
DIGITAL CONSTITUTIONALISM IN INDIA: CONSTITUTIONAL ACCOUNTABILITY IN THE AGE OF ALGORITHMIC GOVERNANCE

Pavithra R, LL.M. (International Law and Organisation), University of Madras

ABSTRACT

The rapid expansion of digital technologies, artificial intelligence, and platform-based governance has fundamentally transformed the relationship between the State, private corporations, and citizens in India. Public administration, law enforcement, welfare distribution, electoral communication, content moderation, financial access, and digital identity verification are all becoming more and more impacted by algorithmic systems. These technologies present significant constitutional problems about privacy, equality, free speech, due process, accountability, and democratic government even as they offer efficiency, transparency, and innovation. Through the prism of constitutional responsibility in the era of algorithmic governance, this study investigates the rise of digital constitutionalism in India.

This paper examines how the Indian Constitution's guiding principles must change to control the use of digital power by the government, IT companies, and algorithmic systems. It critically assesses important court rulings, such as Justice K.S. Puttaswamy v. Union of India, Anuradha Bhasin v. Union of India and Tomosu Bruno v. State of UP and also E.P.Royappa v State of TN, as well as data protection. The study also looks into India's legal system, including the Information Technology Act of 2000, the Digital Personal Data Protection Act of 2023, and new discussions about the governance of artificial intelligence.

This research argues that traditional constitutional safeguards are insufficient in addressing opaque algorithmic decision-making and concentrated digital power. It promotes a revolutionary approach to digital constitutionalism based on democratic oversight, accountability, explainability, transparency, and proportionality. In order to maintain constitutional morality in the digital age, the study concludes that India must create a constitutional framework that can strike a balance between innovation and the protection of fundamental rights.

Keywords: Digital Constitutionalism, Algorithmic Governance, Artificial Intelligence, Fundamental Rights, Constitutional Accountability, Data Protection, Platform Governance, India.

Introduction:

The use of digital technologies has increased at a rate never witnessed before in the twenty-first century. Digital platforms are now essential to every aspect of modern life, from banking and governance to communication and education. But there are also serious legal and constitutional issues with this digital revolution. In the virtual world, rights that were formerly applicable to physical areas are now put to the test. The endeavour to protect constitutional principles-such as equality, privacy, and freedom of speech in the digital sphere is known as "digital constitutionalism." This essay aims to comprehend how these values are being developed and protected in the internet era, particularly in the Indian context.¹

The term "digital constitutionalism" refers to the application of constitutional values like liberty, equality, and dignity including non-arbitrariness, accountability, and the rule of law in the digital sphere. In a world where data gathering, artificial intelligence (AI), and surveillance technologies are dominant, these ideals are under assault. Whether it is through biometric databases, predictive algorithms, or both, modern governance is turning into an unseen system. Digital governance is now having an impact on daily life. Know Your Customer (KYC) verification, welfare distribution, employment applications, medical data, and even social media political expression are all mediated by automated systems. These technologies typically function without substantial disclosure or approval from people. As a result, private businesses, police enforcement organizations, and software designers hold a disproportionate amount of influence. This creates an unequal society in which citizens are not active right-holders as they should be in free democracies, but rather passive data subjects.

This type of covert, ongoing monitoring has the potential to stifle free expression, deter criticism, and upend democracies. The new norm is self-censorship. In India, the right to privacy is increasingly regarded as one of the fundamental rights. The Indian Supreme Court upheld this in *Justice K.S. Puttaswamy (Retd.) And Anr. vs. Union of India and Ors.* (2017). Parliament passed the Digital Personal Data Protection Act, 2023, more recently. Despite being intended to protect citizen data, the law contains a number of serious shortcomings. It provides the government with extensive exemptions, is poorly supervised by an independent authority,

¹ Vivek Kumar Rajbhar, *Digital Constitutionalism and Fundamental Rights: A Contemporary Legal Analysis*, Vintage Legal, <https://www.vintagelegalvl.com/post/digital-constitutionalism-and-fundamental-rights-a-contemporary-legal-analysis>

and offers insufficient individual remedies.²

Digital Constitutionalism:

