

---

# CONSTITUTIONAL ADAPTATION IN THE AGE OF DIGITAL TRANSFORMATION: ADDRESSING AI, PRIVACY, AND CYBER ETHICS IN INDIA

---

N Amuthalakshmi, VELS Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai

R. Nalini, VELS Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai

## ABSTRACT

The rapid pace of digital transformation, driven by advancements in Artificial Intelligence (AI), pervasive data collection, and ubiquitous digital connectivity, poses unprecedented challenges to constitutional governance in India. The Indian Constitution, while drafted in a pre-digital era, remains a dynamic and adaptable framework. However, its interpretative mechanisms are now being tested against complex questions involving privacy, surveillance, algorithmic governance, data rights, and cyber ethics. This abstract explores how constitutional principles can be recalibrated and reinterpreted to address the normative tensions emerging from India's digital revolution. Central to this discourse is the right to privacy, which was elevated to the status of a fundamental right in *Justice K.S. Puttaswamy v. Union of India* (2017). This landmark judgment has since become the bedrock for assessing state and private encroachments into personal data and digital identity. Nonetheless, the increasing deployment of AI systems in public decision-making such as facial recognition, predictive policing, and biometric authentication raises pressing concerns about opacity, accountability, and potential biases. These developments demand a robust constitutional response that harmonizes innovation with individual rights and democratic values. Furthermore, the emergence of digital platforms and algorithmic governance challenges the traditional public-private divide in constitutional jurisprudence. As private entities wield quasi-sovereign powers in moderating speech, shaping public discourse, and collecting vast amounts of user data, there is a compelling case for expanding constitutional accountability beyond the state. The ethical dimensions of AI, including fairness, transparency, and non-discrimination, must also be situated within a constitutional framework that prioritizes dignity, equality, and justice. Moreover, the inadequacy of existing statutory instruments like the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, underscore the need for a more principled, constitutionally anchored regulatory architecture.

## **Introduction**

The digital revolution has ushered in an era marked by profound technological shifts, redefining societal structures, economic paradigms, and governance frameworks. Globally India, is the second-largest internet user base, stands at the forefront of this transformation. Artificial Intelligence (AI), big data analytics, the Internet of Things (IoT), and ubiquitous connectivity are rapidly reshaping the interface between the state and its citizens. The phrase "digital age" encompasses a variety of technological advancements, such as virtual spaces, digital services, smart applications, machine learning, and systems based on knowledge, which shape the characteristics of today's world, including virtualization, electronic communication, globalization, and the sharing of information. While these advances ensure efficiency and innovation, they simultaneously pose complex ethical, legal, and constitutional dilemmas that are particularly concerning privacy, surveillance, accountability, and individual rights. Indian Constitution, is a dynamic and living document, was crafted in an era devoid of digital realities. Yet, its adaptability has been a cornerstone of its endurance. As digital technologies challenge established notions of autonomy, liberty, and governance, the need to recalibrate constitutional frameworks has become increasingly urgent. This article critically examines how India's constitutional machinery can evolve to address the challenges posed by AI, digital privacy, and cyber ethics, ensuring the preservation of fundamental rights in a digitally transformed society. Nevertheless, there is a risk that technologies from the digital age may infringe upon crucial security and privacy principles due to uncontrolled access to information and personal data housed in numerous global network nodes. This article intends to highlight specific aspects of protecting information and personal data while providing an overview of the main threats to user security and privacy in the digital era. Furthermore, this article addresses the Digital Age, which signifies a transition towards the electronic handling of information, transforming the global economy and facilitating the exchange of goods, services, and knowledge among individuals. The Internet has drastically changed communication, shopping, and education, enabling individuals to learn from the comfort of their homes. In India, the Information Technology Act 2000 was enacted to tackle cybercrimes, which include offenses related to computers and obscene content. The constitutional challenges posed by the Digital Age in India involve the right to privacy, the digital divide and the right to equality, freedom of speech and expression, judicial oversight and law enforcement, intellectual property rights, as well as concerns regarding data security and privacy in a connected environment. Addressing these challenges necessitates consideration of matters such as jurisdiction, the admissibility of digital

evidence, and the protection of intellectual property rights. The legal system must strike a balance between promoting innovation and protecting individuals' privacy in the digital landscape. The legal framework in India encounters difficulties in managing cross-border cyber crimes due to the interconnected nature of the internet. To tackle these challenges, there is a need for harmonized legal frameworks, data-sharing agreements, and standardized protocols. The government has initiated efforts to enhance internet accessibility, and the Digital Data Protection Act 2023 aims to create flexible regulations.

