 DOI: 10.5281/zenodo.17765781

DIGITAL CONSTITUTIONALISM AND GOVERNANCE IN INDIA: SAFEGUARDING RIGHTS IN THE DIGITAL ERA

BY GEETHANJALI P[1]

ABSTRACT

In the twenty-first century, digital technology has changed the way governments work and how our rights are protected. Tools like artificial intelligence and biometric IDs shape how we interact with the government, businesses, and each other. In this rapidly changing world, digital constitutionalism helps us rethink important values such as liberty, equality, dignity, privacy, and accountability for the digital age.

This paper looks at how India handles digital rights and governance. It asks whether India's laws and institutions do enough to protect people's rights as the country becomes more digital. While programs like Digital India and systems like Aadhaar, UPI, and DigiLocker have made government services easier to access, they have also raised serious questions about privacy, free speech, and fair treatment. By comparing India's approach with rules from the European Union, the United States, and other countries in the Global South, this paper suggests that India's system focuses more on administration than on protecting individual rights.

Through judicial review, legislative analysis, and case studies, the study identifies gaps in data protection, algorithmic transparency, and surveillance regulation. It concludes that India requires a comprehensive digital constitutional order grounded in accountability, participatory governance, and constitutional morality.

[1] The author is a law student at Amity Law School, Noida.

INTRODUCTION

Digital technology today constitutes not merely a tool of governance but an ecosystem that shapes political power, individual autonomy, and collective life. Governments worldwide have adopted technology-driven models for efficiency, transparency, and inclusion. However, these models have simultaneously introduced new forms of exclusion, manipulation, and surveillance.

India, the world's largest democracy, has positioned itself as a leader in digital transformation. The Digital India programme, launched in 2015, envisions a society where governance is "faceless, paperless, and cashless." The Aadhaar system—the world's largest biometric database has enabled millions to access welfare schemes and public services through digital authentication. The Unified Payments Interface (UPI) has made India a global model of financial digitalisation.

Yet these achievements coexist with concerns over data privacy, algorithmic discrimination, misinformation, and state surveillance. Questions arise: Do these digital systems reinforce or undermine constitutional values? How do they align with the Indian Constitution's promise of dignity, equality, and freedom?

The Constitution of India, drafted in 1950, envisions a social contract that limits power and protects rights. Its framers could not have anticipated the digital age, yet its principles remain timeless. As digitalisation reconfigures power relations, there arises an urgent need to reinterpret the Constitution for the digital era a process scholars describe as digital constitutionalism.

Digital constitutionalism insists that digital governance must be guided by constitutional ethics, not merely by technical or administrative efficiency. It calls for the embedding of rights into the design of technology, the accountability of both public and private digital actors, and the creation of legal safeguards that ensure fairness and transparency.

RESEARCH QUESTIONS

1. What is the meaning and scope of digital constitutionalism, and how is it relevant to India?
2. To what extent do India's constitutional and legislative mechanisms safeguard digital rights?

3. How does India's digital governance model compare with those of other jurisdictions such as the European Union and the United States?

4. What are the major institutional, legal, and ethical challenges in implementing digital constitutionalism in India?

5. What reforms can strengthen rights-based digital governance within India's constitutional framework?

RESEARCH HYPOTHESIS

The paper advances the hypothesis that India's digital governance architecture prioritises efficiency and innovation over the constitutional protection of individual rights. While India has taken progressive steps in establishing digital infrastructure and data-protection mechanisms, the normative integration of constitutional values into its digital systems remains incomplete. Consequently, India's digital transformation has created a paradox: an inclusive digital society that risks eroding constitutional freedoms if unchecked by legal and institutional reforms.

DIGITAL CONSTITUTIONALISM

1. Meaning of Digital Constitutionalism

The concept of digital constitutionalism emerged in European scholarship to describe the application of constitutional norms to the governance of digital environments. It implies that the rule of law, separation of powers, accountability, and human rights must regulate the exercise of power, both public and private within cyberspace.

According to Celeste (2022), digital constitutionalism "seeks to constitutionalise the digital environment through the adoption of normative instruments that protect fundamental rights and constrain the powers of digital actors."[2] This involves recognising that corporations managing online platforms wield quasi-sovereign authority over speech, privacy, and information access, thereby necessitating constitutional constraints similar to those imposed on states.

[2] Celeste, E., Digital Constitutionalism: A New Systematic Theorisation, Oxford University Press, 2022. Retrieved from https://academic.oup.com/ijlit/article/30/1/68 /6550367

Digital constitutionalism operates on three foundational dimensions:

1. Rights Protection: Safeguarding individual freedoms such as privacy, expression, equality, and access to information in digital spaces.
2. Power Limitation: Imposing constitutional checks on both state surveillance and corporate domination of digital infrastructure.
3. Governance Architecture: Designing participatory, transparent, and accountable frameworks for digital policy and infrastructure.