The application of fundamental constitutional principles-liberty, equality, privacy, due process, proportionality, accountability, and the rule of law-to digital technology, online environments, and algorithmic systems is known as "digital constitutionalism". It aims to prevent fundamental rights and democratic standards from being compromised by technological innovation and digital governance.³

Digital Rights, Data Protection and Privacy, Internet Governance, Cybersecurity, Digital Economy, Access and Digital Divide, Content Regulation, Algorithmic Transparency and Accountability, International Cooperation, and Digital Sovereignty are some of the essential components of digital constitutionalism.⁴

Theoretical foundation of digital constitutionalism:

Digital constitutionalism is currently frequently viewed in academic literature as a particular example of societal constitutionalism, a more general theoretical framework that has been developed over the course of more than a decade. Specifically, authors use societal constitutionalism to theoretically define the formation of new normative forms in the regulatory spaces created by new technologies, including public, private, and hybrid normativity. Advocates of digital constitutionalism frequently cite various aspects of societal constitutionalism, particularly in regard to global legal diversity and dispute resolution, even when they do not explicitly adhere to such a species link.

However, these analogies frequently only describe "constitutional" norms and constitutionalization processes in the comparatively independent digital sector or spheres. In general, they tend to ignore the limiting role and instead concentrate on the constitutive/foundational role that social constitutionalism accords to such standards. This

² Faizan Mustafa and Aashank Dwivedi, *A Growing Shadow Over Digital Constitutionalism*, The Hindu, (Dec.6,2025), <https://www.thehindu.com/opinion/lead/a-growing-shadow-over-digital-constitutionalism/article70362964.ece>

³ Vandita Sharma, *Digital Constitutionalism: Protecting Fundamental Rights in the 21st Century*, *International Journal of Creative Research Thoughts*, Vol - 13, (Nov 11, 2025), <https://www.ijcrt.org/papers/IJCRT2511485.pdf>

⁴ Digital Constitutionalism, Kamaraj IAS Academy, (Dec 6,2025), <https://www.kamarajiasacademy.com/current-affairs/digital-constitutionalism>

usage gives the idea that, in general, societal constitutionalism simply serves to legitimize and justify new kinds of governmentality and unchecked power centers.⁵

A comprehensive understanding of the idea of digital constitutionalism is not provided by the body of current literature. Specifically, there is disagreement over two essential aspects of this concept. First, regarding the extent of digital constitutionalism, it is unclear if it seeks to restrict both private and public power. Second, there is no consensus over the tool that ought to put digital constitutionalism's principles into practice. It's interesting to note that we have painted a picture of the state's role gradually waning as society segments' influence grows at the same time. Fitzgerald assigns a constitutionalizing role to private law, Berman to constitutional law, Suzor to a private law based on constitutional principles, Karavas to norms created by private actors, and Redeker, Gill, and Gasser to the Internet bill of rights texts.

On the one hand, the literature now in publication does not raise any questions about the concepts of "constitution" and "constitutional law." Actually, according to Padovani and Santaniello (2018), every author under analysis refers to their customary interpretations that are appropriate for the state dimension. However, the concepts of "constitutionalism" and "constitutionalization" seem to be surrounded by a certain nebulosity, particularly since they are typically projected in a global dimension and disconnected from the traditional state framework.⁶

The term "digital constitutionalism" is a helpful acronym for the theoretical movement that supports applying constitutionalism's basic principles to the digital age. However, such a description could seem deceptive at first. The noun "constitutionalism" is not explicitly qualified by the adjective "digital." It is not comparable to terms like "liberal constitutionalism" or "democratic constitutionalism," which, respectively, describe a recently developed orientation of the philosophy of constitutionalism. The term "digital" is more of an adverb, suggesting that it refers to the branch of constitutional theory that aims to define values for the digital society. Similarly, "global" or "international" constitutionalism has been

⁵ Angalo Jr Golia, *Redefining Digital Constitutionalism As Critique and Ideology: The Perspective of Societal Constitutionalism*, Gigi Con, (Oct.17,2025) <https://digi-con.org/redefining-digital-constitutionalism-as-critique-and-ideology-the-perspective-of-societal-constitutionalism/>