### **India's Digital Evolution and Legal Inertia:**

Over the past decade, India has embarked on an ambitious journey of digital transformation, driven by initiatives such as Digital India, Aadhaar, and the expansion of fintech and e-governance platforms. As services from banking to welfare delivery migrated online, the digital space has effectively become a new public sphere. However, the legal and constitutional framework has struggled to keep pace. The Constitution of India, adopted in 1950, lays down a comprehensive list of Fundamental Rights and Directive Principles. However, digital-era concerns like algorithmic discrimination, AI-based surveillance, data commodification, and digital exclusion were beyond the imagination of the framers. While courts and legislatures have attempted to address these gaps through interpretation and legislation, the pace and nature of technological advancement necessitate a more structured constitutional response.

### **Constitutional Challenges Arising from AI and Digital Technologies**

#### **1. Right to Privacy in the Age of Surveillance and Datafication**

The landmark judgment in *Justice K.S. Puttaswamy v. Union of India* (2017)<sup>1</sup> affirmed the right to privacy as a fundamental right under Article 21. However, this ruling came at a time when the Aadhaar system and numerous surveillance infrastructures were already operational. AI and big data technologies now enable the state and private entities to engage in predictive profiling, behavioral tracking, and automated decision-making—often without meaningful consent or oversight. Finally, in *K.S. Puttaswamy (Privacy-9J.) v. Union of India*, (2017) 10 SCC 1, the 9 Judge Bench of Supreme Court of India, in a historic verdict declared unanimously that, Right to Privacy is protected as an intrinsic part of the right to life and personal liberty

---

<sup>1</sup> AIR 2017 SC 4161

under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution.<sup>2</sup>The challenge lies in translating this abstract right into tangible protections. While the Digital Personal Data Protection Act, 2023,<sup>3</sup> is a step forward, critics argue that it prioritizes state interests over individual autonomy. Moreover, it provides expansive exemptions to government agencies, weakening the Puttaswamy safeguards. Thus, there is a pressing need to embed robust data protection principles such as purpose limitation, data minimization, and algorithmic transparency within the constitutional framework itself, ensuring that privacy remains inviolable even in a data-driven governance regime. The critical challenge faced by legal system worldwide are balancing individual privacy rights with the needs of law enforcement and national security.

**Right to Privacy:** Privacy rights face significant threats from the extensive collection, storage, and processing of personal data by both government bodies and private organizations. Surveillance technologies and data breaches further endanger an individual's control over their personal information and compromise data security.

**Right to Information:** The right to information, derived from Article 19(1)(a) of the Constitution, is essential for promoting government transparency and accountability.

**Data Protection and Access Control:** With the increasing digitalization of government records and services, robust data protection and access control mechanisms are essential. These safeguards ensure that citizens can exercise their right to information without compromising national security or personal privacy. However, cybersecurity threats can disrupt access to critical data and e-governance services.

### Digital Divide and Right to Equality

Article 14 of the Indian Constitution guarantees equality before the law and equal protection of the law. Yet, a significant digital divide persists between urban and rural areas and among different socioeconomic groups. This gap makes it challenging to ensure equal access to digital opportunities and services. Bridging this divide is crucial to eliminate discrimination and promote inclusive development.

---

<sup>2</sup> <https://www.scconline.com/blog/post/2024/10/28/justice-ks-puttaswamy-champion-right-to-privacy-obituary-legal-news/>

<sup>3</sup> Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023

## Freedom of Speech and Expression

Article 19(1)(a) of the Constitution guarantees the right to freedom of speech and expression. However, this right can be undermined by internet shutdowns, censorship, and strict online content regulations. Additionally, the misuse of social media to spread hate speech, misinformation, and defamatory content complicates efforts to balance free speech with the need to maintain public order and national security.<sup>4</sup>