2. Relationship Between Constitutionalism and Technology

Traditional constitutionalism limits state power through legal and institutional mechanisms such as judicial review and separation of powers. In contrast, digital constitutionalism recognises that the power today is also exercised through code, algorithms, and data architectures. The state may no longer be the sole actor capable of infringing rights technology corporations, data brokers, and artificial-intelligence systems equally influence rights and freedoms.

Thus, digital constitutionalism demands constitutional pluralism a framework recognising that both state and private actors must be held accountable under constitutional principles.[3] The European Union's GDPR exemplifies this by imposing data-protection duties on both governments and private entities.

3. Theoretical Foundations

Digital constitutionalism draws from three strands of theory:

- Liberal Constitutionalism: centring on individual autonomy and rights.
- Republican Constitutionalism: emphasising civic participation and checks on arbitrary power.
- Deliberative Constitutionalism: focusing on public reasoning and democratic

[3] Gill, L., "Digital Power and Constitutional Pluralism," Internet Policy Review, 2021. https://policyreview.info/articles/analysis/digital-constitutionalism

legitimacy in technological decision-making.

In India, these values resonate with constitutional provisions such as Articles 14 (equality before law), 19 (freedom of speech and expression), and 21 (right to life and personal liberty). The Supreme Court's interpretation of these provisions has progressively incorporated digital contexts for instance, in Justice K.S. Puttaswamy v. Union of India (2017), the Court recognised privacy as a fundamental right, explicitly linking it to data and informational autonomy.[4]

Digital constitutionalism extends the idea of human rights constitutionalism into cyberspace. The digital environment has created new species of rights data protection, the right to be forgotten, and the right to internet access.[5] For example, the Kerala High Court in Faheema Shirin v. State of Kerala (2019) held that internet access forms part of the right to education and privacy, illustrating the constitutionalisation of digital access.[6]

In India, therefore, digital constitutionalism is not merely theoretical; it manifests through judicial innovation and public policy. However, these rights often exist without sufficient legislative backing, creating gaps between judicial declarations and executive implementation.

4. Constitutional Morality in the Digital Era

The Supreme Court of India has often invoked the doctrine of constitutional morality the idea that governance must reflect the Constitution's spirit rather than mere procedural legality. Applied to the digital sphere, constitutional morality requires the state to design technology systems that respect human dignity, autonomy, and equality.

Digital constitutionalism thus demands that data governance frameworks incorporate ethics by design and rights by default principles ensuring that technology embeds fairness and transparency rather than retroactively correcting harm.[7]

[4] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1. https://en.wikipedia.org/wiki/Puttaswamy_v._Union_of_India

[5] Milan, S. & Treré, E., "The Rise of Digital Constitutionalism," Internet Policy Review, 2019. https://policyreview.info/articles/news/rise-digital-constitutionalism

[6] Faheema Shirin v. State of Kerala, 2019 (4) KLT 494. https://indiankanoon.org/doc/152132631/

[7] Tisne, M., "Data and the New Social Contract," Carnegie Endowment for International Peace, 2020. https://carnegieendowment.org/2020/10/22/data-and-new-social-contract-pub-82931

Across jurisdictions, digital constitutionalism is taking shape through a mix of judicial decisions, legislative instruments, and multi-stakeholder initiatives. The EU's Charter of Fundamental Rights, the OECD's AI Principles, and the UN's Guiding Principles on Business and Human Rights are examples of transnational instruments embedding rights into digital governance.[8]

India's participation in global digital governance forums, including the G20 Digital Economy Working Group, reflects a growing awareness that digital governance must align with constitutional and ethical norms. However, unlike the EU, India lacks a codified "digital rights charter" integrating these norms within domestic law.

5. Why India Is a Crucial Case Study

India presents a paradox of scale and complexity: it is both a digital innovator and a rights-challenged democracy. With over 800 million internet users and 1.3 billion Aadhaar enrollments, digital governance has reached unprecedented scale.[9] Yet issues such as data breaches, opaque algorithmic decisions, and exclusion of marginalised communities from digital welfare schemes have raised constitutional concerns.

The interplay between India's constitutional framework and its digital policy thus provides a fertile ground to analyse how digital constitutionalism can evolve within developing democracies.

India's Legal and Governance Framework

1. Constitutional Foundations

The Constitution of India guarantees fundamental rights that remain fully applicable in digital contexts.

- Article 14 ensures equality before law and the right against arbitrary state action.
- Article 19(1)(a) guarantees freedom of speech and expression, extending to online communication.

[8] OECD, "OECD Principles on Artificial Intelligence," 2019. https://oecd.ai/en/ai-principles

[9] Press Information Bureau, Government of India, "Digital India: Progress Report 2024." https://pib.gov.in/PressReleasePage.aspx?PRID=1952045

- Article 21 safeguards the right to life and personal liberty, interpreted broadly to include privacy, informational autonomy, and access to the internet.