⁶ Edoardo Celeste, *Digital Constitutionalism: A New Systematic Theorisation*, *International Review of Law & Computers & Technology*, Vol - 33, (Feb 27, 2021) https://www.researchgate.net/publication/330135709_Digital_constitutionalism_a_new_systematic_theorisation

discussed in academics.⁷

Algorithmic governance and constitutionalism:

Algorithms are more than just tools in this new environment; they are actively influencing public life and changing the basis of democratic governance. However, the growing reliance on these systems raises a number of significant issues, including: What does the term "algorithmic governance" really entail, and how broad is it? When the processes are concealed by opaque code, how may algorithmic governance impact constitutional rights? What part do the judicial and legislative branches play in finding solutions to these problems? What actions may be taken to enhance equity and justice in algorithmic systems?

In contemporary public administration and law enforcement, algorithms are becoming a crucial part of decision-making. Digital technologies are quickly replacing human authorities in a variety of tasks, from automated legal advice to predictive policing algorithms that identify crime hotspots. The transition from human judgment to data-driven decision-making signifies the emergence of "algocracy," in which algorithms assume expert-managed activities. Although these technologies are more objective and accurate, there is a risk that they will miss subtleties in governance processes by reducing complex human experiences to simple data values.⁸

It has been accurately noted that "every new option introduced by technological evolution affects the substance, eventually changing the way humans think and relate to each other." AI has "affected the information and communication technologies," which have the greatest potential to change society. An algorithmic civilization has progressively emerged as a result of all of this. Legal and particularly constitutional scholarship with a strong theoretical, conceptual orientation has remained relatively rare, despite the fact that the idea of the algorithmic society has undoubtedly drawn a lot of attention from social scientists in general, as we will see below. As Lee and Larsen have shown, social scientists have investigated a plethora of useful ways in which algorithms are entwined with our culture and society. However, rather than exploring deeper conceptual problems with the implicit normativity

⁷ Edoardo Celeste, *Constitutionalism in the Digital Age*, Liber Amicorum for Ingolf Dernice, (2020), <https://www.hiig.de/wp-content/uploads/2020/11/2020-Celeste-Constitutionalism-in-the-Digital-Age.pdf>

⁸ Jaivear Singh and Yagya Agarwal, *Invisible Hand of Cod: Reimagining Constitutionalism In The Age Of Algorithms*, NLR Blogs By NLIU Law Review, (Jan 27,2025) <https://nliulawreview.nliu.ac.in/blog/invisible-hand-of-code-reimagining-constitutionalism-in-the-age-of-algorithms/>

attributed to algorithms, these considerations have mostly remained at a practical, sociological level. Thus, conceptual, meta-theoretical study on the origins, causes, and effects of the algorithmic society is noticeably lacking in the social sciences as a whole, and it is much more noticeable in the legal profession.⁹

The rule of law is thus fundamentally threatened by the State's use of algorithmic tools. Openness in decision-making reduces people's ability to challenge unfavourable decisions and calls into question the need for reasoned commands. Conventional legal accountability systems are complicated by the dispersion of accountability among designers, data producers, and deployment authorities. Algorithmic systems run the potential of turning administrative judgment into a kind of technical authority that is hard to examine or contest in the absence of explicit guidelines controlling their application. Therefore, comprehending algorithmic governance necessitates going beyond a technological or efficiency-based examination. It necessitates a constitutional and legal investigation into the ways in which algorithmic systems interact with basic rights, administrative law, and democratic administration. This requires analysing whether algorithmic governance can be reconciled with principles like equality, due process, transparency, and human dignity within the Indian constitutional framework, or if it necessitates reconsidering current legal doctrines in order to address new forms of state power.¹⁰

Understanding algorithmic prejudice is essential to comprehending the constitutional issues that AI-driven decision-making raises. The existence of systematic mistakes in AI systems that produce unfair or discriminating results is the fundamental definition of algorithmic bias. Although they may not be deliberate, these biases frequently result from the data and algorithmic design decisions. Typically, historical datasets are used to train AI systems, and these datasets may contain biases and societal injustices. These biases can be reinforced and even amplified by the algorithms that come from using such data without sufficient inspection. Algorithmic bias can take many different forms, such as deployment bias, design bias, and data bias. Inaccurate or discriminating predictions result from incomplete,