## 2. Algorithmic Governance and Equality

AI systems are increasingly used in areas such as policing, credit scoring, hiring, and social welfare allocation. However, the opacity of these algorithms often obscures their potential to entrench biases and perpetuate inequality. For example, predictive policing tools can reinforce existing patterns of social discrimination, particularly against marginalized communities such as Dalits, Adivasis, or Muslims. Article 14 guarantees equality before the law and equal protection of laws.<sup>5</sup> Yet, the deployment of algorithmic tools in public decision-making challenges this guarantee when outcomes are opaque, unexplainable, or systematically biased. There is a growing need for “algorithmic accountability” grounded in constitutional principles. This would entail mechanisms to ensure transparency in AI decision-making, avenues for human review, and a right to explanation, particularly where algorithmic determinations affect fundamental rights.

## 3. Freedom of Expression and Platform Governance

Social media platforms, powered by AI-driven recommendation engines, have become dominant spaces for public discourse. However, these platforms are also arenas of content moderation, censorship, and misinformation. The state has sought to regulate them through rules such as the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.<sup>6</sup> While these rules aim to curb online harms, they also raise significant concerns about overreach and the chilling effect on free speech. Article 19(1)(a) guarantees the freedom of speech and expression, subject to reasonable restrictions under Article 19(2).<sup>7</sup> Yet,

---

<sup>4</sup> Digital Age and Constitutional Challenges in India: Adapting to New Technologies-Aug 26, 2024 Information Technology/Cyber Law-Harsh Raj

<sup>5</sup>The Constitution of India, art. 14.

<sup>6</sup> Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, Feb. 25, 2021.

<sup>7</sup> The Constitution of India, art. 19(1)(a), art. 19(2).

the interplay between private platform governance and state regulation creates a grey zone where neither constitutional protections nor corporate policies offer adequate safeguards. A constitutional response would require both regulating private tech power and ensuring that state controls do not undermine democratic discourse.

#### **4. Digital Exclusion and the Right to Access**

India's push for digital governance assumes universal digital access. However, millions still lack reliable internet connectivity, digital literacy, or access to smart devices. This creates a paradox where essential services such as welfare benefits or vaccine registration are increasingly contingent on digital access, thereby excluding the very populations they are intended to serve. This undermines the constitutional promise of equality and dignity. The right to digital access must, therefore, be constitutionally recognized as a derivative of the right to life and equality. Further, digital literacy should be included within the scope of the right to education under Article 21A,<sup>8</sup> ensuring that digital inclusion becomes a constitutional imperative rather than a policy aspiration.

### **Cyber Ethics and Constitutional Morality**

#### **1. Reimagining Cyber Ethics Through Constitutional Values**

Cyber ethics refers to the moral principles governing conduct in digital environments. In India's context, where digital technologies interact deeply with social, political, and economic life, ethical frameworks must be rooted in constitutional morality of justice, liberty, equality, and fraternity. Ethical digital practices are not just about complying with regulations but about aligning technological actions with constitutional ideals.

For instance, AI systems used in welfare delivery must be evaluated not just on efficiency metrics but on whether they uphold the dignity of the beneficiaries. Similarly, online anonymity, while valuable for whistleblowers and activists, must be balanced against accountability in cases of defamation or cyberbullying. The Constitution, therefore, must act as a normative compass guiding ethical behavior in digital spaces, and these principles should be embedded into technology design and policy-making.

---

<sup>8</sup> The Constitution of India, art. 21A.

## 2. Digital Harms and the Gendered Dimensions of Cyber Ethics

Cyber harassment, non-consensual circulation of intimate images, deepfakes, and online stalking disproportionately affect women and marginalized gender identities. These harms are not adequately addressed by existing laws such as the Information Technology Act, 2000, or sections of the Indian Penal Code. The Constitution's guarantee of personal liberty under Article 21 must be expanded to explicitly address digital bodily autonomy and online dignity. Courts must interpret Article 15 (prohibition of discrimination) and Article 21 in tandem to recognize the right to a safe and equitable digital environment, especially for vulnerable populations. The state must adopt a gender-sensitive approach to digital policymaking and ensure effective redressal mechanisms and preventive tools such as content takedown protocols, privacy-by-design platforms, and algorithmic safety audits.<sup>9</sup>