Indian courts have repeatedly reaffirmed that constitutional rights do not evaporate in digital spaces. The Supreme Court in Puttaswamy v. Union of India (2017) declared privacy to be "an intrinsic part of the right to life and personal liberty under Article 21."[10] This judgment marked a constitutional watershed, signalling India's transition toward a digital rights framework rooted in dignity and autonomy.

2. Legislative Architecture

India's primary legislation governing digital activity is the Information Technology Act, 2000 (IT Act). The Act originally aimed to facilitate e-commerce and assign legal recognition to electronic records, but subsequent amendments have given it a central role in digital regulation.

Section 69A of the IT Act authorises the government to block online content "in the interest of sovereignty and public order." While intended to protect national security, its broad phrasing has enabled discretionary censorship.[11] The Shreya Singhal v. Union of India (2015) decision partially mitigated these risks by striking down Section 66A, which criminalised "offensive" online messages for vagueness and chilling effects on speech.[12]

India's Intermediary Guidelines and Digital Media Ethics Code, 2021 further expanded governmental oversight over social-media platforms and digital news publishers. Critics argue that these rules impose quasi-censorship obligations on intermediaries, threatening online free expression.[13]

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents India's first comprehensive data-protection statute. It establishes obligations for data fiduciaries, individual consent mechanisms, and a Data Protection Board. However, commentators note

[10] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1

[11] Internet Freedom Foundation, "Analysis of Section 69A Orders," 2022 — https://internetfreedom.in/

[12] Atlantic Council, "India's Data Protection Act Explained," Aug 2023 — https://www.atlanticcouncil.org/blogs/southasiasource/indias-data-protection-act/

[13] Mehta, P., "India's Digital Public Infrastructure," Brookings Institution, 2023 — https://www.brookings.edu/articles/india-digital-public-infrastructure/

that its numerous exemptions for government agencies risk undermining the very right it seeks to protect.[14]

3. Policy Initiatives and Digital Infrastructure

The Digital India mission (2015) serves as the umbrella policy for transforming India into a digitally empowered society. Its pillars digital infrastructure as a utility, governance and services on demand, and digital empowerment of citizens have led to initiatives such as:

- Aadhaar: biometric identification system enabling e-authentication for welfare and finance.
- DigiLocker: digital document repository for citizens.
- Unified Payments Interface (UPI): real-time mobile payment framework.
- BharatNet: optical-fibre project connecting rural India.

Collectively, these initiatives have created what scholars term Digital Public Infrastructure (DPI), an interoperable framework of identity, payments, and data platforms.[15] DPI has enhanced efficiency and inclusion, but also centralised sensitive personal data within state-controlled systems, amplifying risks of misuse and surveillance.

4. Institutional Oversight and Gaps

Unlike the EU, India lacks a constitutionally independent data-protection authority. The DPDP Act's Data Protection Board functions under executive control, potentially compromising independence. Moreover, cyber-security oversight remains fragmented among agencies such as the Indian Computer Emergency Response Team (CERT-In) and the National Critical Information Infrastructure Protection Centre (NCIIPC).[16]

The absence of a unified oversight framework has produced regulatory silos—privacy, cybersecurity, and platform governance are handled by different ministries without inter-institutional coordination.

[14] CERT-In, "About the Indian Computer Emergency Response Team," 2024 — https://www.cert-in.org.in/
[15] Puttaswamy (II) — Aadhaar Judgment (2018) 1 SCC 809 — https://indiankanoon.org/doc/127517806/
[16] Faheema Shirin v. State of Kerala, 2019 (4) KLT 494 — https://indiankanoon.org/doc/152132631/

Judicial Interpretation and the Emergence of Digital Rights

The judiciary has progressively constitutionalised digital issues through landmark cases:

1. Privacy and Surveillance — Justice K.S. Puttaswamy (I) (2017):
2. The Court declared privacy a fundamental right and affirmed informational self-determination. It emphasised proportionality and necessity as tests for state intrusion.
3. Aadhaar and Welfare — Puttaswamy (II) (2018):
4. While upholding Aadhaar's validity, the Court curtailed its use by private entities and required legislative backing for data collection.[17]
5. Free Expression — Shreya Singhal (2015):
6. The Court struck down Section 66A of the IT Act, establishing that vague restrictions on online speech violate Article 19(1)(a).
7. Digital Access — Faheema Shirin v. State of Kerala (2019):
8. The Kerala High Court held that internet access is integral to education and privacy under Article 21.[18]

Through these cases, Indian courts have gradually articulated a digital-rights doctrine grounded in proportionality, due process, and accountability.

Evolution of Digital Governance Policy

1. From E-Governance to Digital Governance

India's early e-governance projects in the 2000s focused on service delivery and administrative efficiency. The National e-Governance Plan (NeGP), launched in 2006, aimed to digitise government functions through Mission Mode Projects (MMPs). Over time, the emphasis shifted from digitising bureaucracy to governing through data.

