JOURNAL OF LAW, INFORMATION & SCIENCE
ISSN 0729-1485• Vol. 4, Issue 2 (2026) • https://jlisjournal.com/

REVIEW ARTICLE Article ID: JLIS/2026/4/2/002

Digital Governance and Legal Regulation in the Information Society

Stanley Kinley[1], Irene Hienrich[2]

[1] *Head Legal Associates, Irwin& Sara Institute of Information Science, IS College of Law, University of Cork.*
[2] *Professor, Irwin& Sara Institute of Information Science, IS College of Law, University of Cork.*

Received: 18 March 2026 **Revised:** 28 May 2026 **Accepted:** 28 July 2026 **Published:** 16 Aug 2026

ABSTRACT

The transition to an information society governed increasingly through code, platforms, and data flows has generated distinctive challenges for legal regulation, which has traditionally organized itself around territorially bounded, state-centric authority. This chapter analyses the conceptual foundations of digital governance, surveys competing regulatory models—state command-and-control, industry self-regulation, and multistakeholder governance—and analyses India's evolving statutory architecture from the Information Technology Act, 2000 through the Intermediary Guidelines of 2021 to the Digital Personal Data Protection Act, 2023. It considers intermediary liability jurisprudence, the constitutional anchoring of digital rights following the recognition of informational privacy, and the ongoing difficulties of governing inherently transnational digital infrastructures through domestic legal instruments. This chapter maintains that effective digital governance requires layered regulatory strategies combining statutory obligation, technical standard-setting, and constitutional rights review.

Keywords: *digital governance; internet regulation; intermediary liability; data protection; information technology law; platform accountability.*

Introduction

The information society is characterized by the pervasive mediation of social, economic, and political life through digital networks, platforms, and data-processing systems. This transformation has outpaced the doctrinal categories of traditional legal regulation, which developed to govern territorially situated conduct by identifiable actors within relatively stable technological conditions. Digital governance—the composite body of law, technical standards, institutional arrangements, and private ordering that structures behaviour in digital environments—has therefore emerged as a distinct field of legal inquiry, straddling public law, private regulation, and international coordination. This chapter traces the conceptual foundations of digital governance and situates India's regulatory trajectory within the more general global debate over how information societies ought to be governed.

Conceptualizing Digital Governance

Lawrence Lessig's influential account identified four modalities through which behaviour in digital environments is regulated: law, social norms, market forces, and 'code'—the technical architecture of software and hardware systems, which Lessig argued functions as a de facto regulator every bit as powerful as formal legal rules, since it can make certain conduct technically impossible rather than merely legally prohibited.[1] This insight reframes digital governance as extending beyond conventional statutory regulation to encompass the deliberate or incidental regulatory effects of technical design choices made by platform architects and standard-setting bodies.

Jack Goldsmith and Tim Wu challenged early cyber-libertarian assumptions that the internet was inherently unregulable by sovereign states, documenting instead how states successfully asserted jurisdiction over internet intermediaries and infrastructure located within, or transacting with, their territory, thereby re-establishing meaningful, if imperfect, governmental control over digital conduct.[2] Julie Cohen's more recent work emphasizes that digital governance today is shaped to a substantial degree by the informational capitalism of dominant platform firms, whose data-extractive business models generate governance effects—shaping speech, commerce, and behaviour at scale—that increasingly rival, and sometimes exceed, those of formal state regulation.[3]

Models of Internet and Platform Regulation

Three broad regulatory models have shaped the governance of digital infrastructure and platforms. The first, state command-and-control regulation, relies on binding statutory obligations enforced through administrative and judicial mechanisms, exemplified by data protection statutes and cybersecurity mandates. The second, industry self-regulation, delegates standard-setting and enforcement to private actors, often through codes of conduct or terms of service, on the premise that technical expertise and adaptability reside more readily within industry than within legislatures. The third, multistakeholder governance, seeks to integrate government, industry, technical community, and civil society within shared institutional processes, a model most closely associated with internet governance bodies such as the Internet Corporation for Assigned Names and Numbers and reflected in the outcomes of the World Summit on the Information Society's Tunis Agenda.[4]

Jody Freeman's account of 'co-regulation' bridges these categories, describing hybrid arrangements in which state authority sets binding regulatory objectives while delegating implementation and enforcement detail to

[1]Lawrence Lessig, Code and Other Laws of Cyberspace (Basic Books, 1999), and the revised edition, Code: Version 2.0 (Basic Books, 2006).

[2]Jack Goldsmith & Tim Wu, Who Controls the Internet? Illusions of a Borderless World (Oxford University Press, 2006).

[3]Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism (Oxford University Press, 2019).