⁹ Matej Avbelj, *Reconceptualizing Constitutionalism In The AI Run Algorithmic Society*, German Law Journal (Cambridge University Press), Vol-25(7), (Oct 28, 2024) <https://www.cambridge.org/core/journals/german-law-journal/article/reconceptualizing-constitutionalism-in-the-ai-run-algorithmic-society/F83A866AD4B9A80BA3622F49D63AF725>

¹⁰ Akanksha Surana, Arjit Pandey and Watnesn Dubey, *Algorithmic Governance and The Rule of Law in India: Regulatory Artificial Intelligence Beyond Automation*, IJDDT, Vol-6(10), 315-317, (2026) <https://impactfactor.org/PDF/IJDDT/16/IJDDT,Vol16,Issue10s,Article43.pdf>

biased, or unrepresentative training data. The interaction of technology, law, and society is essentially highlighted by the conceptual framework of algorithmic bias and AI-driven governance. Evaluating the constitutional implications of AI and creating efficient regulatory responses require an understanding of these processes.¹¹

Constitutional challenges in the age of algorithm:

The primary pillar of the state system, the constitution serves as the foundation for the legitimacy of all types of governmental authority. The constitution protects citizens' rights, acts as the supreme source of law, and provides direction for governmental officials. The advancement of technology, especially digitalization and artificial intelligence (AI), has created new structural and substantive issues for the constitution. According to John Locke, the legitimacy of power can only be acknowledged to the degree that the state upholds people's fundamental rights. The state's operations, including public service, oversight, and law enforcement, are altered by digital revolution. The challenges of digitalization also bring up new constitutional issues that the traditional legal framework did not fully anticipate, such as data privacy, digital surveillance by the state, the misuse of algorithms for political purposes, and violations of digital rights like the right to be forgotten. Constitutional protection of human rights needs to be expanded to include the digital dimension. The principles of freedom of expression and the right to privacy now encompass not only physical actions but also online activities.¹²

Another problem is institutional reluctance to change. In addition to technology advancements, the shift from paper-based to digital workflows requires judges, attorneys, and court employees to adjust their cultures. To guarantee that technology adoption results in significant productivity advantages rather than procedural confusion, training programs, handholding procedures, and iterative feedback loops are crucial. Lastly, some regulatory issues remain unanswered due to the lack of a thorough legislative framework that expressly governs the judicial use of AI and cutting-edge technologies. To prevent abuse and maintain constitutional guarantees of justice and reasoned judgment, clear norms pertaining to openness,

¹¹ Seema Mumtaz, *Algorithmic Bias, Discrimination and The Rule of Law: Examining the Constitutional Implications of AI Driven Decision-making in Public Administration*, International Journal of Multidisciplinary Trends, Vol-8(4), (116-123), (2026) <https://www.multisubjectjournal.com/article/1045/8-4-45-314.pdf>

¹² Sya'baniatie Ninda Septia, *The Transition from Conventional Constitution to Digital Law: Constitutional Law Challenges in the Age of Artificial Intelligence*, Journal of International Multidisciplinary Research, Vol-4, (59, 61), (Jan 1, 2026)

auditability, and accountability of AI-assisted tools will be required.¹³

This particular guarantee is based on the fundamental right to good administration, which is protected by Article 41 of the EU Charter of Fundamental Rights and is a general principle of EU law. How machine-learning algorithms meet the criteria of Article 41 Charter, including the responsibility of care and the duty to give explanations imposed as a matter of EU law, is a difficult subject resulting from the usage of AI systems in public administrations. Jan draws attention to the issues with the fundamental right to good administration that are brought up by machine learning algorithms utilized in fully automated systems and recommender systems. Then suggests extra precautions and possible by design ways to address these challenges.¹⁴

Specific challenges in constitution:

Online harms against freedom of expression: Digital platforms function as contemporary public spaces, but they also disseminate deepfakes, hate speech, and fake news. Through material removal, censorship, and internet shutdowns, governments attempt to manage this, sometimes limiting true freedom of speech.

Privacy and Data Protection Concerns: Data tracking and gathering are crucial to the digital economy. Privacy rights are frequently violated as a result of lax legislation, extensive governmental authority, and ambiguous consent procedures.