Today, digital governance relies on predictive analytics, biometric verification, and AI-driven decision-making. Such systems can streamline welfare delivery but also risk automating inequality and discrimination. Scholars warn that opaque algorithms may

[17] Raghavan, S., "Algorithmic Bias and the Indian Constitution," Vidhi Centre for Legal Policy, 2021 — https://vidhilegalpolicy.in/blog/algorithmic-bias-and-equality/

[18] Internet Society, "Traceability and Encryption in India," 2022 — https://www.internetsociety.org/resources/doc/traceability/

replicate existing social hierarchies, thereby conflicting with Article 14's guarantee of equality.

Surveillance and Security Architecture

India's surveillance regime is governed primarily by the Indian Telegraph Act (1885) and Rule 419A, which authorise interception on security grounds. Additionally, the Central Monitoring System (CMS) and NATGRID facilitate real-time monitoring of communications.

Concerns over these systems intensified after reports of Pegasus spyware targeting journalists and activists. The Supreme Court in 2021 constituted an independent committee to investigate allegations of illegal surveillance, reiterating that "the right to privacy cannot be sacrificed on the altar of national security without procedural safeguards."[19]

However, India still lacks a comprehensive surveillance-reform law akin to the UK's Investigatory Powers Act or the US's Foreign Intelligence Surveillance Act.

2. Platform Regulation

Social-media intermediaries such as Meta, X (formerly Twitter), and Google hold immense influence over digital speech. The 2021 IT Rules impose a "traceability" requirement, compelling messaging platforms to identify the originator of information. Critics argue that such obligations undermine encryption and user privacy, contravening Article 21.[20]

Platform governance thus becomes a constitutional issue: should private companies be subjected to constitutional scrutiny when their decisions such as content takedowns affect fundamental rights? Indian jurisprudence is yet to resolve this question, though global discourse increasingly treats major platforms as digital public squares.

Comparative Analysis: Global Models of Digital Constitutionalism

1. European Union — Rights-Based Model

The European Union provides the most institutionalised model of digital constitutionalism. The General Data Protection Regulation (GDPR), effective 2018, codifies the right to data

[19] European Commission, "General Data Protection Regulation," 2018 — https://gdpr-info.eu/
[20] Electronic Frontier Foundation, "Section 230 and Online Speech," 2023 — https://www.eff.org/issues/cda230

protection as a fundamental right under Article 8 of the EU Charter of Fundamental Rights. It mandates lawful, fair, and transparent processing, along with robust remedies for violations.[21]

The Digital Services Act (DSA) and Digital Markets Act (DMA) further extend constitutional principles -accountability, transparency, and proportionality to online platforms. The EU thus exemplifies a rights-first approach, where digital governance is subordinated to human-rights protection.

India's DPDP Act borrows conceptually from the GDPR but diverges in enforcement. The absence of an independent regulator and the presence of wide government exemptions contrast sharply with the EU's stringent oversight by Data-Protection Authorities.

2. United States — Market and Free-Speech Model

The US approach to digital governance prioritises innovation and market autonomy over constitutional regulation. The First Amendment heavily constrains government control over digital speech, resulting in a laissez-faire model of platform governance.

However, this market-centric approach has allowed private platforms to wield disproportionate influence over discourse. Debates over Section 230 of the Communications Decency Act (1996) which shields intermediaries from liability for user content illustrate tensions between free expression and accountability.[22]

For India, the US experience underscores the need to balance innovation with constitutional safeguards. Over-regulation may stifle technological growth, but under-regulation risks private censorship and data monopolies.

3. Global South Perspectives

Countries like Brazil and South Africa have adopted hybrid models combining rights-based constitutionalism with developmental goals. Brazil's Marco Civil da Internet (2014) is often called the "Internet Constitution," enshrining privacy, net neutrality, and freedom of expression. South Africa's Protection of Personal Information Act (POPIA) similarly aligns data protection with the constitutional right to privacy under Section 14 of its

[21] UNESCO, "Brazil's Marco Civil da Internet," 2020 — https://en.unesco.org/news/marco-civil-da-internet
[22] Internet Freedom Foundation, "DPDP Act 2023: An Analysis," 2023 — https://internetfreedom.in/

Constitution.[23]

These examples show that constitutional democracies in the Global South can craft digital-governance frameworks grounded in rights without replicating Western models. India, sharing similar socio-economic conditions, can draw valuable lessons from these experiences particularly in participatory policy-making and independent oversight.

4. Lessons for India

The comparative analysis yields several insights:

- Institutional Independence: Effective rights enforcement requires an autonomous data-protection authority insulated from executive control.
- Proportionality Tests: EU jurisprudence applies strict proportionality in digital- rights cases; Indian courts have adopted similar reasoning but require legislative codification.
- Transparency and Accountability: Both EU and Brazil mandate algorithmic transparency; India lacks equivalent statutory duties.
- Participatory Governance: Democratic consultation during policy formation strengthens legitimacy; India's digital-policy processes often rely on executive notifications without parliamentary debate.