[4]World Summit on the Information Society, Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6(Rev.1)-E (2005), paras 29-82, articulating the multistakeholder approach to internet governance.

private or quasi-private bodies operating under public oversight, an arrangement increasingly visible in platform content-moderation regimes that combine statutory obligations with platform-designed enforcement mechanisms.[5] Milton Mueller's institutional analysis of internet governance similarly cautions that no single model has proven fully adequate, given the tension between the internet's transnational technical architecture and the persistently national basis of legal sovereignty and enforcement authority.[6]

India's Statutory Architecture: From the IT Act to the DPDP Act

India's digital governance framework originated with the Information Technology Act, 2000, enacted to provide legal recognition for electronic transactions and to create offences for computer-related contraventions, subsequently amended in 2008 to expand its scope to cybersecurity, data protection, and intermediary liability. Section 66A of the Act, which criminalized sending offensive messages through communication services, was struck down by the Supreme Court in Shreya Singhal v. Union of India on the ground that its vague and overbroad language had a chilling effect on protected speech inconsistent with Article 19(1)(a).[7] The judgment remains the foundational Indian precedent constraining digital speech regulation within constitutional limits.

The regulatory architecture was appreciably reworked through the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which introduced due-diligence obligations for social media intermediaries, including grievance redressal mechanisms, traceability requirements for notable social media intermediaries, and a distinct regulatory framework for digital news and OTT content through a three-tier self-regulatory structure.[8] The most substantial recent development is the Digital Personal Data Protection Act, 2023, which establishes a consent-based framework for processing digital personal data, creates the Data Protection Board of India as an adjudicatory authority, and imposes graded obligations on data fiduciaries proportionate to the volume and sensitivity of personal data processed.[9] This legislative sequence captures a gradual shift from a transaction-facilitation statute toward a thorough framework addressing platform accountability and informational self-determination.

The Digital Personal Data Protection Act's consent-centric architecture invites comparison with the European Union's General Data Protection Regulation, which similarly requires a lawful basis for processing but recognises a wider range of such bases, including legitimate interest, alongside more extensively codified data subject rights of access, rectification, erasure, and portability, and markedly higher maximum financial

[5]Jody Freeman, 'The Private Role in Public Governance' (2000) 75 New York University Law Review 543.
[6]Milton L. Mueller, Networks and States: The Global Politics of Internet Governance (MIT Press, 2010).
[7]Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[8]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, notified under Sections 69A, 79, and 87 of the Information Technology Act, 2000.
[9]Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), Sections 4-10 (grounds for processing) and Sections 18-26 (Data Protection Board).

penalties for non-compliance.[10] Indian scholars and policymakers have debated whether the DPDP Act's comparatively streamlined consent-and-notice framework, paired with wide exemptions for state processing in the interests of sovereignty, security, and public order, achieves an appropriate balance between facilitating India's data-driven digital economy and providing meaningful individual control over personal data, a debate that is likely to shape the framework's implementing rules and early enforcement practice before the Data Protection Board.

Cybersecurity Regulation and Critical Information Infrastructure

Beyond data protection, digital governance encompasses the distinct regulatory domain of cybersecurity, addressed in India principally through Sections 70 and 70A of the Information Technology Act, which empower the government to declare protected systems and critical information infrastructure and to designate a nodal agency for their protection, and through the Indian Computer Emergency Response Team, functioning as the national agency for incident response under Section 70B.[11] The Indian Computer Emergency Response Team's 2022 directions on cybersecurity incident reporting mandated that a wide category of service providers, intermediaries, and data centres report specified categories of cybersecurity incidents within six hours of detection and maintain prescribed logs for defined retention periods, a compressed reporting timeline that generated sizeable industry debate over its operational feasibility and jurisdictional reach.[12]

Cybersecurity regulation reveals a governance challenge distinct from, though related to, data protection: while data protection law centres on the rights of the individual data principal against a data fiduciary, cybersecurity regulation is oriented toward systemic resilience and national security, often justifying more expansive and less individually contestable regulatory obligations. The layering of these two regulatory logics—rights-protective data governance and security-oriented cyber regulation—within a single digital governance architecture requires careful doctrinal calibration to avoid security-justified exceptions from swallowing the rights guarantees that data protection law is designed to secure. The Digital Personal Data Protection Act's own exemptions for processing in the interests of sovereignty, security, and public order, discussed above, demonstrate precisely this interface, and the manner in which the Data Protection Board and constitutional courts interpret the boundaries of such exemptions will materially determine whether India's digital governance framework maintains a workable equilibrium between security-driven regulation and individual data rights.

Intermediary Liability and Platform Accountability

[10]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Articles 5-6 and 12-22.