Algorithmic Bias and Equality Issues: AI systems may generate biased outcomes, particularly impacting marginalized populations, because they are not always transparent or fair. The constitutional provision of equal treatment is directly challenged by this

Excessive Power of Big Tech corporations: By establishing guidelines for online conduct, big tech corporations function as quasi-governments. Without being held democratically accountable, they are able to restrict material, remove users, and sway political debates.

¹³ W.Micklitz, Oreste pollicino, Amnon Reichman and Andrea Simoncini, *Constitutional Challenges In The Algorithmic Society*, Cambridge University Press, (1,57), (2022) https://www.cambridge.org/core/services/aop-cambridgecore/content/view/831B39F76C7870B330052D852D598F98/9781108843126AR.pdf/Constitutional_Challenges_in_the_Algorithmic_Society.pdf?event-type=FTLA

¹⁴ Can Oirsouw, Charlotte and Jurgen, *Constitutional Law in the Digital Era*, TILBURG University, (2, 6), (2024) <https://repository.tilburguniversity.edu/server/api/core/bitstreams/0abe31bb-c0e4-4390-8a4a-5d3eab4e7a52/content>

Digital Divide and Inequality: People without adequate internet access or digital skills are left behind as services like banking, healthcare, education, and governance shift online. This affects the right to life and equal opportunity by causing inequality and restricting access to fundamental rights.¹⁵

Judicial, Regulatory and Constitutional Accountability framework for algorithmic governance in India:

Constitutional Protection of Digital Rights: The Constitution of India forms the foundation for protecting rights even in the digital world.

State of West Bengal v. Anwar Ali Sarkar, AIR 1952 SC 75:

In India, Article 14 jurisprudence essentially starts at this point. A section of the West Bengal Special Courts Act, 1950 that permitted the government to refer cases to a special court without establishing any standards for doing so was overturned by the Supreme Court. It maintained that every categorization made by the State must be based on "intelligible differentia" that have a logical connection to the goal of the legislation. Apply that to an algorithm: if a government system divides people into groups for benefits or scrutiny, the data points used to create those groups must pass the Anwar Ali Sarkar test. A variable that has no logical relationship to the scheme's goal fails this test.

E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3:

Twenty years later, the Court introduced arbitrariness as a second criteria to Article 14 in a ruling by Justice P.N. Bhagwati. It maintained that equality and arbitrariness are "sworn enemies" and that, regardless of whether a formal classification is involved, any arbitrary State action is unfair and illegal. Once judgments are transferred to code, consider the implications. Royappa was designed to forbid a system that denies a benefit based on a score that no one can explain, not even the individuals in charge of it.¹⁶

¹⁵ Vajiram Content Team, *Digital Constitutionalism, Challenges, Legal Framework in India & Global*, Vajiram & Ravi, Institute for IAS Examination, (June 1, 2026) <https://vajiramandravi.com/current-affairs/digital-constitutionalism/>

¹⁶ Ayushman Anand, *Algorithmic Discrimination and Article 14: Constitutional Challenges in the Age Of AI*, Legal Blur, (June 22, 2026) <https://legalblur.com/algorithmic-discrimination-and-article-14-constitutional-challenges-in-the-age-of-ai/>

Tomaso Bruno v. State of Uttar Pradesh, (2017) 7 SCC 178:

The importance of digital artifacts as possible "best evidence" is highlighted by this ruling. The Supreme Court ruled that the prosecution's inability to provide accessible electronic material and instead relied on witness statements that they had seen such footage was legally insufficient, citing the presence of CCTV cameras at the pertinent area. "The Court determined that the adverse inference under Section 114(g) of the Evidence Act was justified by the failure to produce readily available electronic evidence." The decision is a strong indication from the court that, in cases where such evidence is available, investigative agencies must preserve and present electronic recordings.