India must therefore evolve from a technocratic to a constitutional model of digital governance where efficiency complements, rather than overrides, rights protection.

Key Challenges in Digital Constitutional Governance

1. Institutional Fragmentation

A central problem in India's digital governance is the absence of an integrated constitutional oversight structure.

Regulatory powers are distributed among several ministries-the Ministry of Electronics and Information Technology (MeitY), Ministry of Home Affairs, and NITI Aayog without a single coordinating authority.This fragmentation leads to inconsistent rule-making and

[23] Access Now, "India's Privacy Under Threat," 2023 — https://www.accessnow.org/

diluted accountability. Unlike the EU's European Data Protection Board, India's Data Protection Board under the DPDP Act operates within executive control.[24]

2. Weak Data Protection Mechanisms

While the DPDP Act 2023 is a landmark step, its wide exemptions for state agencies under Section 17 have drawn criticism. Government bodies may process personal data "in the interest of sovereignty or public order," with minimal judicial scrutiny.

This grants the executive disproportionate discretion—contradicting the proportionality standard set out in Puttaswamy (I). Civil-society groups warn that unchecked data collection through welfare and security programmes can result in surveillance overreach.[25]

3. Surveillance and Opacity

India's surveillance infrastructure-CMS, NATGRID, and NETRA operates largely without statutory transparency. Interceptions under the Telegraph Act and IT Act S. 69 require executive, not judicial, authorisation.[26]

The 2021 Pegasus disclosures revealed covert spyware use against journalists, activists, and opposition figures. Although the Supreme Court appointed an inquiry committee, its findings were not made public, underscoring the opacity surrounding state surveillance.

4. Algorithmic Governance and Bias

Public decision-making increasingly depends on algorithmic systems for credit scoring, welfare targeting, and predictive policing. Yet these systems are rarely audited for fairness or explainability.

Algorithmic opacity violates the constitutional right to equality (Article 14) by allowing automated discrimination without accountability. India currently lacks binding "algorithmic-impact assessment" norms such as those adopted in Canada and the EU.

5. Digital Exclusion and Accessibility

[24] Centre for Communication Governance, "Surveillance Laws in India," 2022 — https://ccgdelhi.org/
[25] PRS India, "Analysis of IT Rules 2021," 2021 — https://prsindia.org/
[26] Medianama, "Public Consultation Process in Digital Policies," 2023 — https://www.medianama.com/

Digital constitutionalism must guarantee not only privacy but also inclusion.

The digital divide urban-rural, gendered, linguistic continues to exclude millions from state services. Aadhaar-based biometric authentication failures have denied welfare benefits to the poor and elderly. Without universal digital literacy and infrastructure, constitutional guarantees of equality risk becoming theoretical.

Criticisms of India's Digital Governance Approach

1. Technocratic Centralisation

Scholars argue that India's digital-governance model privileges efficiency over rights. Programmes like Aadhaar and UPI centralise citizen data within state-controlled databases, creating a "techno-bureaucratic Leviathan." This centralisation contradicts the constitutional principle of limited government, replacing participatory governance with algorithmic decision- making.

2. Executive Rule-Making by Notification

Many digital regulations such as the IT Rules 2021 and CERT-In Directions 2022 were issued through executive notifications without parliamentary debate.

This undermines the doctrine of separation of powers and bypasses democratic deliberation.[27] Courts have noted that digital governance, if unchecked, may evolve into "rule by executive fiat."

3. Lack of Judicial Capacity and Digital Expertise

Although Indian courts have recognised digital rights, judicial capacity to interpret complex technological issues remains limited. Judges depend on executive agencies or amici for technical insight, risking asymmetry in adjudication.

Without technological literacy, the judiciary's ability to ensure constitutional compliance in digital governance is constrained.

4. Private-Sector Dominance and Data Colonialism

[27] Puttaswamy (II) (2018) 1 SCC 809 — https://indiankanoon.org/doc/127517806/

The rapid expansion of foreign technology firms in India -Meta, Google, Amazon has created concerns about data sovereignty and monopolistic control. These entities harvest vast datasets from Indian users, often processed abroad.

Critics describe this phenomenon as "data colonialism," where developing nations supply raw data to global corporations without equitable governance rights. India's constitutional model, focused primarily on the state, has yet to evolve tools to regulate such transnational private power.

5. Inadequate Transparency and Public Consultation

Transparency is integral to democratic legitimacy. Yet, public consultations on major digital policies are brief and often limited to English-language documents.

Grassroots groups argue that the policy process excludes citizens most affected by digitalisation— the rural poor, women, and linguistic minorities.[28]

Case Studies in Digital Governance and Constitutional Scrutiny

1. ***Case Study 1*** **— Aadhaar and the Right to Privacy**

The Aadhaar programme, initiated in 2009, assigns a 12-digit biometric identity to residents, linking fingerprints and iris scans to welfare schemes.