[11]Information Technology Act, 2000, Sections 70, 70A, and 70B.

[12]Indian Computer Emergency Response Team, Directions under Section 70B(6) of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents (28 April 2022).

Section 79 of the Information Technology Act provides intermediaries a conditional safe harbour from liability for third-party content, provided they observe due diligence and do not initiate the transmission, select the receiver, or modify the content in question. The Delhi High Court's decision in MySpace Inc. v. Super Cassettes Industries Ltd. considered the scope of this safe harbour in the context of copyright infringement claims, addressing when actual knowledge of infringing content, as opposed to generalized awareness, triggers an intermediary's obligation to act.[13] The related decision in Kent RO Systems Ltd. v. Amit Kotak further examined intermediaries' obligations upon receiving a specific complaint alleging infringement, holding that intermediaries are not required to independently adjudicate infringement claims but must act upon court orders or properly constituted notices.[14]

These decisions show the recurring tension in platform accountability doctrine between imposing proactive monitoring obligations—which raise concerns of privatized censorship and disproportionate compliance burdens—and preserving a narrow, notice-based liability standard that may leave harmful content inadequately addressed. Comparative reference is frequently made to the European Union's e-Commerce Directive and its successor, the Digital Services Act, which similarly conditions intermediary immunity on the absence of actual knowledge and imposes graduated due-diligence obligations scaled to platform size and systemic risk, a model that has influenced subsequent Indian regulatory thinking on differentiated obligations for consequential social media intermediaries.[15]

The traceability requirement introduced for meaningful social media intermediaries under the 2021 Rules has proven especially contentious, obliging such platforms to enable identification of the first originator of specified categories of information upon judicial or competent authority order. Messaging platforms employing end-to-end encryption have argued that compliance would require fundamentally re-engineering their encryption architecture in ways that compromise the confidentiality of all users' communications, not merely those under investigation, framing the requirement as disproportionate under the Puttaswamy privacy standard discussed later in this chapter. The unresolved status of this dispute exemplifies a recurring structural problem in platform accountability regulation: technical design choices made for security or business reasons can themselves become the site of marked, and not always fully anticipated, constitutional contestation.

Digital Rights and Constitutional Anchoring

The constitutional foundation for digital governance in India was appreciably strengthened by the recognition of a fundamental right to privacy in Justice K.S. Puttaswamy (Retd.) v. Union of India, where a nine-judge bench held privacy, including informational privacy, to be intrinsic to the right to life and personal liberty under Article 21.[16] The decision established that any state action restricting privacy, including digital

[13]MySpace Inc. v. Super Cassettes Industries Ltd., 236 (2017) DLT 478 (Delhi High Court).
[14]Kent RO Systems Ltd. v. Amit Kotak, 2017 SCC OnLine Del 7201.
[15]Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 (Digital Services Act), Articles 4-6 and 33-43.
[16]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

surveillance or mandatory data collection, must satisfy a threefold test of legality, legitimate state aim, and proportionality. This standard was subsequently applied in the Aadhaar judgment, Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar case), where the Court upheld the constitutional validity of the Aadhaar biometric identification scheme subject to notable reading-down of provisions permitting private-sector use of Aadhaar data.[17]

Anuradha Bhasin v. Union of India extended proportionality analysis to internet access restrictions, holding that indefinite suspension of internet services could not be sustained without periodic review and that freedom of trade and expression through the internet enjoyed constitutional protection under Articles 19(1)(a) and 19(1)(g).[18] Together, these decisions constitute a body of digital constitutional rights jurisprudence that anchors statutory digital governance instruments within enforceable constitutional limits, ensuring that regulatory or platform-facilitated intrusions on digital rights remain subject to judicial scrutiny.

Digital Public Infrastructure and E-Governance

A distinctive feature of India's digital governance landscape is the state's role not merely as regulator but as architect of foundational digital public infrastructure. The Aadhaar Act, 2016 established a statutory basis for a biometric and demographic identification system intended to facilitate targeted delivery of subsidies, benefits, and services, following its earlier operation under executive notification without dedicated legislative backing.[19] The constitutional validation of Aadhaar in the 2019 Puttaswamy judgment, subject to restrictions on private-sector use, has shaped the subsequent expansion of interoperable digital public infrastructure, including the Unified Payments Interface for real-time digital payments and the larger 'India Stack' framework of application programming interfaces enabling identity verification, paperless documentation, and consent-based data sharing across public and private service providers.