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

In a unanimous verdict delivered by a 9 judge's bench of the hon'ble SC recognised that "the right to privacy as a fundamental right intrinsic to Articles 14, 19, and 21 of the Constitution". The Court established three criteria for acceptable limitations: proportionality, legitimate governmental purpose, and legality. Puttaswamy offers the constitutional foundation for data governance in the context of judicial digitalization, which includes e-filing systems, live streaming of sessions, online cause lists, and digital decision repositories. Along with the Digital Personal Data Protection Act, 2023, it strengthens the concepts of purpose limitation and data minimization, influencing later policy discussions and legislative actions. Therefore, the use of technology in courts must be restricted, driven by necessity, and authorized by law.¹⁷

Digital Personal Data Protection (DPDP) Act, 2023:

In India, the gathering, storing, processing, and use of personal data are governed under the Digital Personal Data Protection Act, 2023. It gives people, referred to as Data Principals, significant control over their personal data, including the ability to access, amend, correct, and request that their data be erased. Organizations known as "Data Fiduciaries" are subject to substantial requirements under the Act, which include processing personal data in a way that is lawful, secure, and responsible while putting in place the necessary protections to prevent misuse or unauthorized access. Additionally, the Act promotes better transparency, trust, and

¹⁷ Gourav and Diptimoni Boruah, *Reimagining the Indian Judiciary in Digital Era: A Critical Study*, International Journal of Applied Research, Vol-12(2), (8, 12), (2026)
<https://www.allresearchjournal.com/archives/2026/vol12issue2/PartA/12-1-87-538.pdf>

privacy protection in the digital ecosystem by introducing sanctions and enforcement procedures for non-compliance, data breaches, and the abuse of personal information.

Information Technology (IT) Act, 2000:

Hacking, identity theft, online fraud, cyberstalking, and data breaches are just a few of the offenses covered by India's cyberspace law framework, which also establishes appropriate punishments and enforcement measures. The law also outlines the obligations of intermediaries, including social media sites and service providers, providing them with safe harbour protection from liability with relation to third-party content, provided that they comply with legal requirements and due diligence standards. Additionally, by giving electronic documents, digital signatures, and online agreements legal validity and enforcement, this framework supports e-commerce and digital trade. The Indian Cyber Crime Coordination Centre (I4C), which operates under the Ministry of Home Affairs, is the central nodal agency for coordinating efforts among law enforcement agencies, raising awareness of cybercrime, and enhancing India's overall cybersecurity ecosystem in order to strengthen cybercrime prevention and investigation.¹⁸

Sector-specific Rules & Policies:

Cybersecurity, digital platforms, telecommunications, and financial technology are all regulated by a number of sector-specific laws and policies that make up India's digital governance framework. The Indian Computer Emergency Response Team's guidelines set forth necessary standards for data retention, cyber incident response, and cybersecurity event reporting. While telecom and fintech regulations control the gathering, processing, and safeguarding of communication and financial data to guarantee security, privacy, and consumer protection, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 set forth due diligence requirements for social media intermediaries and digital platforms.

Net Neutrality Regulations:

The Telecom Regulatory Authority of India's suggestions served as the foundation for

¹⁸ Vajiram Content Team, *Digital Constitutionalism, Challenges, Legal Framework in India & Global*, Vajiram & Ravi, Institute for IAS Examination, (June 1,2026) <https://vajiramandravi.com/current-affairs/digital-constitutionalism/>

India's net neutrality policy, which aims to maintain an open and nondiscriminatory internet. In response to these suggestions, the Department of Telecommunications modified telecom operators' licensing requirements to forbid discriminatory treatment, blocking, throttling, or prioritization of online content, apps, or services. Therefore, all legal online information must be handled equally, with the exception of situations where appropriate traffic management techniques are required to preserve network security, effectiveness, and service quality.¹⁹

Rules and Regulations for Digital Platforms (IT Rules, 2021):

A legal framework for the operation of social media intermediaries and online platforms in India is established by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. According to these regulations, platforms must designate grievance officers and set up efficient procedures for handling user complaints and issues. After obtaining legitimate court orders or notices, intermediaries are required to remove or disable access to unlawful materials, including misinformation, harmful material, and other illegal content, within specified timescales. Significant social media intermediaries may also be obliged by authorized governmental or judicial directives to identify the original sender of particular messages in some serious circumstances involving national security, public order, or criminal investigations. The regulations aim to achieve a compromise between guaranteeing accountability, transparency, and user safety in the digital ecosystem and safeguarding freedom of expression.