While it has streamlined service delivery, Aadhaar's constitutional legitimacy has been hotly contested.

Constitutional Issues

- Privacy: Critics argued that Aadhaar enabled mass surveillance by aggregating sensitive personal data.
- Exclusion: Authentication failures led to denial of food-ration and pension entitlements.
- Proportionality: Mandatory Aadhaar linkage for multiple services was alleged to violate minimal-intrusion standards.

[28] Justice Chandrachud, dissent in Puttaswamy (II) — ibid.

In Justice K.S. Puttaswamy (II) v. Union of India (2018), the Supreme Court upheld Aadhaar's constitutional validity but restricted its use to government subsidies and taxation.[29]

The Court emphasised data-minimisation, limited purpose, and informed consent.

However, dissenting judges warned that Aadhaar's architecture enables "surveillance by design."[30]

Despite judicial safeguards, Aadhaar has expanded into private sectors banking, telecom, and fintech raising continuing privacy concerns.

Civil-society groups argue that technical fixes cannot substitute for strong legal guarantees.

2. *Case Study 2* — Pegasus Surveillance and National Security

In 2021, an international consortium of journalists revealed that Pegasus spyware, developed by NSO Group, had been deployed against Indian journalists, activists, and opposition leaders.[31]

Constitutional Questions

- Does the government's use of surveillance technology without statutory authorisation violate the right to privacy under Article 21?
- What procedural safeguards are required before intercepting digital communications?

The Supreme Court, recognising the "seriousness of allegations," constituted an independent expert committee led by Justice R.V. Raveendran.

The Court reaffirmed that national security cannot be a talismanic justification for secrecy, and state actions must pass constitutional scrutiny.

[29] Amnesty International, "Pegasus Project Findings," 2021 — https://www.amnesty.org/en/latest/news/
[30] The Quint, "IT Rules 2021: Platforms as State Gatekeepers," 2022 — https://www.thequint.com/
[31] Atlantic Council, "India's Data Protection Act Explained," Aug 2023 — https://www.atlanticcouncil.org/blogs/southasiasource/indias-data-protection-act/

Although the final report was not fully disclosed, the proceeding established a precedent: the executive cannot claim blanket immunity in digital-surveillance matters.

3. *Case Study 3* — IT Rules 2021 and Online Free Expression

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 mandate traceability, content takedown within 36 hours, and government-approved grievance officers for platforms.

Criticism

- Traceability undermines end-to-end encryption, affecting privacy.
- Content takedown provisions chill free speech and empower arbitrary censorship.
- The "Code of Ethics" for digital news allows state control over journalistic content.[18]

Multiple High Courts (Bombay, Madras, Kerala) have stayed enforcement of parts of these Rules, noting potential violations of Articles 19 and 21.

Scholars term the Rules an attempt to convert intermediaries into "digital gatekeepers for the state."[32]

4. *Case Study 4* — The Digital Personal Data Protection Act 2023

The DPDP Act 2023 establishes a consent-based data-processing framework and introduces rights such as correction and erasure of personal data.

However, the Act's Section 17 permits the Central Government to exempt agencies from compliance for reasons of sovereignty or public order.[33]

Constitutional Analysis

While the Act aligns superficially with global data-protection principles, it fails the

[32] Economic Times, "Experts Question DPDP Board's Independence," 2023 — https://economictimes.indiatimes.com/

[33] UNESCO, "Brazil's Marco Civil da Internet," 2020 — https://en.unesco.org/news/marco-civil-da-internet

proportionality test.

No requirement exists for judicial pre-authorisation before data access, and the oversight Board lacks independence.

Legal scholars warn that this architecture replicates the "surveillance state" under a rights-based façade.[34]

Broader Themes and Theoretical Insights

1. From Rule of Law to Rule of Code

Digital governance increasingly substitutes algorithmic procedures for traditional rule-of-law processes. Decisions once made by accountable officials are now embedded in code, which is opaque and unreviewable.

Legal theorists argue that this shift from rule of law to rule of code undermines constitutional transparency and contestability.

2. Constitutionalism Beyond the State

Digital power transcends national borders and state control.

Therefore, constitutionalism must expand to include non-state actors corporations, platforms, and algorithms. This emerging notion of polycentric constitutionalism treats private entities as duty- bearers of digital rights.

3. The Participatory Deficit

Indian digital policy has largely followed a top-down approach.

Unlike Brazil's Marco Civil, drafted through multi-stakeholder consultation, India's laws are often executive-driven.[35] A constitutional digital framework must institutionalise citizen participation, data trusts, and community-based governance models.

Synthesis of Findings

[34] Economic Times, "Experts Question DPDP Board's Independence," 2023 — https://economictimes.indiatimes.com/

[35] UNESCO, "Brazil's Marco Civil da Internet," 2020 — https://en.unesco.org/news/marco-civil-da-internet

The preceding analysis demonstrates that India's digital transformation represents both a constitutional opportunity and a challenge. The Indian state has leveraged technology to expand welfare delivery, promote inclusion, and modernise governance through initiatives such as Digital India, Aadhaar, and UPI. These efforts have enhanced efficiency and transparency in public administration, positioning India as a global leader in digital innovation.