This model of state-built digital public infrastructure, layered with privately developed applications and services, has been described by policymakers as a distinctive alternative to both the primarily state-controlled digital governance model associated with some jurisdictions and the primarily platform-controlled model associated with dominant private technology firms elsewhere. Its legal governance nonetheless raises questions that remain only partially settled: the adequacy of consent mechanisms embedded in infrastructure that citizens have limited practical ability to opt out of where such infrastructure becomes a de facto precondition for accessing essential services, the allocation of liability for infrastructure failures or data breaches occurring across a multi-party technical stack, and the mechanisms available for individuals to seek redress against algorithmic or infrastructural decisions with material consequences for access to entitlements.

Global Governance and Cross-Border Challenges

[17] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1.
[18] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
[19] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, Sections 3-8.

The transnational architecture of digital infrastructure generates ongoing jurisdictional and enforcement difficulties for domestically legislated governance frameworks. The Budapest Convention on Cybercrime, the first international treaty addressing cross-border cybercrime cooperation, established mechanisms for mutual legal assistance and expedited preservation of electronic evidence, though its adoption remains uneven among major digital economies, including India, which has not acceded to it.[20] The Organisation for Economic Co-operation and Development's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, though non-binding, have exercised marked normative influence on the design of subsequent national data protection statutes, including principles of purpose limitation, data quality, and accountability reflected in India's Digital Personal Data Protection Act.[21]

These transnational frameworks demonstrate a larger structural challenge: digital infrastructure, data flows, and platform operations routinely cross jurisdictional boundaries in ways that domestic statutes, however thorough, cannot fully address in isolation. Effective digital governance therefore increasingly requires layered strategies combining domestic constitutional and statutory regulation with international coordination on cross-border data transfer, mutual legal assistance, and interoperable technical standards.

Cross-border data transfer regulation exemplifies this layered challenge in concrete form. The Digital Personal Data Protection Act, 2023 adopts a comparatively liberal approach, permitting transfer of personal data to countries outside India except those specifically restricted by government notification, a 'blacklist' approach that departs from the European Union's 'adequacy' model, under which transfers are permitted only to jurisdictions the European Commission has affirmatively determined to provide an essentially equivalent level of data protection.[22] This divergence in cross-border transfer philosophy has practical consequences for Indian businesses seeking to process data originating from jurisdictions that apply adequacy-based restrictions, since compliance with India's domestic framework does not, by itself, satisfy the receiving obligations imposed by counterpart jurisdictions with stricter transfer regimes, requiring Indian data processors engaged in cross-border business to navigate multiple, only partially harmonised regulatory frameworks simultaneously.

Conclusion

Digital governance occupies an increasingly central position within contemporary legal regulation, requiring the integration of constitutional rights analysis, statutory intermediary obligations, technical standard-setting, and international coordination. India's regulatory trajectory—from the facilitative Information Technology Act, 2000 through the due-diligence obligations of the 2021 Intermediary Guidelines to the extensive Digital Personal Data Protection Act, 2023—embodies a maturing statutory architecture increasingly anchored in the constitutional recognition of privacy as a fundamental right. Yet the continuing tension between platform

[20]Council of Europe, Convention on Cybercrime (Budapest Convention), ETS No. 185 (2001).
[21]OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980, revised 2013).
[22]Digital Personal Data Protection Act, 2023, Section 16; compare General Data Protection Regulation, Article 45 (adequacy decisions).

accountability and free expression, between effective enforcement and privatized censorship, and between domestic regulatory sovereignty and the transnational architecture of digital infrastructure ensures that digital governance will remain among the most dynamic and contested areas of contemporary legal regulation.

Looking ahead, the maturation of India's digital governance framework will depend substantially on the institutional capacity and independence of the bodies charged with its implementation, including the Data Protection Board of India and the technical and grievance-redressal mechanisms established under the Intermediary Guidelines. Statutory text alone cannot secure effective digital governance where implementing institutions lack adjudicatory independence, technical expertise, or adequate resourcing. As digital infrastructure becomes further embedded in the delivery of essential public services, the legal community's task extends beyond the interpretation of individual statutory provisions to the overarching constitutional project of ensuring that the immense administrative and commercial power concentrated in digital systems remains answerable to the rights-bearing individuals whose lives those systems increasingly govern.

Declarations

Conflict of interest: The author declares that they have no conflict of interest.

Funding: This review received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Ethical approval: Not applicable. This article is a review of published literature and did not involve human participants or animal subjects.

Data availability: No new data were generated or analysed in support of this review. All sources relied upon are cited in the References.

Use of AI tools: No generative artificial intelligence tool was used in the conception, drafting or analysis of this article. The authors take full responsibility for the content.

Author contributions: Author contributed to the conception of the review, the survey of the literature, and the drafting and revision of the manuscript. Author read and approved the final version.