Governance Model for Non-High-Risk AI Systems*, 13 Internet Pol'y Rev. (2024), https://policyreview.info/articles/analysis/balancing-public-interest-fundamental-rights-and-innovation [https://perma.cc/T5B4-BL4L]; Nemitz, *supra* note 17, at 2-3 (discussing the importance of embedding principles of democracy, the rule of law, and human rights in AI governance); Mark Coeckelbergh, *Artificial Intelligence, the Common Good, and the Democratic Deficit in AI Governance*, AI Ethics 1-7 (2024).

208. *See e.g.,* Chris Tenove, *Protecting Democracy from Disinformation: Normative Threats and Policy Responses*, 25 Int'l J. Press/Pol. 517–537 (2020); Chris Tenove et al., Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy, Research Report, Centre for the Study of Democratic Institutions, University of British Columbia (2018); Niels Nagelhus Schia & Lars Gjesvik, *Hacking Democracy: Managing Influence Campaigns and Disinformation in the Digital Age,* 5 J. Cyber Pol'y, 413-428 (2020); Judit Bayer et al., *Disinformation and Propaganda: Impact on the Functioning of the Rule of Law and Democratic Processes in the EU and Its Member States: 2021 Update*, Eur. Parliament (2021), https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653633 [https://perma.cc/6KJP-YTC9]; Jens David Ohlin & Duncan B. Hollis, Defending Democracies: Combating Foreign Election Interference in a Digital Age (Oxford Univ. Press. 2021).

209. *See* Kroll et al., *supra* note 44; Ananny & Crawford, *supra* note 34, at 983-84 (warning that transparency alone can misdescribe algorithmic systems).

210. *See generally* Balkin, *supra* note 51, at 1161-62 (introducing the concept of "information fiduciaries" and proposing that tech companies have a responsibility to protect users' information transparently and accountably); *see also* Julia Powles & Helen Nissenbaum, *The Seductive Diversion of 'Solving' Bias in Artificial Intelligence*, Medium

complement, not replace, democratically set standards. The agency's mandate should be bounded by statutory goals and rights-based thresholds set by the legislature, subject to judicial review and periodic legislative reauthorization, so that audits operate as risk-calibrated enforcement tools rather than as a substitute for democratically accountable rule-setting. Such an agency should be equipped with technical forensic capacity, including ex-post black-box auditing tools. The agency should also have procedural authority to compel disclosure under judicial control and the power to issue binding transparency orders. To ensure cross-border effectiveness, the agency could be integrated into a transnational regulatory network, akin to the European Data Protection Board but focused on algorithmic accountability.

Regulators should also formalize the fiduciary obligations of platforms – especially those involved in shaping political discourse – requiring that they act not only with procedural transparency but also in accordance with constitutional norms of fairness, inclusion, and deliberative integrity. Existing regulatory frameworks such as the Digital Services Act (DSA),[211] the Digital Markets Act (DMA),[212] and the AI Act[213] provide an initial blueprint for oversight, but their effectiveness depends on coordinated and consistently resourced enforcement, and on the clarity and operability of remedial pathways, that include administrative supervision, user redress, and judicial review, across Member States.[214] This blueprint is particularly visible in the DSA: it introduces important obligations aimed at improving transparency and accountability in content moderation, and operationalizes a risk-based due diligence architecture for very large online platforms and search engines through the identification, assessment, and mitigation of "systemic risks."[215] Rather than mandating broad removal of lawful speech, it targets systemic risks, including civic discourse and electoral processes, through governance duties such as risk assessment, mitigation, reporting, and independent auditing.[216] Read through the tripartite

(Dec. 7, 2018), https://onezero.medium.com/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53 (proposing that the government and our communities create policies surrounding A.I. to protect users). [https://perma.cc/6SXS-GSKL]

211. Digital Services Act, *supra* note 113.

212. *Id.*

213. Artificial Intelligence Act, *supra* note 70.

214. *See* Pietro Mattioli, *Navigating the Complexities of the DSA's Enforcement Framework: Sincere Cooperation in Action*?, 21 Utrecht L. Rev. 19, 22 (2025); Eur. Comm'n, *Lack of effective implementation of the Digital Services Act* (May 6, 2025), https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1081 [https://perma.cc/PWM5-LP26]; Eur. Comm'n, *Commission Decides to Refer Czechia, Spain, Cyprus, Poland and Portugal to the Court of Justice of the European Union due to their Failure to Effectively Implement the Digital Services Act* (May 6, 2025), https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1081 [https://perma.cc/E5R7-MHW9] ("Uniform application" can be undermined by Member State design and penalty-rule gaps).