Yet, constitutionalism demands that technological advancement remain subordinate to the rule of law and the protection of fundamental rights. India's legal and institutional responses to digitalisation—particularly under the Information Technology Act (2000), IT Rules (2021), and DPDP Act (2023)—reflect a fragmented approach that prioritises administrative control over constitutional safeguards.

The emergence of digital constitutionalism offers a framework for reconciling this imbalance. It insists that constitutional values—liberty, equality, accountability, and due process—must structure the digital order just as they structure the analogue one. This principle requires embedding rights-based norms in the design, deployment, and governance of technology.

The Future of Digital Constitutionalism in India

1. Embedding Rights in Code

To ensure technological systems respect constitutional values, rights must be encoded into design. This includes implementing privacy by-design, non-discrimination by-design, and transparency by-design standards.

2. Building an Independent Digital Rights Commission

India should establish an independent constitutional body- a Digital Rights Commission with investigative and adjudicatory powers over digital rights violations. It would function akin to the Election Commission or the National Human Rights Commission, ensuring autonomy from executive influence.

3. Judicial Reform and Digital Expertise

Courts require digital capacity-building to interpret complex technological cases. Regular

training programmes and the appointment of technical amici curiae can enhance judicial oversight. Additionally, specialised benches on digital rights could ensure consistency in jurisprudence.

4. Constitutionalising Algorithmic Governance

Algorithmic decision-making must adhere to constitutional principles of non-arbitrariness and equality. India should adopt a Digital Fairness and Accountability Code, mandating audits of government algorithms for bias and transparency. Such statutory audits would align governance technologies with Articles 14 and 21.

5. Strengthening Parliamentary Oversight

Parliament must reclaim its central role in digital governance. Major policies like the IT Rules and DPDP exemptions should undergo pre-legislative scrutiny and public consultation. Legislative committees can ensure accountability and limit executive dominance.

6. Public Participation and Digital Literacy

Digital constitutionalism thrives only when citizens can meaningfully engage in governance. Public participation should extend beyond token consultations to deliberative models, where citizens co-design data policies through open forums and citizen assemblies. Simultaneously, enhancing digital literacy across rural and marginalised communities is essential to bridge the participation gap.

7. Towards a Global Constitutional Dialogue

Digital constitutionalism is not an insular phenomenon. As cross-border data flows and global platforms reshape governance, India must actively engage in international forums such as the UN Internet Governance Forum and G20 Digital Economy Working Group to promote a Global South perspective on digital rights and justice.

Conclusion

India's rapid digital transformation has fundamentally reshaped the nature of governance and citizenship. Initiatives such as Digital India, Aadhaar, and UPI have enhanced efficiency and accessibility in public administration, positioning India as a global leader in

digital governance. However, this progress also brings new constitutional challenges concerning privacy, data protection, accountability, and individual freedom.

This study has demonstrated that digital constitutionalism offers a coherent framework to balance technological innovation with the protection of constitutional rights. It calls for embedding constitutional principles — liberty, equality, dignity, and due process — into the design and operation of digital systems. The goal is not to restrict technology but to ensure that it serves democratic governance rather than undermines it.

While India has taken significant steps toward regulating the digital space, gaps remain. The Digital Personal Data Protection Act, 2023, though a milestone, provides broad state exemptions and limited safeguards for citizens' data. Similarly, the increasing use of surveillance tools and opaque algorithmic systems raises concerns about state overreach and digital inequality. Judicial interventions such as Puttaswamy and Shreya Singhal have been vital in upholding digital rights, yet a consistent and proactive judicial approach is still needed to secure privacy, free speech, and autonomy in cyberspace.

Legislative and institutional reforms must therefore strengthen accountability and transparency in digital governance. Parliament should ensure rights-based lawmaking through open consultations and rigorous oversight, while an independent Digital Rights Commission could provide a specialised forum for addressing violations. Moreover, digital policymaking should respect federal principles, allowing states greater participation in shaping data and governance frameworks.

Equally essential is public empowerment. Citizens must be informed about their digital rights and capable of engaging meaningfully with technology. Building digital literacy and awareness can transform individuals from passive data subjects into active participants in democratic digital governance.

On the international stage, India must advocate for a Global South perspective that balances technological development with equity and human rights. By promoting a model of ethical and inclusive digital governance, India can contribute to shaping global standards for digital constitutionalism.

In essence, the challenge before India is to ensure that the digital state remains bound by the same constitutional morality that governs the physical state. A truly constitutional digital

order will emerge only when technological systems, algorithms, and data frameworks operate under the discipline of constitutional rights and democratic oversight.