Comparative perspective:

Countries all over the globe are struggling to develop strong frameworks to safeguard digital rights as the digital environment becomes more and more important to daily life and governance. The idea of extending constitutional concepts to the digital sphere, known as "digital constitutionalism," has been applied with differing degrees of success. In addition to examining the difficulties encountered by other countries, this part offers a comparative study of case studies from countries that have made notable advancements in digital governance. As nations like India seek to create a strong framework for digital rights, the lessons acquired from

¹⁹ *Digital Constitutionalism*, Vision IAS (Digital Current Affairs), (Jan 23, 2026) <https://visionias.in/current-affairs/monthly-magazine/2026-01-28/polity-and-governance/digital-constitutionalism>

these case studies provide insightful information.²⁰

European Union: Preventive Digital Constitutionalism

The best example of constitutionalism's incorporation into technology governance is the European Union. The European Union's Charter of Fundamental Rights codifies the rights to non-discrimination (Article 21), privacy (Article 7), data protection (Article 8), and human dignity (Article 1). The constitutional foundation of the EU's digital regulation system is represented by these clauses. These rights are operationalized by GDPR (2018) through legally obligatory principles of accountability, transparency, and purpose limitation. The "right not to be subject to a decision based solely on automated processing" is guaranteed under Article 22 of the GDPR, which guarantees human oversight in algorithmic governance. In addition, the AI Act (2024) takes a risk-based approach, classifying AI systems into three categories: unacceptable, high risk, and minimal risk.

The European courts have reinforced the rights-centric governance concept. The CJEU ruled in *Digital Rights Ireland Ltd. v. Minister for Communications* (2014) that mass data retention directives were unconstitutional due to violations of proportionality and privacy. The ECHR ruled in *Big Brother Watch and Others v. United Kingdom* (2021) that indiscriminate surveillance without protections violates Article 8 of the ECHR. The EU's multi-state enforcement framework is complicated, and its regulations can occasionally be overly stringent, which hinders innovation. However, the EU has the most cogent constitutional framework for striking a balance between technological advancement and fundamental rights and human dignity.²¹

United States: Free Speech and Market-Focused Model Strong Rights to Free Speech

Free expression is firmly protected under the U.S. Constitution, particularly the First Amendment. This implies that the government is typically powerless to prevent people from expressing their opinions, even if those opinions are divisive or unpopular. The U.S. government largely avoids stringent regulations regarding what can be said, particularly on

²⁰ Pawan Kumar, *Locating Digital Constitutionalism in India and South Asia - Preliminary Enquiry*, Kathmandu School Law Review, Vol-13, (88,97), (2024) <https://kslreview.org/index.php/kslr/article/view/2237/1576>

²¹ Ashita, *Reimagining Constitutionalism in The Age of Artificial Intelligence: A Comparative Study of India, The European Union and The United States*, International Journal of Innovative Research Technology, Vol-12(6), (6607,6632), (Nov 2025) https://ijirt.org/publishedpaper/IJIRT187866_PAPER.pdf

private websites and platforms, in contrast to many other nations. This demonstrates a strong commitment to individual liberty and concern over excessive governmental power. The United States encourages a competitive atmosphere that fosters the development of novel concepts and innovations. Free markets allow private businesses to develop new tools and platforms that facilitate communication and information sharing. Large private corporations, such as social media platforms, determine what speech is permitted or prohibited. They are not subject to the same restrictions on free speech because they are not a member of the government. This raises a difficult question: should these businesses that regulate public discourse be subject to the same laws as the government?. The United States places more emphasis on preserving free speech and promoting innovative ideas than other nations with more restrictive speech laws. This demonstrates faith in communities and companies to control speech rather than the government intervening.²²

India: Delays in the Personal Data Protection Bill (PDPB)

India is one of the biggest digital economies in the world, with over 850 million internet users in 2024, yet it does not have a comprehensive data protection law. The PDPB was initially presented in 2019 with the intention of establishing a legal framework for data processing regulation and digital rights protection. However, its passage has been delayed by political disputes, worries about state spying, and opposition from digital titans. Despite increasing public demand for its implementation, India still lacks an enforceable data protection law as of 2024 despite the bill's numerous revisions. Rules have not yet been announced as of December 28, 2024.