215. Digital Services Act, *supra* note 113, recitals 34(1), 40, 86 (requiring very large online platforms and very large online search engines to identify, analyze, and assess "systemic risks," and to adopt reasonable, proportionate, and effective mitigation measures tailored to those risks, with particular consideration to impacts on fundamental rights).

216. Digital Services Act, *supra* note 113, recitals 30 (no general monitoring), 22 (notice-and-action), 40 (proportionate risk-mitigation considering fundamental-rights impacts), recitals 51, 86 (targeted action on illegal content; proportionality and avoidance of unnecessary restrictions, esp. freedom of expression).

lens proposed here, this is best understood as an EU move toward systemic accountability: but it leaves structural dominance and enforcement fragmentation largely unresolved.[217] The DMA addresses anti-competitive practices through ex-ante obligations on gatekeepers but stops short of dismantling systemic dominance.[218] The AI Act also relies on a risk-based architecture but does not introduce a dedicated substantive regime for the licensing, remuneration, or market-power implications of copyrighted training data, leaving core questions about extraction and monetization to existing EU copyright law.[219] These blind spots reveal a systemic accountability deficit. Strengthening these frameworks, alongside more targeted legislative reforms, will be necessary to curb corporate overreach while preserving democratic resilience. Specifically, amendments to the DSA could mandate digital ombuds institutions at national or EU levels to handle user complaints, investigate failures, and check platform practices. These mechanisms would operationalize rights-based contestability in day-to-day platform governance.[220]

While anonymity protects privacy and speech, its unfettered use fosters disinformation and undermines credible discourse. A balanced framework should preserve the benefits of anonymity for legitimate expression while enabling accountability through tiered identity-verification mechanisms for abuse cases.[221] One concrete application would be to require verified-user protocols for political advertising and election-related communications, to reduce coordinated anonymous manipulation.[222] Implementing tiered verification, however, must navigate constitutional tensions: identity verification can suppress dissent in authoritarian

---

217. Digital Services Act, *supra* note 113, recital 76 (applying the additional "very large" platform/search engine regime to services reaching at least 45 million average monthly active recipients in the Union); id. recital 86 (requiring risk assessments that are service-specific and proportionate to the systemic risks); *id.* recital 79 (linking the "very large" category to the capacity to strongly influence online safety, public opinion and discourse, and online trade).

218. *See, e.g.,* Pierre Larouche & Alexandre de Streel, *The European Digital Markets Act: A Revolution Grounded on Traditions*, 12 J. Eur. Competition L. & Prac. 542 (2021); Oles Andriychuk, *The Digital Markets Act: Tailoring the Tailors, in* Kalpana Tyagi et al., Digital Platforms, Competition Law, and Regulation: Comparative Perspectives 43 (Hart Publishing 2024) (limitations of the DSA and DMA in addressing structural dominance and ensuring market contestability).

219. Artificial Intelligence Act, *supra* note 70, recital 26 (risk-based approach); *id.* art. 53(1)(c)–(d) and recital 108 (GPAI obligations to adopt a copyright-compliance policy and publish a training-data summary; "does not affect the enforcement of copyright rules"); Eur. Parliamentary Rsch. Serv., *AI and Copyright: The Training of General-Purpose AI* (Apr. 23, 2025), https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/769585/EPRS_ATA(2025)769585_EN.pdf [https://perma.cc/4PT3-SK4Z] (noting the AI Act does not regulate licensing for GPAI training); Alexander Peukert, *Copyright in the Artificial Intelligence Act – A Primer*, 73 GRUR Int'l 497, 502 (2024) (describing the AI Act as risk-based and without prejudice to copyright).

220. *See e.g.,* Edoardo Celeste & Giovanni De Gregorio, *Digital Humanism: The Constitutional Message of the GDPR*, 3 Glob. Priv. L. Rev. 4-18 (2022).

221. *See e.g.,* Shuting (Ada) Wang et al., *Cure or Poison? Identity Verification and the Posting of Fake News on Social Media*, 38 J. Mgmt. Info. Sys., 1011–1038 (2021); Michelle Anna Ruesch & Oliver Märker, *Making the Case for Anonymity in E-Participation*, 4 J. E-Democracy & Open Gov't, 301–317 (2012); Helen Nissenbaum, *The Meaning of Anonymity in an Information Age*, 15 Info. Soc'y, 141-144 (1999); Michael Salmony, *'Rethinking Digital Identity*,' 12 J. Payments Strategy & Sys. 40–57 (2018).