Digital constitutionalism thus represents not the rejection of technology but the reaffirmation of human dignity in a technological age. India's digital future must rest on the conviction that progress is meaningful only when it preserves freedom — the very foundation of the Constitution itself.

Bibliography

1. Celeste, E., Digital Constitutionalism: A New Systematic Theorisation, Oxford University Press, 2022. Retrieved from https://academic.oup.com/ijlit/article/30/1/68/6550367
2. Gill, L., "Digital Power and Constitutional Pluralism," Internet Policy Review, 2021. https://policyreview.info/articles/analysis/digital-constitutionalism
3. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1. https://en.wikipedia.org/wiki/Puttaswamy_v._Union_of_India
4. Milan, S. & Treré, E., "The Rise of Digital Constitutionalism," Internet Policy Review, 2019. https://policyreview.info/articles/news/rise-digital-constitutionalism
5. Faheema Shirin v. State of Kerala, 2019 (4) KLT 494. https://indiankanoon.org/doc/152132631/
6. Tisne, M., "Data and the New Social Contract," Carnegie Endowment for International Peace, 2020. https://carnegieendowment.org/2020/10/22/data-and- new-social-contract-pub-82931
7. OECD, "OECD Principles on Artificial Intelligence," 2019. https://oecd.ai/en/ai-principles
8. Press Information Bureau, Government of India, "Digital India: Progress Report 2024." https://pib.gov.in/PressReleasePage.aspx?PRID=1952045

9. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 — https://en.wikipedia.org/wiki/Puttaswamy_v._Union_of_India
10. Internet Freedom Foundation, "Analysis of Section 69A Orders," 2022 — https://internetfreedom.in/
11. Shreya Singhal v. Union of India, (2015) 5 SCC 1 — https://indiankanoon.org/doc/110813550/
12. Human Rights Watch, "India: New Rules Threaten Internet Freedom," Feb 2021 — https://www.hrw.org/news/2021/02/27/india-new-rules-threaten-internet-freedom
13. Atlantic Council, "India's Data Protection Act Explained," Aug 2023 — https://www.atlanticcouncil.org/blogs/southasiasource/indias-data-protection-act/
14. Mehta, P., "India's Digital Public Infrastructure," Brookings Institution, 2023 — https://www.brookings.edu/articles/india-digital-public-infrastructure/
15. CERT-In, "About the Indian Computer Emergency Response Team," 2024 — https://www.cert-in.org.in/
16. Puttaswamy (II) — Aadhaar Judgment (2018) 1 SCC 809 — https://indiankanoon.org/doc/127517806/
17. Faheema Shirin v. State of Kerala, 2019 (4) KLT 494 — https://indiankanoon.org/doc/152132631/
18. Raghavan, S., "Algorithmic Bias and the Indian Constitution," Vidhi Centre for Legal Policy, 2021 — https://vidhilegalpolicy.in/blog/algorithmic-bias-and-equality/
19. The Wire, "Supreme Court Appoints Pegasus Probe Panel," 2021 —

https://thewire.in/law/supreme-court-pegasus-probe

20. Internet Society, “Traceability and Encryption in India,” 2022 — https://www.internetsociety.org/resources/doc/traceability/
21. European Commission, “General Data Protection Regulation,” 2018 — https://gdpr-info.eu/
22. Electronic Frontier Foundation, “Section 230 and Online Speech,” 2023 — https://www.eff.org/issues/cda230
23. UNESCO, “Brazil’s Marco Civil da Internet,” 2020 — https://en.unesco.org/news/marco-civil-da-internet
24. Internet Freedom Foundation, “DPDP Act 2023: An Analysis,” 2023 — https://internetfreedom.in/
25. Access Now, “India’s Privacy Under Threat,” 2023 — https://www.accessnow.org/
26. Centre for Communication Governance, “Surveillance Laws in India,” 2022 — https://ccgdelhi.org/
27. The Wire, “Supreme Court Appoints Pegasus Probe Panel,” 2021 — https://thewire.in/law/supreme-court-pegasus-probe
28. EPW, “Technocratic Centralisation and Digital Governance,” 2022 — https://www.epw.in/
29. PRS India, “Analysis of IT Rules 2021,” 2021 — https://prsindia.org/
30. Puttaswamy (II) (2018) 1 SCC 809 — https://indiankanoon.org/doc/127517806/
31. Justice Chandrachud, dissent in Puttaswamy (II) — ibid.
32. Internet Freedom Foundation, “Aadhaar and Privacy After Five Years,” 2023 —

https://internetfreedom.in/

33. The Quint, “IT Rules 2021: Platforms as State Gatekeepers,” 2022 — https://www.thequint.com/
34. Atlantic Council, “India’s Data Protection Act Explained,” Aug 2023 — https://www.atlanticcouncil.org/blogs/southasiasource/indias-data-protection-act/
35. UNESCO, “Brazil’s Marco Civil da Internet,” 2020 — https://en.unesco.org/news/marco-civil-da-internet