The PDPB's enactment delays reveal a number of lessons for other countries. Reaching an agreement among stakeholders is a major obstacle. Both the tech sector, which worries about excessive regulation, and civil society organizations, which contend that the measure gives the government too much power, have opposed it. The necessity of legislative process openness is another lesson to be learned from India's experience. The bill's delayed pace has been attributed by critics to a lack of public input and limited debate. India must promote inclusive discourse and strike a balance between state interests and individual rights if it wants to advance with

²² Dr.Aparajita Bhatt, *Comparative Insights Towards A Global Constitutionalism*, Slideshare, (Feb 27,2026)<https://www.slideshare.net/slideshow/digital-constitutionalism-comparitive-insights-towards-a-global-world/286544910>

digital constitutionalism.²³

Recommendations:

1. Enact a Comprehensive AI Governance Law: A specific legal framework governing the use of AI and algorithmic decision-making by public and private entities should be adopted in India. Transparency, accountability, justice, and human monitoring should all be governed by the law.
2. Require Explainability and Transparency in Algorithms: The goal, operation, and decision-making logic of algorithmic systems should be made public by government organizations and online platforms that use them. People who are impacted by automated choices ought to have access to clear explanations.
3. Strengthen Data Protection and Privacy Safeguards: Stronger accountability mechanisms, strong cybersecurity requirements, and efficient remedies for data breaches and misuse should be implemented alongside the Digital Personal Data Protection Act, 2023.
4. Develop Constitutional Principles for AI Governance: In order to create a framework of "constitutional-by-design" government, Indian policymakers should integrate constitutional ideals like equality, justice, liberty, dignity, and the rule of law into the development and implementation of algorithmic systems.
5. Promote the Development of Digital Constitutionalism in the Judiciary: In order to ensure that technological innovation is still subject to constitutional examination, courts should keep developing constitutional law pertaining to algorithmic governance, digital rights, surveillance, and automated decision-making.

India should transition from a technology-centric governance model to a constitution-centric digital governance model, which promotes innovation while adhering to constitutional restrictions, democratic supervision, transparency, and the defense of fundamental rights. India's constitutional democracy can be strengthened rather than undermined by algorithmic

²³ Pawan Kumar, *Locating Digital Constitutionalism in India and South Asia - Preliminary Enquiry*, Kathmandu School Law Review, Vol-13, (88,97), (2024)
<https://kslreview.org/index.php/kslr/article/view/2237/1576>

governance if a strong framework of digital constitutionalism is in place.

Conclusion:

The relationship between the government, private digital platforms, and citizens has changed dramatically as a result of the development of digital technology and algorithmic governance. The growing use of platform governance, data-driven decision-making, artificial intelligence, and surveillance technologies in India has given rise to new constitutional issues that were not intended to be handled by conventional legal frameworks. Digitalization has increased public service delivery and administrative efficiency, but it has also sparked worries about privacy, equality, freedom of speech, accountability, and transparency. In order to guarantee that constitutional principles continue to direct governance in the digital era, the idea of "digital constitutionalism" has become crucial.

The study shows that the Indian Constitution's dedication to fundamental rights, the rule of law, and democratic government gives it the normative power to adapt to technological changes. The basis for defending citizens against arbitrary digital invasions has been established by judicial interventions, including the acknowledgement of privacy as a basic right in *Justice K.S. Puttaswamy v. Union of India*. However, the problems caused by opaque algorithms, automated decision-making, platform domination, and massive data collecting are still not adequately addressed by the current legal framework, which is still disjointed. The lack of thorough guidelines for algorithmic accountability and transparency poses serious threats to constitutional governance.

Therefore, India must develop a robust framework of constitutional accountability that effectively regulates both state and private digital power. Stronger data protection measures, algorithmic transparency requirements, independent regulatory monitoring, protections for digital due process, and significant democratic involvement in technological governance should all be included in such a system. India can guarantee that technology progress stays in line with the ideals of liberty, dignity, equality, and justice by incorporating constitutional principles into the development and functioning of digital systems. In the end, digital constitutionalism is an essential development of constitutional governance for the twenty-first century rather than just a reaction to technical advancement.