222. *See e.g.,* Cass R. Sunstein, Republic.com 2.0 163–65 (2007); Danielle Keats Citron, Hate Crimes in Cyberspace, (Cambridge Univ. Press 2014); Eric Goldman, *Unregulating Online Harassment*, 57 Denver U. L. Rev. 60 (2010).

contexts or disproportionately affect marginalized users. To mitigate such risks, regulations could require context-specific thresholds like mandatory identification for paid political ads, but pseudonymous participation allowed for general discourse, with safeguards against misuse through traceable cryptographic keys held by independent trustees.

Digital literacy and public trust must also be reinforced. Without civic resilience, even strong regulations fail. Media literacy in education and support for independent journalism are crucial complementary measures. In order to counter corporate dominance, antitrust rules must evolve. In AI, data-rich incumbents can extract copyright-protected content in ways that may distort competition and raise concerns about creators' rights. Mandatory data-use impact assessments and FRAND licensing obligations for training data can promote fair AI competition. The DMA's gatekeeper logic could be extended to include AI-specific provisions preventing enclosure of training datasets and foundational models.[223] At the same time, competition law, including the DMA, remains a targeted instrument: it is designed to restore contestability and curb specific gatekeeper strategies, not to supply a general-purpose regime for author remuneration, data governance, or democratic integrity. Any AI-facing extension of the DMA's logic would therefore need careful scoping and coordination with copyright, data protection, and the AI Act, rather than presuming that antitrust tools alone can internalize the full set of constitutional and distributive concerns raised by foundation-model ecosystems. More fundamentally, the broader challenge calls for reinterpreting constitutional authority as final constitutional responsibility in order to protect against algorithmic and economic domination. Courts and independent regulators should be empowered to scrutinize digital practices that undermine rights, extending constitutional protections to digital infrastructures.

While geopolitical rivalries hinder the emergence of a unified global regulatory framework, regional alliances remain a viable path for harmonizing digital governance standards. The European Union's efforts through the GDPR, DSA, and DMA have already shaped international debate and inspired normative emulation. As Anu Bradford explains in Digital Empires, the EU, the US, and China are advancing competing regulatory paradigms–rights-driven, market-driven, and state-driven respectively–each seeking to shape the global digital order according to their own political and normative foundations.[224] In this context, targeted cooperation among like-minded jurisdictions on AI governance, cross-border data flows, and algorithmic accountability could provide a strategic pathway toward regulatory convergence without requiring full multilateral alignment. Such interoperability frameworks would help prevent regulatory arbitrage by dominant technology firms and establish common safeguards against the concentration of informational power. Bilateral and plurilateral agreements could serve as functional stepping stones toward broader frameworks, enabling gradual convergence through cumulative norm diffusion

223. *See* Christophe Geiger & Bernd Justin Jütte, *Designing Digital Constitutionalism: Copyright Exceptions and Limitations as a Regulatory Framework for Media Freedom and the Right to Information Online*, *in* Cambridge Handbook of Media L. and Pol'y in Eur. (forthcoming 2025) (arguing copyright exceptions can support media freedom and democratic checks).

224. *See* Anu Bradform, Digital Empires: The Global Battle to Regulate Technology, 324, 325 (Oxford Univ. Press 2023).

and institutional learning. These proposals, though normatively grounded, raise important implementation dilemmas. Transparency mandates may conflict with trade secrets and intellectual property protections; identity verification mechanisms, while enhancing accountability, risk chilling anonymous speech; antitrust reforms face resistance from entrenched incumbents; and jurisdictional fragmentation continues to undermine enforcement efforts. Yet, acknowledging these trade-offs only reinforces the urgency of adaptive, reflexive, and expert-informed legal frameworks. The proposed strategies–from algorithmic audits and platform duties to AI-specific antitrust and data governance–operationalize the tripartite framework of digital constitutional accountability. They offer a roadmap for legislators, regulators, and courts to recalibrate digital infrastructures in accordance with democratic constitutional values, ensuring that innovation does not come at the expense of autonomy, fairness, and institutional legitimacy.

Conclusion

This Article has argued that digital technologies are reshaping the architecture of democratic governance in ways that strain traditional models of accountability and participation. Algorithmic infrastructures now mediate civic space and political communication at scale, while the State's ability to ensure the prescriptive force of constitutional norms is increasingly weakened when governance functions are exercised by private actors through opaque and proprietary systems.

These shifts cannot be adequately addressed through isolated regulatory principles such as privacy or transparency. They require constitutional oversight mechanisms capable of confronting epistemic opacity, normative privatization, and systemic concentration as interconnected dimensions of the same governance problem. The core claim is structural: algorithmic infrastructures reallocate the production of knowledge, the setting of norms, and the conditions of participation to private systems that remain only partially contestable. Without legal architectures capable of interrogating how digital systems generate knowledge, define norms, and structure participation, democratic governance remains vulnerable to forms of algorithmic power that operate below the threshold of institutional visibility and contestation.