### State Responsibility and the Limits of Digital Governance

#### 1. The Role of the State in Safeguarding Digital Rights

The Indian state plays a dual role in the digital space as a facilitator of digital services and as a regulator. While initiatives like Aadhaar and digital public infrastructure aim to improve governance, they also raise concerns about surveillance, data misuse, and exclusion. The Supreme Court's Aadhaar judgment (*Justice K.S. Puttaswamy (Aadhaar-5J)*, 2018)<sup>10</sup> declared the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 to be valid and not violative of the fundamental right to privacy and upheld the constitutionality of the scheme but imposed limitations on its use by private players. However, subsequent legislative and executive actions have often diluted these safeguards. Constitutional adaptation must involve judicial reinforcement of digital rights through regular review of executive actions, sunset clauses on surveillance frameworks, and the establishment of independent oversight bodies. Parliament too must play a more proactive role in enacting rights-based digital laws rather than technocratic regulations.

#### 2. Decentralization and Digital Federalism

Digital governance in India has largely followed a centralized model, with the Union government managing core digital infrastructure and policy making. However, this undermines

---

<sup>9</sup> The Constitution of India, art. 15, art. 21

<sup>10</sup> *Justice K.S. Puttaswamy (Aadhaar-5J) v. Union of India*, (2018) 1 SCC 809.

the spirit of cooperative federalism. For instance, data localization policies and internet shutdowns are executed centrally, often sidelining the interests of states and local communities. Constitutional reform in the digital context must include provisions for digital federalism empowering states to frame context-specific digital rights charters, ensure local digital infrastructure development, and participate in data governance debates. This will align with the principles of decentralization under the Seventh Schedule and foster more inclusive governance.<sup>11</sup>

## **Comparative Insights: Learning from Global Constitutional Practices**

### **1. European Union: The Charter of Fundamental Rights and GDPR**

The European Union's Charter of Fundamental Rights recognizes data protection as a distinct right (Article 8),<sup>12</sup> separate from the right to privacy. The General Data Protection Regulation (GDPR) operationalizes this right through robust consent frameworks, the right to be forgotten, and strict accountability mechanisms for data controllers.<sup>13</sup> Indian constitutional evolution can draw from this by enshrining a separate constitutional right to data protection. Currently, privacy is protected under Article 21, but data protection needs to be recognized not just as a subset but as a standalone right with clear, enforceable principles.

### **2. United States: First Amendment and Algorithmic Transparency**

In the U.S., debates around free speech on digital platforms have led to calls for transparency in content moderation algorithms. While the First Amendment restricts government regulation of speech, the growing power of tech companies has spurred discussions about platform accountability and algorithmic bias.<sup>14</sup>

India can take cues by balancing the right to free expression with the need to regulate opaque algorithms used in public and private discourse. Judicial interpretations must recognize algorithmic governance as a potential violator of free speech and require due process in moderation decisions.

### **3. Estonia and South Korea: Digital Sovereignty and AI Ethics**

---

<sup>11</sup> The Constitution of India, Schedule VII.

<sup>12</sup> Charter of Fundamental Rights of the European Union, art. 8, 2012 O.J. (C 326) 391.

<sup>13</sup> General Data Protection Regulation, (EU) 2016/679, 2016 O.J. (L 119) 1.

<sup>14</sup> U.S. Const. amend. I.



Estonia has institutionalized digital citizenship and e-governance with strong legal safeguards, while South Korea has developed comprehensive AI ethics charters. These countries emphasize trust, transparency, and public participation in tech policymaking.

India's constitutional future in the digital age must similarly institutionalize ethical and participatory frameworks through parliamentary tech ethics committees, public consultations, and constitutionally grounded AI ethics principles.

### **Recommendations for Constitutional and Legal Reform**

To meaningfully address the constitutional implications of AI, privacy, and cyber ethics in India, a multi-pronged reform strategy is required. The following policy and legal recommendations are rooted in constitutional values and global best practices.

#### **1. Enshrine a Right to Data Protection and Algorithmic Fairness**

India must constitutionally recognize a standalone right to data protection, distinct from the broader right to privacy under Article 21. This right should encompass: Informed consent requirements for data collection, Algorithmic transparency standards in automated decision-making systems, The right to explanation for decisions made by AI, The right to be forgotten, particularly in the context of digital footprints and profiling. These elements should be integrated into the Constitution through a formal amendment or a comprehensive judicial reinterpretation of existing provisions.

#### **2. Establish a Constitutional Body for Digital Rights Oversight**

To institutionalize accountability, the creation of a Digital Rights Commission of India (DRCI) is recommended. This quasi-judicial, independent constitutional body would have powers to: Investigate violations of digital rights by state and non-state actors, Audit government AI and surveillance systems, Ensure enforcement of ethical AI standards and privacy obligations, Act as an ombudsman for digital grievances.

#### **3. Draft a Digital Bill of Rights**

India should introduce a Digital Bill of Rights is a statutory codification of citizens' rights and responsibilities in the digital domain. This document would reinforce constitutional protections with specific guarantees related to: Access to the internet as a basic right, Protection from

algorithmic discrimination, Freedom from targeted misinformation and deepfake abuse, Digital literacy as a constitutional duty of the state. Such a bill would serve as a touchstone for future legislation and court interpretations concerning technology and rights.

#### **4. Constitutionalizing Digital Inclusion**

The government must move toward constitutionalizing the right to digital access and literacy. This can be achieved by: Expanding Article 21A (Right to Education) to include digital literacy as a core component, Mandating universal and equitable internet access under Article 39 (Directive Principles of State Policy), Enforcing net neutrality and curbing arbitrary internet shutdowns to protect freedom of speech under Article 19(1)(a). These initiatives would ensure that no citizen is left behind in the digital era, bridging the digital divide that currently threatens democratic equality.

#### **5. Legislate Ethical Frameworks for AI and Emerging Tech**

India must draft and adopt a comprehensive AI ethics law, rooted in constitutional morality. The law should mandate: Ethical audits of AI systems, Impact assessments for high-risk AI applications, Ethical design principles that prioritize human dignity, non-discrimination, and consent, Public transparency obligations for tech firms and state agencies. These measures must be judicially enforceable and harmonized with international standards like the UNESCO Recommendation on AI Ethics<sup>15</sup> and the OECD AI Principles.<sup>16</sup>

#### **The Way Forward: A Digitally Resilient Constitution**

India's constitutional journey in the digital age must be informed by both its foundational values and the new realities of a hyperconnected world. As AI and data technologies shape the future of work, education, governance, and personal identity, the Constitution must evolve—not through radical overhaul, but through principled, incremental adaptation.

Courts must act as vigilant sentinels of digital liberty, interpreting the Constitution in ways that reflect technological nuances. The legislature must avoid reactionary policymaking and instead engage in rights-centered, forward-thinking digital legislation. Civil society and academia must

---

<sup>15</sup> UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).

<sup>16</sup> OECD, Principles on Artificial Intelligence (2019).

hold digital powers accountable, ensuring that constitutional ideals are not subordinated to market or security imperatives.

Constitutional adaptation is not merely about updating laws—it is about renewing the social contract in a new era. The digital transformation of India should not come at the cost of constitutional erosion. Rather, it offers an opportunity to reaffirm the republic's commitment to justice, liberty, equality, and fraternity in every byte, bot, and blockchain.

## **Conclusion**

In conclusion, India stands at a constitutional crossroads where it must decisively adapt its foundational principles to the digital age. Through a purposive and context-sensitive interpretation of rights, institutional reforms, and the integration of cyber ethics into legal discourse, the Indian constitutional order can evolve to safeguard democratic values while embracing technological change. This transformation requires a collaborative engagement between the judiciary, legislature, civil society, and technologists to ensure that constitutionalism in India remains resilient and responsive in the age of AI and digital disruption. India stands at a defining juncture. The digital age has brought immense promise but also unprecedented challenges to the constitutional order. Artificial Intelligence, mass data collection, and cyber technologies are not just technical issues, they are fundamentally constitutional ones. They touch upon who we are, how we relate to the state, and what it means to be free and equal in a digital society. To preserve the soul of the Constitution, its letter must evolve. Through judicial innovation, legislative foresight, and participatory policymaking, India can build a constitutional framework that safeguards digital rights while harnessing the full potential of technology. In this balance between innovation and ethics, lies the future of Indian democracy.