The framework also clarifies what a credible reform agenda must accomplish. Epistemically, it requires institutionalized auditability and targeted disclosure obligations for high-impact systems, including in political advertising, recommender infrastructures, and content governance. Normatively, it requires standards of procedural fairness, reason-giving, and contestability that prevent constitutional values from being replaced by discretionary enforcement preferences. Systemically, it requires governance designs that reintroduce counterpower through independent oversight, cross-border coordination, and structural tools that address dominance over data and infrastructures, including competition enforcement and carefully calibrated IP policy.[225]

225. *See e.g.,* Michael A. Heller & Rebecca S. Eisenberg, *Can Patents Deter Innovation? The Anticommons in Biomedical Research*, 280 Sci. 698 (1998); Yochai Benkler, *Intellectual Property and the Organization of Information Production*, 22 Int'l Rev. L. & Econ. 81 (2002).

Because algorithmic governance evolves rapidly, these measures should be coupled with adaptive techniques such as iterative review and sunset mechanisms and complemented by a nuanced approach to online anonymity that preserves its democratic function while allowing conditional verification where persistent abuse threatens democratic integrity.[226]

Beyond its policy implications, this Article identifies a deeper doctrinal gap: across jurisdictions, constitutional law has struggled to conceptualize algorithmic power in structural and infrastructural terms. Whether through the rights-centric orientation often associated with U.S. doctrine, the EU's regulatory model, or the UK's hybrid approach, existing tools frequently fail to capture how private infrastructures organize discourse, shape political preferences, and mediate participation. Digital constitutional accountability provides a conceptual and normative lens for addressing this gap by treating platform power not as a series of isolated infringements, but as a structural challenge to democratic legitimacy. If algorithmic infrastructures increasingly assume functions once reserved to public institutions, they must be subjected to constitutionally grounded accountability built around rights-relevant duties, structured contestability, independent oversight, and effective remedies. Without such a renewal, the constitutional promise of democratic self-government risks being shaped by invisible code and unaccountable infrastructures.

226. *See* Luigi Ferrajoli, Per una Costituzione *della* Terra: l'umanità al bivio, 129 (Bari 2022) (arguing that global constitutionalism is necessary to constrain technological power).

Appendix

Institutional Mapping (Baseline): Dimension → Actors → Tools → Remedies

Table 1. Operational map of the tripartite framework

Accountability dimension	Core institutional actors (illustrative)	Triggering tools and procedures (illustrative)	Remedies and outputs (illustrative)
Epistemic accountability (transparency, intelligibility, auditability)	Independent audit bodies and technical auditors; data protection and transparency authorities; researchers and vetted oversight actors; courts (disclosure litigation).	Access-to-information and disclosure duties; structured transparency reporting; audit mandates and model/system assessments; record-keeping and traceability obligations; investigatory powers and expert review.	Information remedies (disclosure orders, reason-giving, access to logs); corrective transparency (rectification, improved explanations); compliance plans and monitored remediation; sanctions for persistent opacity.
Normative accountability (legitimacy, due process, pluralism in private governance)	Regulators and sectoral supervisors; courts (procedural rights, proportionality, remedies); independent dispute resolution and ombuds-type mechanisms; standard-setting bodies and co-regulatory fora.	Notice-and-action and reasoned decision requirements; appeal and internal complaint-handling systems; due process standards for enforcement; oversight of terms, rules, and enforcement patterns; participatory rulemaking and review of platform policies.	Procedural remedies (reinstatement, reversal, internal reconsideration); injunctive relief and targeted orders; damages or statutory redress where available; requirements to revise rules and enforcement criteria; enhanced user rights in contestation.

Accountability dimension	**Core institutional actors (illustrative)**	**Triggering tools and procedures (illustrative)**	**Remedies and outputs (illustrative)**
Systemic accountability (checks and balances; institutional counterpower; structural governance)	Legislatures and parliamentary oversight; constitutional/ supreme courts; competition and consumer authorities; cross-border and transnational oversight networks; public-interest institutions with supervisory mandates.	Ex ante duties calibrated to scale and systemic impact; independent auditing and risk governance duties; market-structure tools (competition enforcement, interoperability, gatekeeper obligations); periodic review and accountability "learning" mechanisms; coordinated enforcement across jurisdictions.	Structural remedies (behavioral commitments, interoperability, access obligations); governance remedies (independent monitoring, audit follow-up, escalation duties); administrative sanctions and periodic compliance review; institutional reforms that re-embed platforms within public checks.